secure
sba-research.org

COMET
Competence Centers for
Excellent Technologies

CURRENT RESEARCH

2014

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwfw Bundesministerium für Wissenschaft, Forschung und Wirtschaft
Christian Doppler Forschungsgesellschaft
FFG
FWF
wirtschaftsagentur wien
zit Die Technologieagentur der Stadt Wien

secure
sba-research.org

Table of Content

AREA 4: Hardware and Network Security

A Community Knowledge Base for IT Security

Stefan Fenz

COMET
Competence Centers for Excellent Technologies
www.ffg.at/comet

secure
sba-research.org

Motivation and Problem

- Corporate IT security managers have a difficult time staying on top of the endless tide of new technologies and security threats.
- IT security managers in different organizations face many of the same threats and establish similar solutions, which is clearly inefficient.

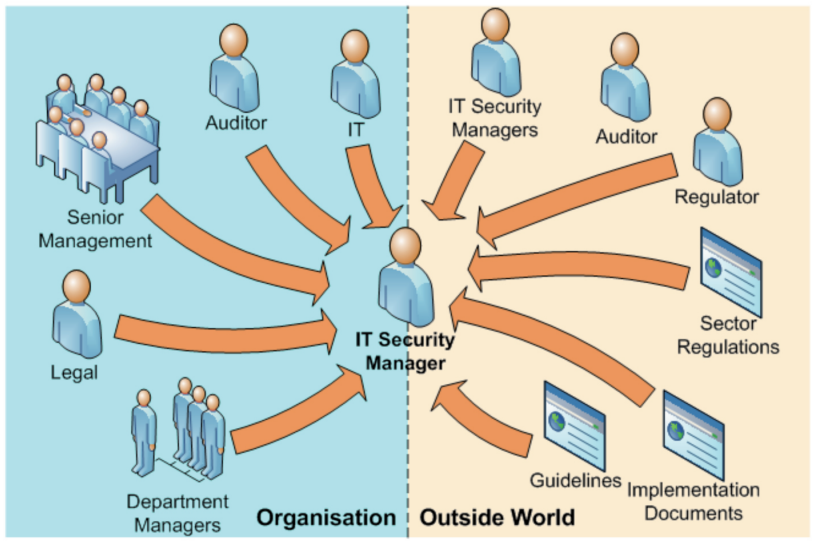


Figure 1: Motivation and Problem

Creating a community knowledge base

- We propose taking an open, shared approach to creating and managing information security knowledge by pooling our efforts to formalize a user-community knowledge base.
- Using consistent, unambiguous classification for the underlying knowledge systematizes the addition and subsequent communication of new and disparate sources of advice and their inherent vocabularies.
- A formalized knowledge base can inform many aspects of information security management, such as risk management, IT security investment trade-offs, compliance checks, and awareness training in an automated way.

The security ontology web portal (sec.sba-research.org)

- Supports role-based user access control, so editing is restricted to defined roles and the corresponding users.
- On the left-hand side, the user selects the entity of interest in the context of the ontological knowledge model (for example, "Malware" threat).
- The right-hand side shows detailed knowledge such as natural-language labels, definitions and comments, entity relationships (such as vulnerabilities that are exploited by the malware threat), and community notes regarding the entity.
- The portal enables structured knowledge sharing by
  - providing a fixed high-level knowledge structure (threats, vulnerabilities, controls, etc.)
  - enabling registered users to edit, discuss, and agree on the knowledge;
  - annotating each change with metadata such as username and time stamp; and
  - providing the knowledge in a standardized form to other applications (for example, for risk or compliance management).

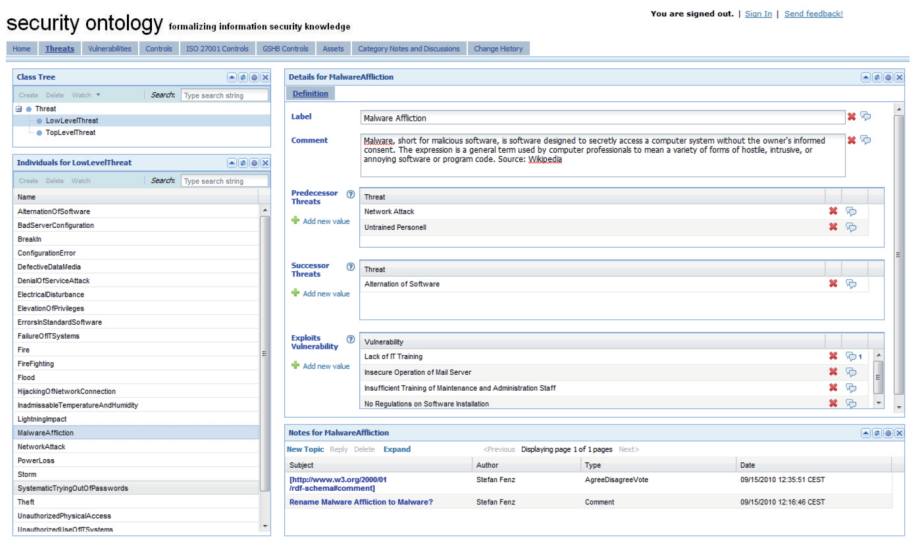


Figure 2: The security ontology portal: sec.sba-research.org

Upcoming Challenges

- Reaching critical mass of users
- All users edit the same ontology and its concepts, so moderators have to decide which knowledge fragments are – according to the majority of users – more accurate and which aren't broadly accepted by the community.
- The knowledge base serves to address shared problems that arise and change. Potential inconsistencies must be addressed by the community, moderators, and (on a logical level) reasoning engines, but despite being perpetually incomplete, a knowledge base can empower the community to address shared challenges.

S. Fenz, S. Parkin, A. van Moorsel: "A Community Knowledge Base for IT Security," in IT Professional, Vol. 13/3, 2011.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

A Holistic Security Concept for Workflow Systems

Jürgen Mangler, Maria Leitner and Stefanie Rinderle-Ma

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org
universität wien

The SPRINT* Approach – Responsibility-based RBAC Model

(1) Step 1 – Acquisition and Security Design

A responsibility is a piece of data (e.g., a document, information) or a set of interrelated tasks from the point of a certain role. Responsibilities enumerate data and interrelated work tasks as objects that can be constrained, bundled and assigned to roles in an organizational structure to describe all aspects of security policies.

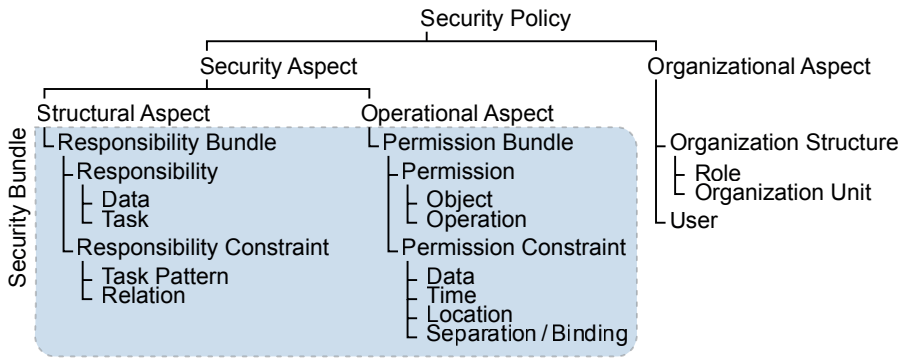


Figure 1: Security Policy – Aspects, Bundles and Relationships

(2) Step 2 – Assigning Responsibilities to Process Models

Responsibilities (data, tasks) are directly assigned to process steps.
All other aspects are connected to responsibilities and thus indirectly to process steps.

- **Structural process model security: responsibilities and constraints**
- **Runtime process security enforcement: permissions and constraints**
- **Role selection based on mapping by looking up roles for responsibilities assigned to process steps**

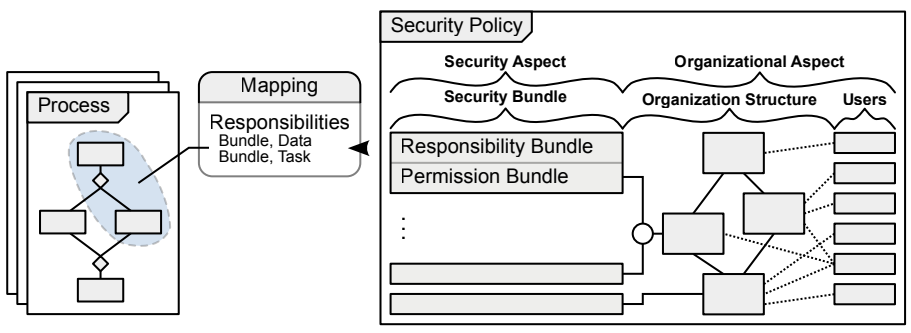


Figure 2: Security Policy Mapping

Evaluation

(1) Comparison to Existing Approaches

	AristaFlow / SeaFlows	Apache ODE	Declare	YAWL	SPRINT
Policy Modeling					
Notation	WSM-Net / CRG, FOL	WS-BPEL	LTL	Extended Workflow Nets	PPMEX
Implementation	Task / Repository	Task	Task	Task	Repository
Basic Role Assignment	☒ / ⊡	⊡	☒	☒	☒
Advanced Role Assignment	☒ / ⊡	⊡	☐	☒	☒
Policy Constraint Properties					
Basic Data	☒ / ☒	☒	☒	☒	☒
Basic Time	☒ / ⊡	☒	☒	☒	☒
Basic Location	⊡ / ☒	⊡	⊡	⊡	☒
Policy Enforcement and Monitoring (Examples)					
Data	☒ / ☒	☒	☒	☒	☒
Time	☒ / ⊡	☒	⊡	☒	☒
Location	⊡ / ☒	⊡	⊡	⊡	☒
Separation/Binding of Duty	☒ / ⊡	⊡	☒	☒	☒
Policy Verification					
Conflicting Policies	☒ / ⊡	☐	☒	☒	⊡
Empty Valid Actor Set	⊡ / ⊡	☐	⊡	⊡	☒

Legend:
☒ . . . supported
⊡ . . . support with extensions possible
☐ . . . not supported

Figure 3: Evaluation of Workflow Execution Tools

(2) Prototype Implementation

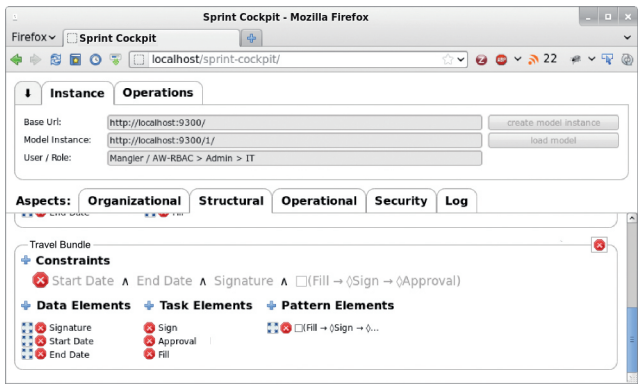


Figure 4: SPRINT Cockpit: Security Mapping

State of the Art in Workflow Security

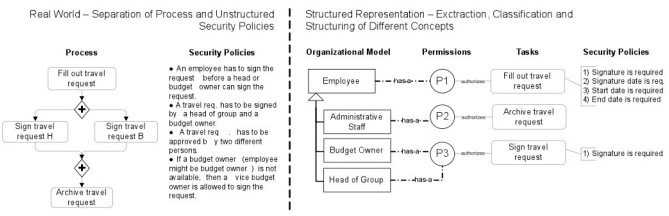


Figure 5: Process Modeling and Security Policies

Future Work

- **Performance and scalability evaluation compared to other approaches**
- **Visualization of the relationship between security and processes**
- **Efficient security management in organizations by streamlining the whole security design process based on the proposed approach**
- **Cross-organizational process settings**

Reference
M. Leitner, J. Mangler, and S. Rinderle-Ma, "SPRINT- Responsibilities: Design and Development of Security Policies in Process-aware Information Systems," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), vol. 2, no. 4, pp. 4–26, Dec. 2011.

bmvit bmwf FFG zit Christian Doppler Forschungsgesellschaft FWF Der Wissenschaftsfonds.
Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

An ontology-based approach for constructing Bayesian networks

Stefan Fenz

COMET
Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

Motivation and Problem

- **Bayesian networks are commonly used for determining the probability of events that are influenced by various variables.**
- **The following challenges arise at the construction of Bayesian networks:**
  - identification of variables that are relevant to the considered domain (nodes),
  - identification of relationships between the identified variables (links), and
  - creation of the conditional probability table for each variable.
- **Approaches aiming at reducing the number of probabilities to be assessed and tools for supporting the quantification task in the construction of Bayesian networks are required.**

Goals

- **Based on existing domain ontologies, we developed a method for the ontology-based construction of Bayesian networks. The method supports the automated**
  - construction of the graphical Bayesian network structure (nodes and links)
  - construction of CPTs that preserve semantic constraints of the ontology, and
  - incorporation of already existing knowledge facts (findings).

Approach

- **The proposed ontology-based approach for constructing Bayesian networks consists of four main phases:**
  1. Selection of relevant classes, individuals, and properties
  2. Creation of the Bayesian network structure
  3. Construction of the CPTs
  4. Incorporation of existing knowledge facts
- **While the first phase requires the input of a domain expert, the remaining three phases are conducted automatically based on the output of phase 1.**

Evaluation

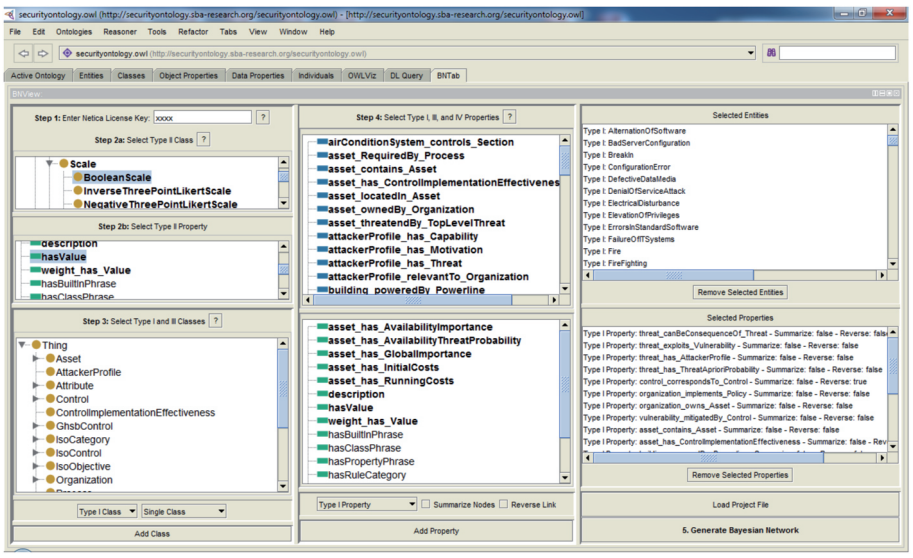


Figure 1: Prototype – user interface

- **Within the evaluation we produced a basic Bayesian network containing 557 nodes, 579 directed links, and 30,687conditional probabilities. Our tool enabled the domain expert to create a Bayesian network within 5 min.**
- **Estimated manual construction time without the calculation of 30,687 conditional probabilities: 2.5 h.**
- **The proposed method saves time, especially in the construction of Bayesian networks with more than 18 nodes.**

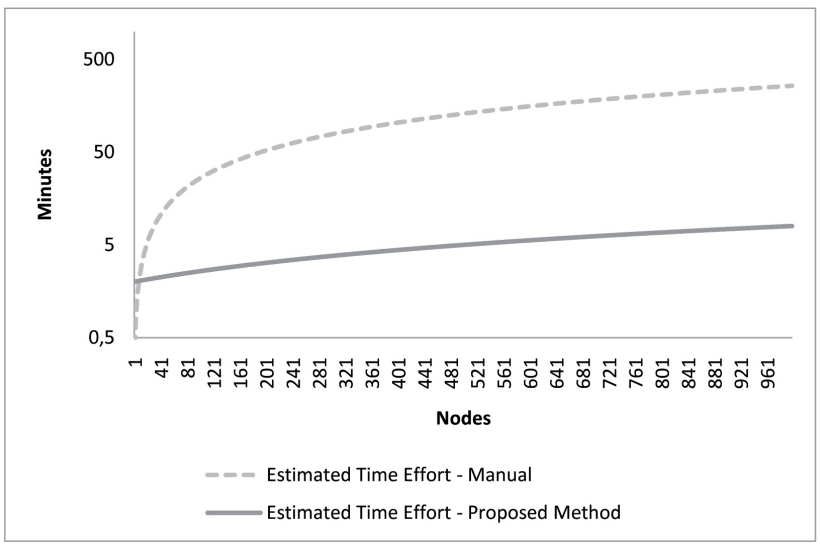


Figure 2: Evaluation – estimated time effort

Conclusion

- **Compared to existing approaches we provide a Bayesian network construction method that**
  - uses already existing ontologies without the requirement for specific extensions for Bayesian network construction
  - reduces the complexity and time effort of modeling Bayesian networks by using high-level classes and properties to integrate relevant sub-classes into the Bayesian network
  - utilizes already existing findings and their weights at the construction of CPTs
  - preserves the ontological semantics at the CPT construction.

S. Fenz: "An ontology-based approach for constructing Bayesian networks" in Data & Knowledge Engineering, Vol. 73, 2012.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Changes in Process Life Cycle: Requirements Analysis for Visualizations

Simone Kriglstein and Stefanie Rinderle-Ma

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org
universität wien

Motivation

Process models evolve over time. Hence changes are necessary and have an impact on security-relevant information in each phase of the business process life cycle, e.g., because of:

- **incomplete specifications because events cannot always be prescribed**
- **modifications that are based on new or changed conditions**

Visualizations are helpful, because they:

- **help users to understand the changes and their dependencies easier**
- **make things visible or present things in a new light that users were not aware of before and support them in their decisions**

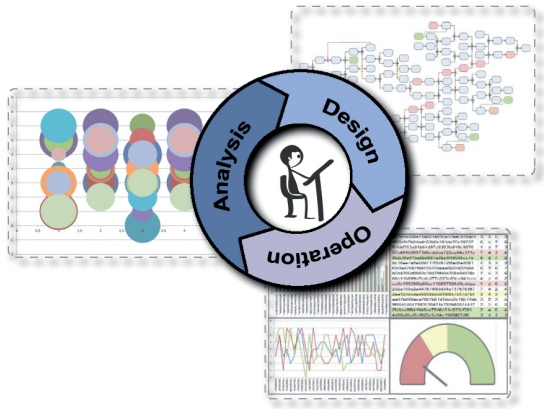


Figure 1: Scenarios for analysis of changes

State of the Art

Characteristics of Changes

- **Ad-hoc vs. Evolutionary**
  - Ad-hoc changes are only relevant for one or more selected process instances
  - Evolutionary changes are modifications of the process model that are relevant for all instances
- **Entry Time vs. On-the-fly**
  - Entry time means that changes can be performed only before the process instance is created
  - On-the-fly means that changes can be performed at any time and they can have an impact on running as well as new process instances
- **Change Patterns**
  - Change patterns specify how processes can be changed

Visualization Approaches

- **Graph**
  - Business processes are usually visualized as directed graphs to make the flow of resources, tasks, and time visible
- **3D vs. 2D**
  - 3D is a possibility to encode further information in a single view
- **Animation**
  - Animations can help users to trace changes and to understand the process flow more easily

Methodology

For an effective use of visualizations, it is important that the design meets users' needs and is adequate for the tasks users want to solve with the visualization. For the requirement analysis we used:

- **Literature review**
  - What are the characteristics of changes in processes?
  - Which visualization approaches exist already?
- **User survey**
  - Which experiences do users have with process visualizations?
  - Which expectations do users have of the visualization of changes in processes?

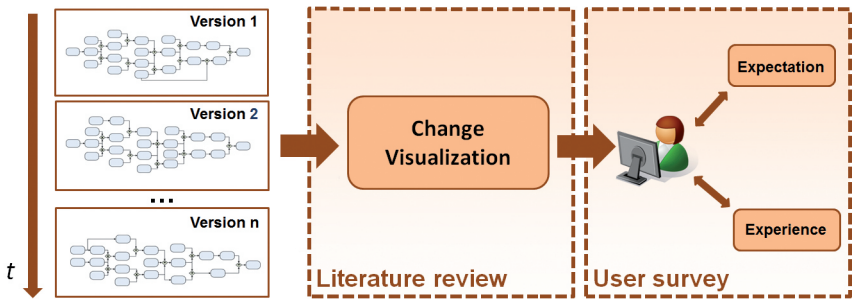


Figure 2: Structure of the requirements analysis

Requirements

- **Clear change representation**
  - to enable users to track the changes between the different versions
- **Visibility of relationships between versions**
  - to see the dependencies between the different process versions
- **Different views**
  - to support users in analyzing changes from different perspectives
- **Interaction**
  - to support strategies for manipulating the visualization

Future Work

We will investigate different forms of presentation for analyzing change information and we plan to design multi-modal approaches (e.g., to combine visualization methods with sonification methods) especially in cases where visualizations reach their limits.

References
Kriglstein, S., and Rinderle-Ma, S.: Change Visualization in Business Processes - Requirements Analysis. In Proc. of the International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (GRAPP/IVAPP), SciTePress, 2012, pp. 584-593.
Hildebrandt, T., Kriglstein, S., and Rinderle-Ma, S.: On Applying Sonification Methods to Convey Business Process Data. In CAiSE Forum 2012 (to be published in 2012).

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Context-aware Security Analysis of Mashups

Heidelinde Hobel, Edgar Weippl, Amin Anjomshoaa

COMET
Competence Centers for Excellent Technologies
www.ffg.at/comet

secure
sba-research.org

Background

Mashups facilitate software development:

- support from mashup editors
- programming is just dragging and dropping of predefined modules (operations) and connecting them

Mashup solutions are aimed to exploit the full potential of software development for end users.
Mashups are used for (sophisticated) data processing applications.

Software development is shifting into end users' hands.

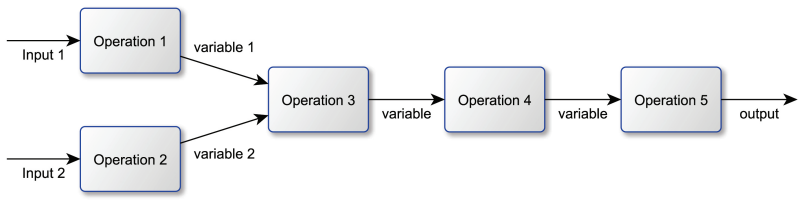


Figure 1: Mashup concept – programming is just dragging and dropping of predefined operations

Methodology

Identification and analysis of security, privacy, and other problems arising with the mashup concept.
Introduction of a new security model / framework in order to prevent or mitigate

- information leakage
- sensitive aggregation
- distribution of data to unauthorized people

Presentation of a prototype implementation and experimental evaluation based on use cases.

Prototype & Proof of Concept (PoC)

The prototype is based on a central platform where mashup solutions can be uploaded and evaluated to see if the mashup's design adheres to the enterprise's policies.
The mashup's design, the context, such as the enterprise's data structure or staff roles, as well as the enterprise's policies are described and implemented through Semantic Web technologies.
The Proof of Concept implementation of the proposed platform is based on a typical peer-review system.

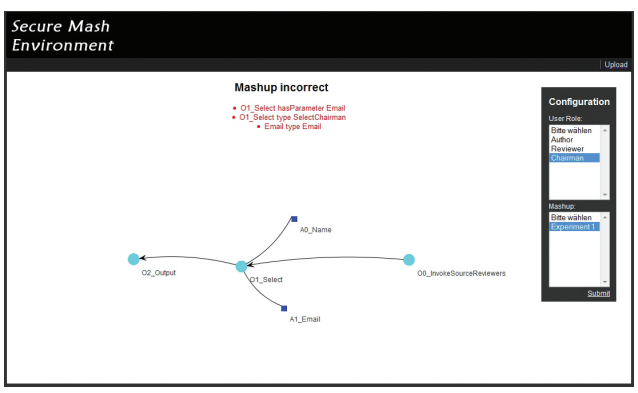


Figure 4: Screenshot of the implemented analysis tool – analysis of security-related relations of a submitted mashup solution (visualized as a graph) and output of the automatically generated explanation (in red).

Motivation

- With the use of mashups, security, privacy and trust issues arise.
- Mashups are used for business (Enterprise Mashups).
- Hence, we need new security models for the protection of
  - the enterprise's data
  - personal data
  - aggregation of sensitive data

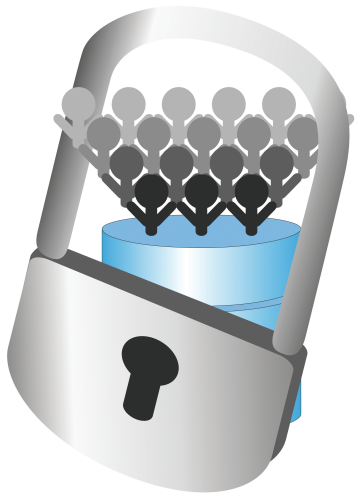


Figure 2: Protecting sensitive data

Enterprise Mashups facilitate unregulated data processing.

Framework

IThe system architecture of the proposed approach is based on the fundamental Enterprise/Web Architecture and extends the existing functionality by a module that

- validates mashups based on a ruleset and
- allows the server-side execution of accepted mashups

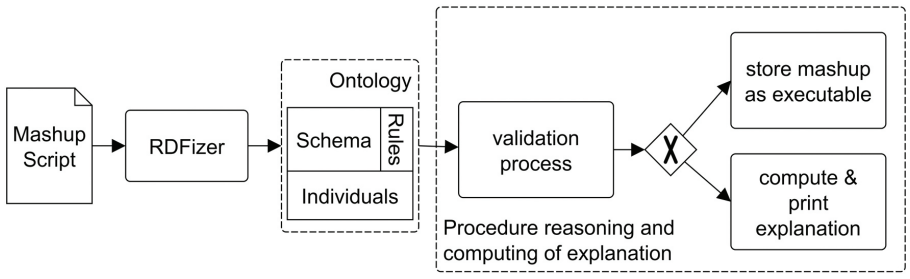


Figure 3: Validation procedure

Evaluation & Conclusion

The security model based on Semantic Web technologies facilitates

- establishing and enforcing rules for composing a mashup
- context-awareness
- pattern specifications for mashup designing

The policies are described by logic, therefore

- the analysis of mashup compositions could be automatically processed by machines or reasoners
- the ontology can only cover what is defined for our domain; this means that anything that is forgotten in the design of the ontology will not be enforced by the reasoning system

From the experiments we can learn that the proposed approach could be used to prevent malicious mashup compositions that violate the defined policies or restrictions.

Master Thesis: Context-aware Security Analysis of Mashups (Heidelinde Hobel, Advisor: Edgar Weippl, Assistance: Amin Anjomshoaa)
H. Hobel, J. Heurix, A. Anjomshoaa, E. Weippl: "Towards security-enhanced and privacy-preserving mashup compositions", in IFIP International Information Security Conference 2013: Security and Privacy, 2013. (forthcoming).

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwf Bundesministerium für Wirtschaft, Familie und Jugend
FFG
wirtschaftsagentur wien zit Die Technologieagentur der Stadt Wien
Christian Doppler Forschungsgesellschaft
FWF Der Wissenschaftsfonds.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Ethics in Security Research

Sebastian Schrittwieser, Martin Mulazzani, Edgar Weippl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

Recent Publications

- Spamalytics – An empirical analysis of spam marketing conversion
  - Analysis of the economics behind a spam-sending botnet
  - Infiltration of a botnet and analysis and manipulation of a small percentage of messages in a way that the receivers' actions were trackable
  - **Arguments:** "passive actors", "ensuring neutral actions", "users should never be worse off due to our activities"
- Your Botnet is My Botnet: Analysis of a Botnet Takeover
  - Description of the takeover of a botnet for analysis purposes
  - **Arguments:** "The sinkholed botnet should be operated so that any harm and/or damage to victims and targets of attacks would be minimized", "The sinkholed botnet should collect enough information to enable notification and remediation of affected parties"
- Pharmaleaks – understanding the business of online pharmaceutical affiliate programs
  - Analysis of underground economics of affiliate networks for pharmaceutical products on the Internet
  - **Arguments:** "[...] ethics of using data that was, in all likelihood, gathered via illegal means. [...] We justify our own choice [...] by reasoning about harm", "some [...] contents have already been widely and publicly documented. Consequently, we cannot create any new harm simply through association with these entities or repeating these findings"
- Is the Internet for Porn? An Insight Into the Online Adult Industry
  - Analysis of the economics behind traffic trading networks for websites offering adult content
  - **Arguments:** "Clearly, one question that arises is if it is ethically acceptable [...] to participate in adult traffic trading. [...] we believe that realistic experiments are the only way to reliably estimate success rates of attacks in the real-world", "we did not withdraw any funds but forfeited our traffic trading accounts at the end of the experiments"

Problem Description

- Thinking about how research results could be misused
- Research activities themselves should not harm others
- Encouraging a discussion of how research activities in the field of information security can be evaluated from an ethical point of view and how we can establish universal standards

Fundamental Principles

These principles do not follow any particular ethical guidelines nor are they borrowed from other science areas such as medicine. Instead, we tried to derive the most fundamental principles from common sense.

- Do not harm humans actively!
  - Researchers should not actively harm others
  - Medical research: Tuskegee syphilis experiment
  - Non-scientific Craigslist Experiment
- Do not watch bad things happening!
  - Researchers should not watch bad things happening without helping
  - Spamalytics: "passive actors" = Watching without helping
  - Botnet: "damage to victims [...] would be minimized" – victims were only informed after the experiments
- Do not perform illegal activities to harm illegal activities!
  - Is being unethical to the unethical unethical?
  - Botnet: Intercepting a "legal botnet" (SETI@home) would be unethical
    → Is a similar activity ethical simply because it is aimed at "bad" people?
- Do not conduct undercover research!
  - In academic research, cooperation with law enforcement is not yet common in many countries
  - Paper on adult traffic trading: "Believe that realistic experiments are the only way to reliably estimate success rates of attacks in the real-world"

Conclusions und Outlook

- The information security research community is well aware of ethical questions within their field → discussion of ethical issues in research papers, IRBs at universities in the US, review board for FP7 projects
- The comparison has shown how difficult it is to fulfill even the most fundamental ethical principles
- A more open discussion of ethical aspects of our research would be desirable (cf. Menlo Report)
- The gap between what is technically possible and what is acceptable from legal and ethical points of view is huge

S. Schrittwieser, M. Mulazzani, E. Weippl: „Ethics in Security Research - Which Lines Should Not Be Crossed?" in Cyber-security Research Ethics Dialog & Strategy Workshop (CREDS 2013).

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Implementation and Evaluation of the BusinessActivities Framework

Sigrid Schefer-Wenzl, Mark Strembeck

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

WU Wirtschaftsuniversität Wien Vienna University of Economics and Business

BusinessActivities Modeling Framework

- aims to support the specification, implementation, and enforcement of process-related security properties
- provides support for process-related security properties at the computation-independent model (CIM), platform-independent model (PIM), and platform-specific model (PSM) layers
- at the PIM level, we provide a number of UML extensions that extend the UML with modeling primitives for process-related security properties

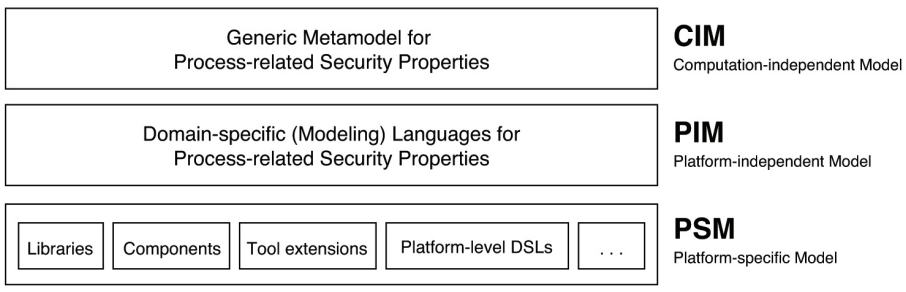


Figure 1: The approach includes all MDD layers

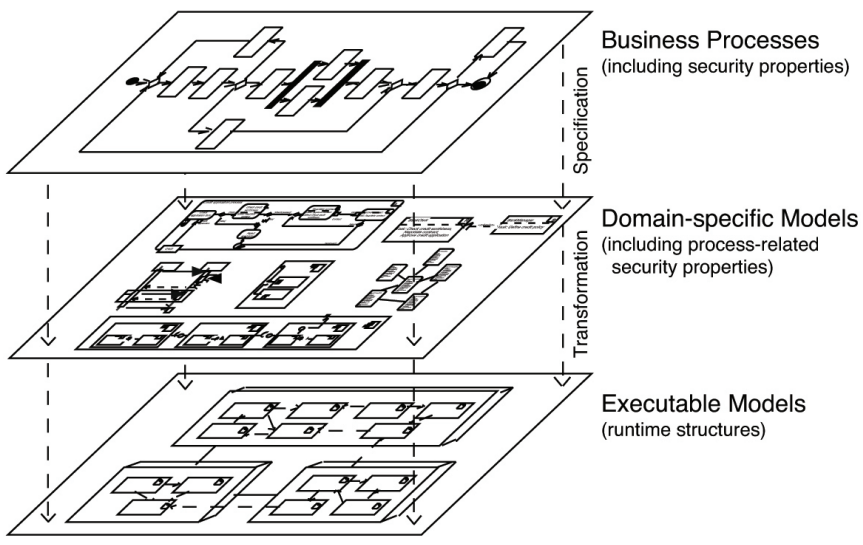


Figure 2: Mapping of process-related security properties to runtime structures

Business Activity Library and Runtime Engine

- software platform to manage process-related security properties and enforce different kinds of security policies and constraints
- provides a runtime environment for executable BusinessActivity models
- BusinessActivity (UML) models can be mapped to corresponding runtime instances
- automatically enforces all invariants that are defined for the BusinessActivity UML extensions

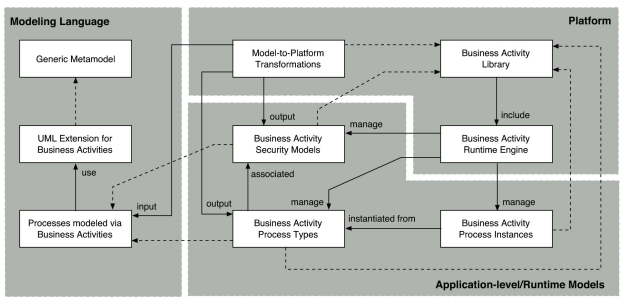


Figure 3: Modeling and runtime support for Business Activities: conceptual overview

Qualitative Multi-Method Study

- evaluation of the practical applicability of our approach on real-world business processes
- evaluation based on case studies and interviews

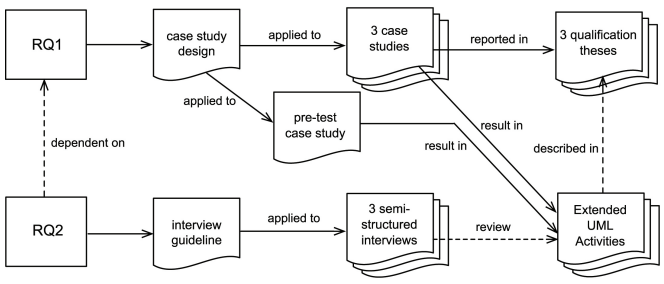


Figure 4: Multi-method evaluation of modeling extensions

Results:

- extension syntax was used correctly by case study participants
- BusinessActivity UML extensions easy to learn for users who are familiar with the UML
- enables a consistent and easy-to-understand documentation of business processes and related security concerns
- improvement of general awareness of security requirements

Outlook

- additional case studies to further evaluate the approach
- experimental studies to evaluate tailored graphical symbols for modeling process-related security properties
- extension of the BusinessActivity library and runtime engine
- integration with (other) security engineering software tools

S. Schefer-Wenzl, M. Strembeck: Modeling Context-Aware RBAC Models for Mobile Business Processes In: International Journal of Wireless and Mobile Computing (IJWMC), 2013,
B. Hoisl, S. Sobernig, M. Strembeck: Modeling and Enforcing Secure Object Flows in Process-driven SOAs: An Integrated Model-driven Approach, In: Software and Systems Modeling (SoSyM), Springer, 2013
S. Schefer-Wenzl, S. Sobernig, M. Strembeck: Evaluating a UML-Based Modeling Framework for Process-Related Security Properties: A Qualitative Multi-Method Study, In: Proc. Of the European Conference on Information Systems (ECIS), Utrecht, The Netherlands, June 2013
S. Schefer-Wenzl, M. Strembeck: Generic Support for RBAC Break-Glass Policies in Process-Aware Information Systems, In: Proc. of the 28th ACM Symposium on Applied Computing (SAC), Coimbra, Portugal, March 2013.
S. Schefer-Wenzl, M. Strembeck: A UML Extension for Modeling Break-Glass Policies, In: Proc. of the 5th International Workshop on Enterprise Modelling and Information Systems Architectures (EMISA), Lecture Notes in Informatics (LNI), Vol. 206, Vienna, Austria, September 2012.
S. Schefer-Wenzl, M. Strembeck, A. Baumgrass: An Approach for Consistent Delegation in Process-Aware Information Systems, 15th International Conference on Business Information Systems (BIS), Springer LNBIP, Vol. 117, May 2012.
S. Schefer, M. Strembeck, J. Mendling, A. Baumgrass: Detecting and Resolving Conflicts of Mutual-Exclusion and Binding Constraints in a Business Process Context, In: Proc. of the 19th International Conference on Cooperative Information Systems (CoopIS), Springer LNCS, Vol. 7044, October 2011.
M. Strembeck and J. Mendling: Modeling Process-related RBAC Models with Extended UML Activity Models. In: Information and Software Technology (IST), Vol. 53, No. 5, May 2011
M. Strembeck, J. Mendling: Generic Algorithms for Consistency Checking of Mutual-Exclusion and Binding Constraints in a Business Process Context, In: Proc. of the 18th International Conference on Cooperative Information Systems (CoopIS), Springer LNCS, Vol. 6426, Crete, Greece, October 2010

The complete list of publications and the source code the BusinessActivity library and runtime engine is available at: http://wi.wu.ac.at/home/mark/BusinessActivities/index.html

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwf Bundesministerium für Wirtschaft, Familie und Jugend
FFG
wirtschaftsagentur wien zit Die Technologieagentur der Stadt Wien
Christian Doppler Forschungsgesellschaft
FWF Der Wissenschaftsfonds.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Information Security Risk Management: In which security solutions is it worth investing?

Stefan Fenz, Andreas Ekelhart and Thomas Neubauer

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

Motivation

- Companies are increasingly exposed to information security threats
- Information security risk management provides an approach for measuring the security through risk assessment, risk mitigation, and risk evaluation.
- Decision makers lack well-founded techniques that (1) show them what they are getting for their investment, (2) show them if their investment is efficient, and (3) do not demand in-depth knowledge of the IT security domain.

Goals

- How can we comprehensibly calculate information security standard-compliant IT security solution portfolios?
- How can we effectively communicate the portfolios' risk versus cost trade-off figures to management decision makers?

Solution

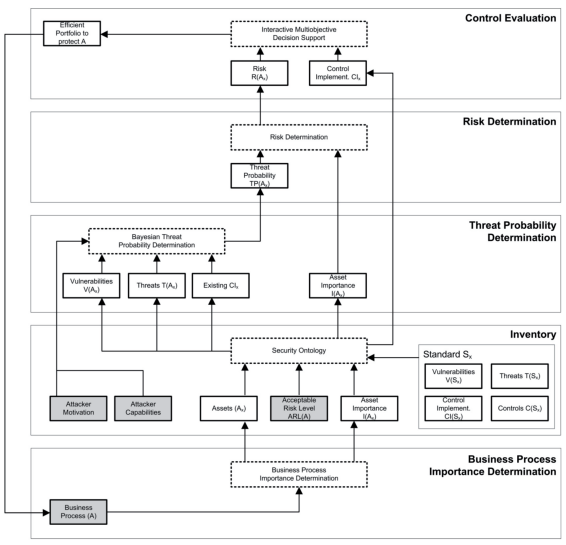


Figure 1: AURUM methodology

- Using a novel information security ontology to provide best practice knowledge regarding threats, vulnerabilities, controls, potential control implementations, and asset classes

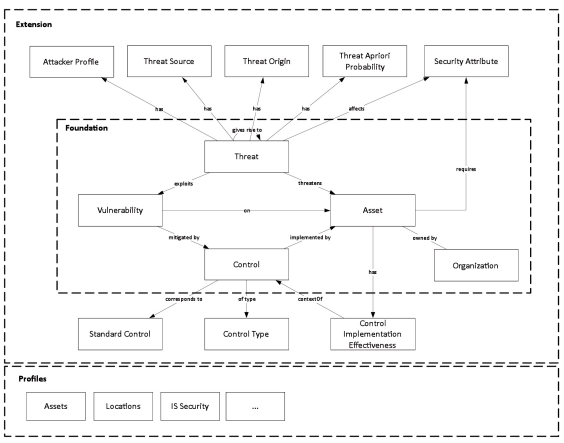


Figure 2: Security Ontology

- Automatically calculating the importance of business-critical assets based on their involvement in business processes and the overall importance of these processes

- Automatically determining threat probabilities based on the organization-specific threat environment and existing control implementations

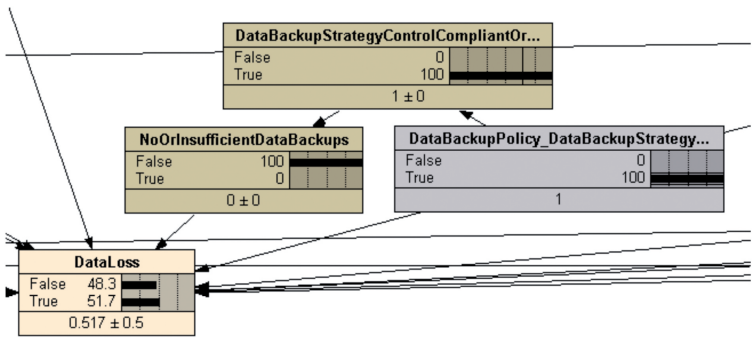


Figure 3: Bayesian Threat Probability Determination

- Using reasoning engines and the ontology to automatically determine potential control implementations that can be used to fill identified gaps
- Providing novel multi-objective decision support methods to interactively select control implementation portfolios based on existing control implementations

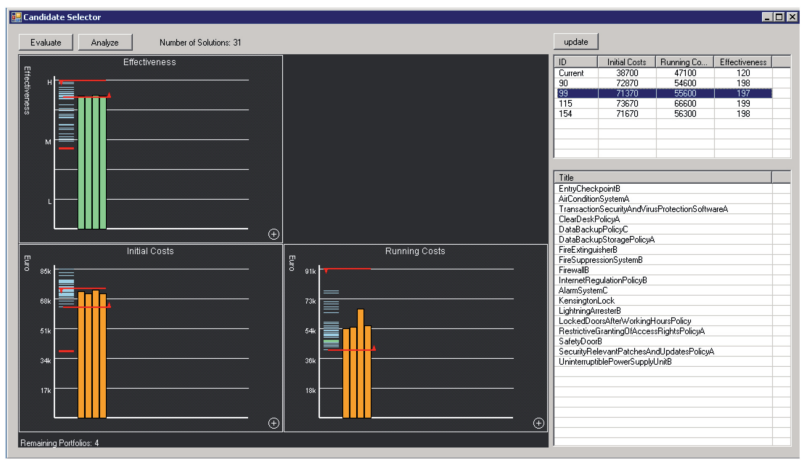


Figure 4: Interactive Decision Support

Benefits

(1) the ontological information security knowledge base ensures that the information security knowledge is provided to the risk manager in a consistent and comprehensive way,

(2) the incorporation of existing best practice guidelines and information security standards ensures that only widely accepted information security knowledge is used for threat/vulnerability identification and control recommendations,

(3) the proposed Bayesian threat probability determination ensures that the threat probability determination has a more objective basis than existing approaches,

(4) controls to reduce risks to an acceptable level are offered automatically,

(5) the use of interactive decision support allows to investigate various scenarios and, as a result, to learn more about the characteristics of the underlying problem, while the system guarantees that only an efficient solution can be selected, and

(6) by considering multiple objectives and providing gap analysis we support decision makers in getting a much better understanding of the problem in terms of what can be achieved in some objectives at what "price" in terms of opportunity costs in other objectives.

S. Fenz, A. Ekelhart, T. Neubauer: "Information Security Risk Management: In which security solutions is it worth investing?" in Communications of the Association for Information Systems, Vol. 28/1, 2011.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Interdependency Modeling Tools and Simulation-Based Risk Assessment of ICT Critical Infrastructures Contingency Plans

Peter Kieseberg and Lorenz Zechner

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org
FWF Der Wissenschaftsfonds.

Project Overview

Interdependencies among critical infrastructures, both inside the ICT domain and between ICT and other sectors, are complex to understand. Typically, European critical infrastructures have good contingency plans, but these are often not evaluated in complex scenarios and dependencies with contingency plans of other critical infrastructures are not always taken into account. The aim of INMOTOS is to define and develop a methodology and tools for a simulation-based risk assessment of contingency plans for critical infrastructures.

Key Targets

- Definition of a risk assessment methodology for critical infrastructure contingency plans and their interdependencies based on simulation
- Development of tools for critical infrastructure interdependencies and contingency plans modeling, simulation and risk evaluation
- Analysis, validation and optimization of contingency plans in complex scenarios including interdependencies

Project Characteristics

Project Details

- **Research program: FP7/CIP**
- **Volume: 1,598,980€ costs / 1,119,270€ granted**
- **Duration: 01.12.2010 - 30.11.2012 (24 months)**

The Consortium

- **D' Appolonia S.p.A. (Consortium Leader) (Italy)**
- **Consiglio Nazionale delle Ricerche (Italy)**
- **ITTI (Poland)**
- **AmanziTel AB (Sweden)**
- **Research and Education Laboratory in Information Technologies (Greece)**
- **SBA Research (Austria)**

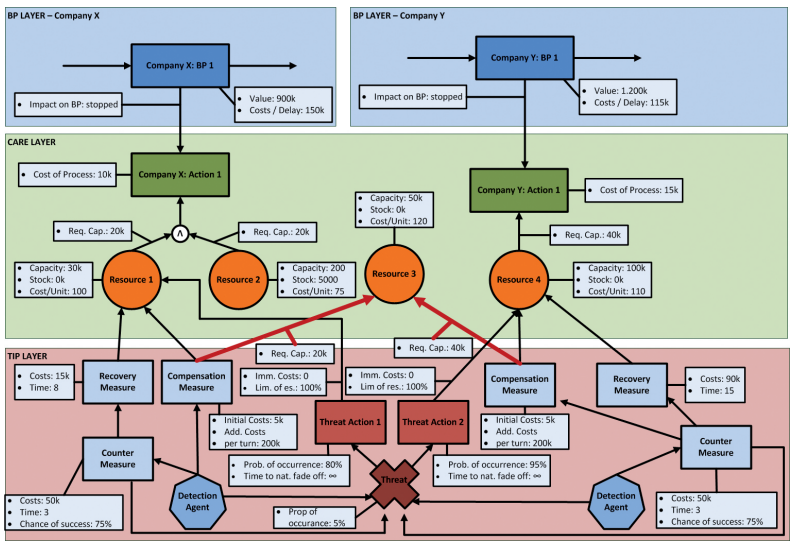
The Methodology

Developments by SBA Research

- SBA Research is the lead partner concerning the development of the methodology.
- The INMOTOS methodology is based on the ROPE methodology developed by SBA Research during the first K-Ind phase.

Enhancements Developed by SBA Research

- Addition of compensation and recovery measures to cover more complex scenarios
- Inclusion of several risk assessment types that can be evaluated together



Tool Development

Key Characteristics of the Tool

- Modeling of the methodology as colored Petri nets
- Search engine is based on the novel Neo4J graph-based database
- Easy-to-use configuration interface
- Targeted towards high performance in complex scenarios

Contribution by SBA Research

- Contribution in the realm of user interface design
- Adaptation of the abstract methodology to a form usable by colored Petri nets
- Contribution in the adaptation of the ICT scenario for testing purposes

Analysis and Validation of Existing Contingency Plans

Scenario in the ICT Sector

- Scenario is concerned with stations for measuring air radiation.
- Target: Modeling and simulation of the contingency plans that coordinate the application of alternative measuring equipment

Scenario in the Oil & Gas Industry

- Scenario deals with an international pipeline for gas.
- Target: Modeling and simulation of the contingency plans triggered in the case of failures

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Model-Driven Specification of Access Control Constraints in Process-Aware Information Systems

Sigrid Schefer-Wenzl and Mark Strembeck

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org
WU Wirtschaftsuniversität Wien Vienna University of Economics and Business

Problem & Motivation

Integrated modeling of access control concepts and business processes

- Improvement of business processes - number one priority of CIOs [Gartner CIO Studies, 2005-2011]
- Compliance requirements arise from, e.g., SOX, HIPPA, or Basel II/III
- The definition, monitoring, and enforcement of security concerns is highly important for organizations

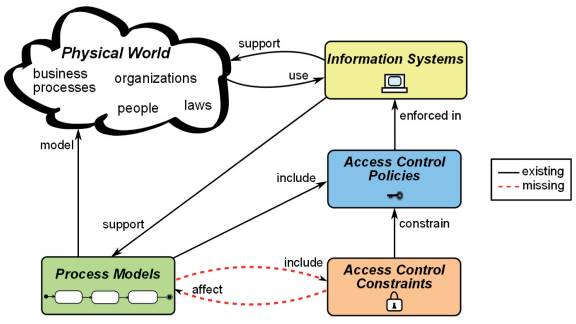


Figure 1: Conceptual overview

Access Control Constraints

Support for access control constraints at the business process level

- Different types of access control constraints that affect task execution should be considered in business process models
- Fine-grained customization of access control policies to organization-specific requirements
- Consideration of contextual information (e.g., time, location, task history)

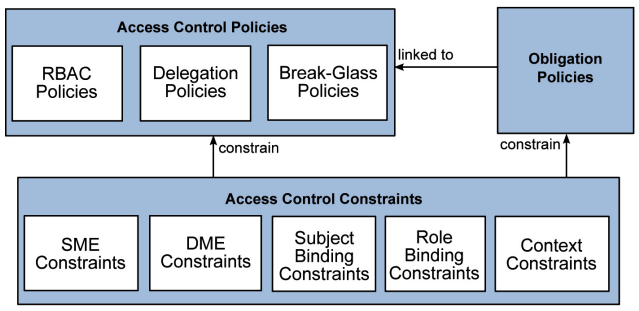


Figure 2: Interrelations between policies and access control constraints

Example

- CIM and corresponding UML extensions to model access control constraints in a business process context
- Satisfiability and consistency checks (conflict detection and resolution)

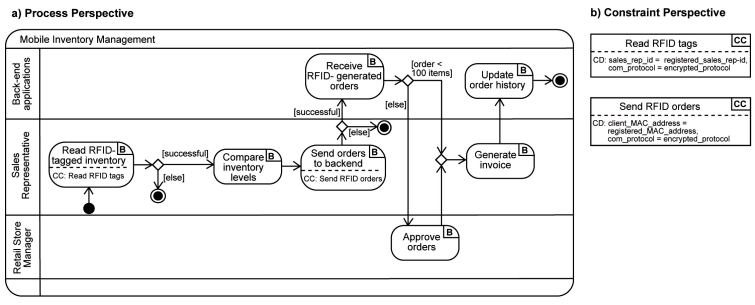


Figure 5: Mobile inventory management process including context constraints

Approach

Model-driven development approach

- Formal definitions and metamodels (computation-independent models (CIM))
- Domain-specific modeling support (platform-independent models (PIM))
- Executable models (platform-specific models (PSM)

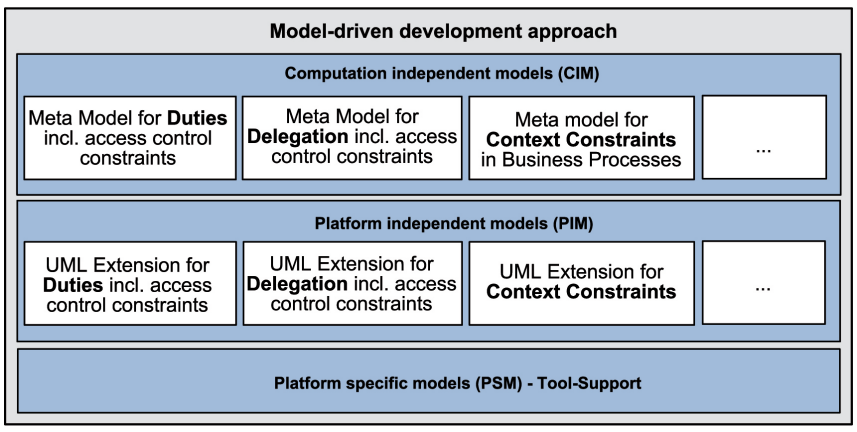


Figure 3: Model-driven development approach

$$
\begin{aligned}
&btown(r) = \bigcup_{r_{inh} \in rh^*(r)} bbr(r_{inh}) \cup bbr(r) \\
&rown(s) = \bigcup_{r \in rsa(s)} rh^*(r) \cup rsa(s) \\
&\forall t_T \in T_T : town^{-1}(t_T) \cap btown^{-1}(t_T) = \emptyset \\
&\forall t_T \in T_T, r \in R \text{ with } t_T \in bbr(r) : rown^{-1}(r) \cap bbs^{-1}(t_T) = \emptyset \\
&\forall t_2 \in sb(t_1) : t_1 \neq t_2 \text{ and } \forall t_2 \in rb(t_1) : t_1 \neq t_2
\end{aligned}
$$

Figure 4: Formal definitions

References
S. Schefer-Wenzl, M. Strembeck: Modeling Context-Aware RBAC Models for Business Processes in Ubiquitous Computing Environments, International Conference on Mobile, Ubiquitous and Intelligent Computing (MUSIC), IEEE CPS, June 2012.
S. Schefer-Wenzl, M. Strembeck, A. Baumgrass: An Approach for Consistent Delegation in Process-Aware Information Systems, 15th International Conference on Business Information Systems (BIS), Springer LNBIP, Vol. 117, May 2012.
S. Schefer, M. Strembeck, J. Mendling, A. Baumgrass: Detecting and Resolving Conflicts of Mutual-Exclusion and Binding Constraints in a Business Process Context, In: Proc. of the 19th International Conference on Cooperative Information Systems (CoopIS), Springer LNCS, Vol. 7044, October 2011.
S. Schefer, M. Strembeck, J. Mendling: Checking Satisfiability Aspects of Binding Constraints in a Business Process Context, In: Proc. of the Workshop on Workflow Security Audit and Certification (WFSAC), Springer LNBIP, Vol. 100, August 2011.
S. Schefer: Consistency Checks for Duties in Extended UML2 Activity Models, In: Proc. International Workshop on Security Aspects in Process-Aware Information Systems, of the 6th International Conference on Availability, Reliability and Security (ARES), IEEE CPS, August 2011.
S. Schefer, M. Strembeck: Modeling Support for Delegating Roles, Tasks, and Duties in a Process-Related RBAC Context, In: Proc. of the International Workshop on Information Systems Security Engineering (WISSE), Springer LNBIP, Vol. 83, June 2011.
M. Strembeck and J. Mendling: Modeling Process-related RBAC Models with Extended UML Activity Models. In: Information and Software Technology (IST), Vol. 53, No. 5, May 2011
S. Schefer, M. Strembeck: Modeling Process-Related Duties with Extended UML Activity and Interaction Diagrams, In: Electronic Communications of the EASST: Kommunikation in verteilten Systemen, Vol. 37, March 2011.

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwfj Bundesministerium für Wirtschaft, Familie und Jugend
FFG
wirtschaftsagentur wien zit Die Technologieagentur der Stadt Wien
Christian Doppler Forschungsgesellschaft
FWF Der Wissenschaftsfonds.
Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Moses^3: Multi-Objective Decision Support for Efficient Information Security Safeguard Selection

Andreas Ekelhart, Stefan Fenz, Elmar Kiesling, Christine Strauß and Christian Stummer

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

FWF Der Wissenschaftsfonds.

Supported by Austrian Science Fund (FWF): P 23122-N23

Research Problem

Moses^3 tackles the highly relevant and theoretically challenging problem of strategically selecting an appropriate portfolio (i.e., bundle) of information security safeguards while considering that optimal investment in security is dependent upon:

(i) characteristics of the system and assets to be protected

(ii) the "threat model"

(iii) available resources

(iv) decision-makers' risk preferences

Challenges

- Security investments require trade-offs between monetary and non-monetary risk, cost, and benefit objectives
- A system's overall security depends on the joint effect of all implemented safeguards; this effect is generally not cumulative
- Actions of malicious and goal-driven threat agents do not follow particular statistical patterns
- Threat agents differ in their motivation, objectives, resources, risk tolerance, points of entry, etc.
- The best way to defend a system always depends on the question "against whom?"

Solution Approach

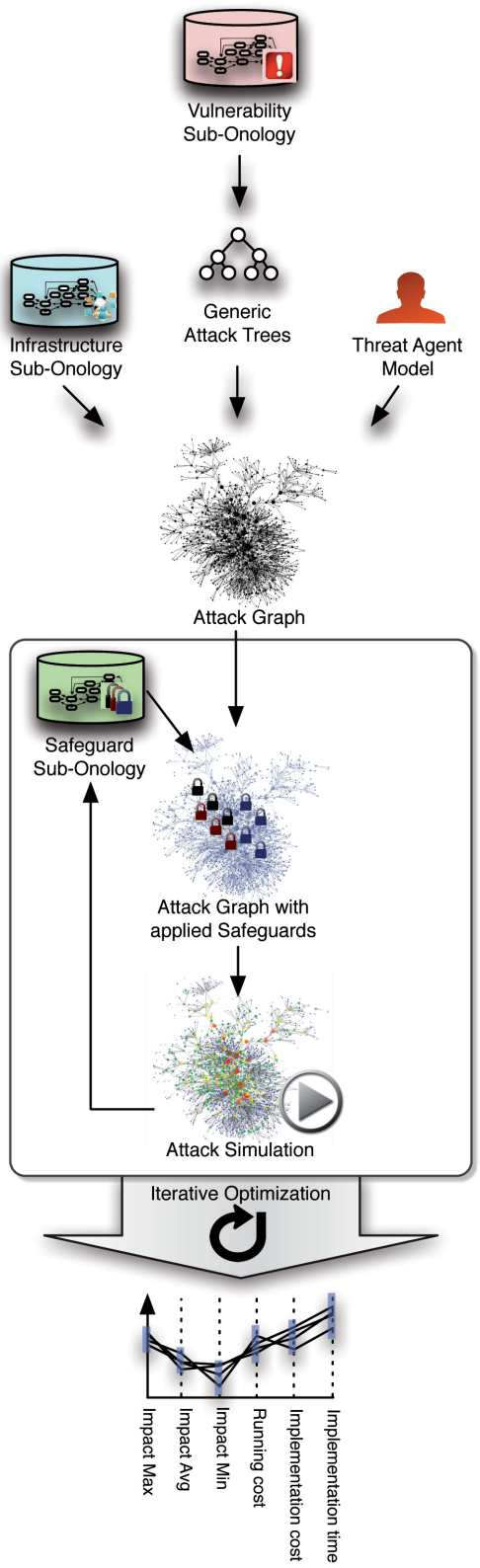


Figure 1: Model overview

Methodologies

1. Ontological modeling of security knowledge
2. Dynamic attack tree and attack graph generation techniques
3. Attack simulation based on probabilistic model of threat agent behavior
4. Meta-heuristic identification of efficient safeguard portfolios
5. Interactive decision support to balance multiple objectives

Conceptual Model

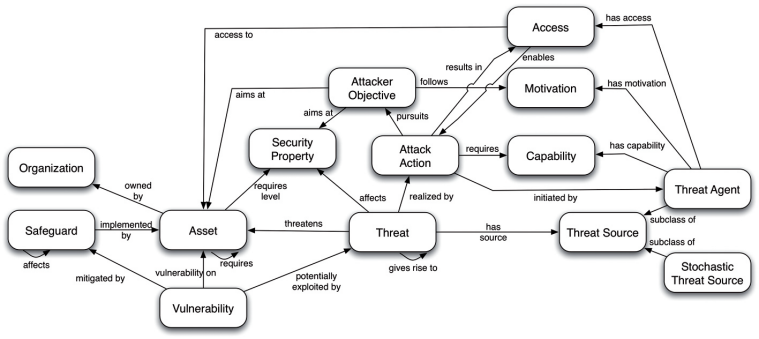


Figure 2: Ontology

Attack Trees and Attack Graphs

- Attack trees capture generic causal structure of possible attack actions
- Attack graphs capture possible routes of attacks in a particular context (infrastructure, environment) and for a particular threat agent
- In both attack graphs and trees, actions are linked dynamically through pre- and postconditions
- Attack trees and attack graphs can be queried from ontologies

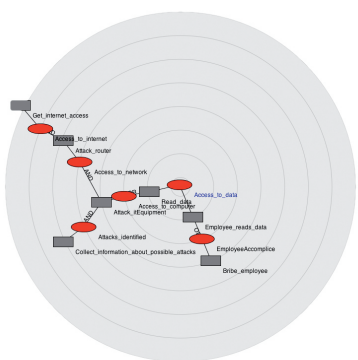


Figure 3: Example attack tree

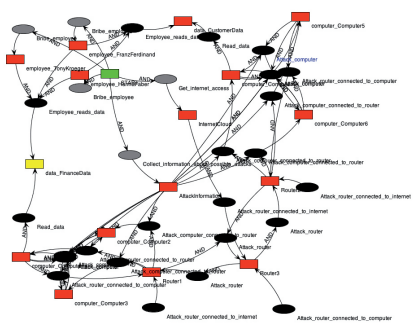


Figure 4: Example attack graph

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Towards Cloud-Centric Service Environments

Andreas Mladenow, Natalia Kryvinska, Christine Strauß

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

Value Drivers Using Clouds

Analysis for Start-Ups and Small and Medium-Sized Enterprises in the Textile and Apparel Industry

Cloud computing has evolved and is expected to grow further into an enormously booming market segment, especially for start-ups and SMEs, as they can benefit from the concept of "Anything as a Service" (XaaS) without the need to invest significant financial resources in IT capabilities. Through usage-based models, seemingly infinite resources based on rapid elasticity, multi-user systems, and the ability to access the network anytime and anywhere, organizations can achieve increased cost-effectiveness and efficiency in their business operations.

This paper discusses, with a particular emphasis on start-ups and SMEs in the B2B and B2C markets, how e-business value creation drivers such as novelty, efficiency, complementarities and lock-in can leverage and enhance business value in practice. Using the example of the textile and apparel industry, this paper pinpoints how cloud computing can foster an environment in which new opportunities can blossom and added value is created for both businesses and consumers through modern marketing and networking technologies using an inclusive social and technological environment.

Opportunities in Clouds	*Main value driver in terms of…*	*Challenges in Clouds*
Improved, simplified access to resources Global accessibility/availability Most actual software available (SaaS) via Updates without any additional fees (access to resources)	Accessibility	Data transfer (supply) shortfall Dependency on Internet access
Enhanced protection due to professional cloud-provider Spread the risk Potential savings (upfront and ongoing) Improved flexibility for all parties High scalability in terms of processing power and storage capacity à efficient resource allocation	Capability	Security risk by outsourcing data (e.g., loss of control, confidentiality) Vulnerability due to many relations between supplier and other stakeholders of the Cloud Potential restructuring-difficulties of Web applications
Variable, usage-based billing (based on measured service)	Measurability	Unpredictable and lacking Performance
Focus on core competencies by outsourcing ancillary activities	Network externalities	Dependency on provider (Vendor Lock-in)

Table 1: Discussed Opportunities and Challenges in Clouds

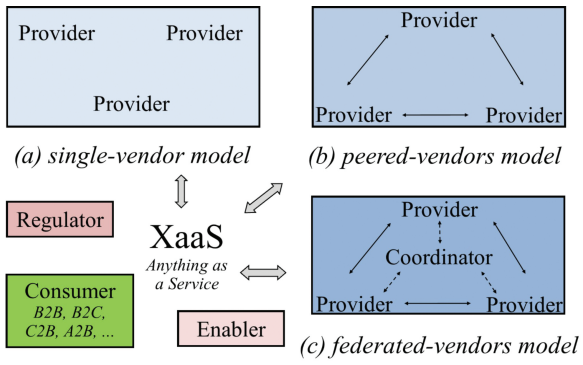


Figure 1: Stakeholders in Cloud-Centric Service Environments

Value Creation for…	*Businesses (B2B)*	*Businesses (B2C)*	*Consumers (B2C)*
Benefits derive from…	… collaborative activities & new opportunities	…consumer Input	…offering new Services to the consumer
Practical impacts of benefits	• Increased efficiency due to better information symmetries • Participative solutions on cloud communities/ platforms • Cloud based PLA/ ERP systems • Use-what-you-need and pay-what-you-use business models • On-demand availability	• Providing a more complex Customer Relationship Management (CRM) • Distribution of content for buyers • Hosting Platforms for B2C and C2C communications • Offering mass customization according to personal preferences	• Increasing consumer feedback • Analyzing public opinions and trends to obtain information concerning consumer preferences • Acquiring innovations designed by the consumer, attracting lead users • Using information to set appropriate business measures

Table 2: Value Creation in Cloud-Centric Service Environments

Conclusion and Limitations

Our approach revealed significant advantages that cloud computing/ cloud-systems offer to Start-Ups and SMEs driving profitability due to enhancements in capability, accessibility, measurability, demand and trend management, as well as network effects. A number of highly interdependent factors in cloud platforms generate value creation opportunities in the textile and apparel industry. For example, efficient transactions can be carried out through novel business models; lock-in and other effects are possible due to better and faster information at the disposal of platform participants. SMEs and Start-Ups may act successfully in competitive supply chains due to quickly established and low-cost information symmetries, which in turn enable dynamic and strategic partnerships. Although there are several advantages to cloud computing and its expected benefits to businesses, IT enterprise control will remain a significant weakness as a 3rd party control exists. The case study on the textile and apparel industry could be used as a starting point to perform similar analyses on (selected) other sectors. Potential findings could influence worldwide federated cloud models, but more importantly, it could provide a basis for the development of sector-specific tool-sets and/or decision support systems fostering cloud-centric service environments.

Anjomshoaa A, Tjoa A (2011) How the Cloud Computing Paradigm Could Shape the Future of Enterprise Information Processing", The 13th International Conference on Information Integration and Web-based Applications&Services (iiWAS2011), Ho Chi Minh City, Vietnam, 05.12.2011 - 07.12.2011; in: Proceedings of the13th International Conference on Information Integration and Web-based Applications&Services (iiWAS2011).
Armbrust M., Fox A., Griffith R., Joseph AD., Katz RH., Konwinski A., Lee G., Patterson DA., Rabkin A., Stoica I. and Zaharia M. (2009) Above the clouds: a Berkeley view on cloud computing, UC Berkeley Reliable Adaptive Distributed Systems Laboratory, Technical Report No. UCB/EECS-2009-28.
Amit R, Zott C (2001) Value creation in e-business, Strategic Management Journal, vol. 22, pp. 493-520.
Buyya R, Ranjan R, Calheiros RN (2010) InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services, LNCS Springer, vol. 6081, pp. 13-31.
Damodaram AK, Ravindranath K (2010) Cloud Computing for Managing Apparel and Garment Supply Chains – an Empirical study of Implementation Frame Work, Int. J. Computer Science Issues, vol. 7(6), pp. 325-336.
Dimitrakos T (2009) Common Capabilities for Service Oriented Infrastructures – Grid and Cloud Computing, in: Grid and Cloud Computing: A Business Perspective on Technology and Applications, K. Stanoevska-Slabeva, Eds. Berlin: Springer, pp. 123-145.
Gantz, John F./Minton, Stephen/Toncheva, Anna (2012): Cloud Computing's Role in Job Creation, IDC.
Kumar J, Vernon, Kumar S (2011) Ther economic perspective of cloud computing. International Journal of Advances in Computer Networks and its Security, pp. 145-152.
Ma B, Zhang KJ (2009) Research of Apparel Supply Chain Management Service Platform, Proc. IEEE Int. Conf. on Manage¬ment and Service Science (MASS 09), IEEE Press, pp. 1-4.
Marston S, Li Z, Bandyopadhyay S, Ghalsasi A (2011) Cloud Computing – The business perspective, Decision Support Systems, vol. 51, Dec. 2011, pp. 176-189.
Mell P,Grance T (2011) The NIST definition of Cloud Computing, Nat. Inst. of Standards and Technology, Spec. Pub. 800-145.
Moch R, Merkel A, Günther L, Müller E (2011) The Dimension of Innovation in SME Networks – a case study on Cloud Computing and Web 2.0 Technologies in a Textile Manufacturing Network, Int. J. of Innovat. and Sustainable Development, vol. 5(2/3), pp.185-198.
Wang C, Wang Q, Ren K, Lou W (2010) Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. Proc. IEEE INFOCOM '10, March 2010.
Wen YG, Shi GY, Wang GQ (2011) Designing an Inter-Cloud Messaging Protocol for Content Distribution as a Service (CoDaas) over Future Internet. 6th Int. Conf. on Future Internet Technologies (CFI'11) Seoul, Korea, June 2011.
Zhang KJ, Ma B, Dong PJ, Tang BY, Cai H (2010) Research on Producer Service Innovation in Home-Textile Industrial Cluster Based on Cloud Computing Platform," Proc. IEEE Int. Conf. on Service Operations and Logistics and Informatics (SOLI 10), IEEE Press, pp. 155-160.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Verification, Validation, and Evaluation in Information Security Risk Management

Stefan Fenz and Andreas Ekelhart

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

Motivation and Problem

- **Over the last four decades, various information security risk management (ISRM) approaches have emerged.**
- **A lack of sound verification, validation, and evaluation methods for these approaches exists.**
- **While restrictions, such as the impossibility of measuring exact values for probabilities and follow-up costs, obviously exist, verification, validation, and evaluation of research is essential in any field, and ISRM is no exception.**

Goals

- **Survey of verification, validation and evaluation methods referenced in ISRM literature**
- **Discussion and recommendation in which ISRM phases the methods should be applied**

Information Security Risk Management phases

Generic ISRM phase and its output	CRAMM phase	NIST SP 800-30 phase	OCTAVE phase	EBIOS phase	ISO 27005 phase
System Characterization **Output: inventory list of assets to be protected, including their acceptable risk level**	Asset Identification	System Characterization	Identification of Critical Assets and Corresponding Security Requirements Identification of Current Security Practices	Study of the Organization Study of the Target System Determination of the Security Study Target Expression of Security Needs	Identification of Assets
Threat and Vulnerability Assessment **Output: list of threats and corresponding vulnerabilities endangering the identified assets**	Threat Assessment Vulnerability Assessment	Threat Identification Vulnerability Identification Control Analysis	Identification of Threats and Organizational Vulnerabilities Identification of Current Technology Vulnerabilities	Study of Threat Sources Study of Vulnerabilities Formalization of Threats	Identification of Threats Identification of Vulnerabilities
Risk Determination **Output: quantitative or qualitative risk figures/levels for identified threats (input: threat probability and magnitude of impact)**	Asset Valuation Risk Assessment	Likelihood Determination Impact Analysis Risk Determination	Risk Determination for Critical Assets	Comparison of Threats with Needs (Risk Determination)	Identification of Impact Assessment of Threat Likelihood Assessment of Vulnerability Likelihood Risk Estimation
Control Identification **Output: list of potential controls that can mitigate the risks to an acceptable level**	Countermeasure Selection	Control Recommendations	Identification of Risk Measures	Formalization of Security Objectives	Evaluation of Existing and Planned Controls
Control Evaluation and Implementation **Output: list of cost-efficient controls that have to be implemented to reduce the risk to an acceptable level**	Countermeasure Recommendation	Control Evaluation Cost/Benefit Analysis Control Selection Safeguard Implementation Plan Development Control Implementation	Protection Strategy Development Risk Mitigation Plan Development	Determination of Security Levels Determination of Security Requirements Determination of Security Assurance Requirements	Information Security Risk Treatment (Risk Avoidance, Risk Transfer, Risk Reduction, or Risk Retention)

Results

How to verify, validate, and evaluate information security risk management phases?

	System Characterization	*Threat and Vulnerability Assessment*	*Risk Determination*	*Control Identification*	*Control Evaluation and Implementation*
Verification					
Sensitivity Analysis			•		•
Internal Result Comparison	•	•	•	•	•
Simulation			•		
Validation					
Experts	•	•	•	•	•
Alternate Decision Process	•	•	•	•	•
Statistical Evidence			•		•
Evaluation					
Management Decision Behavior Analysis	*Both methods evaluate the influence of the overall ISRM activities on the considered organization.*				
Control Quality Assessment					

Figure 1: ISRM verification, validation, and evaluation framework

Implications for Research and Practice

- **Our review of existing ISRM literature revealed that there are no standardized methods for verification, validation, and evaluation of ISRM-related research.**
- **Verification of ISRM approaches can be conducted objectively with the introduced methods, while validation turned out to be of a rather interpretive nature.**
- **The evaluation methods listed and the defined criteria allow organizations to survey effects of introduced ISRM approaches.**
- **Depending on the focus of the ISRM research, specific ISRM phases can be targeted and researchers can select suitable verification, validation and evaluation methods as described by our research results.**
- **Practitioners have to establish trust in potential or already implemented ISRM approaches. This usually requires the verification and validation of all ISRM phases. While verification and validation should be conducted at the beginning of the process, evaluation should be continuous so as to determine the benefit of the implemented approach.**

S. Fenz, A. Ekelhart: "Verification, Validation, and Evaluation in Information Security Risk Management," in IEEE Security and Privacy, Vol.8, 2010.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Vulnerability Management Tool (VMT) & Vulnerability Notification Customer Platform (VNCP)

Gernot Goluch, Dusan Domany, Daniel Puchner and Lorenz Zechner

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

Facts

VMT
- Project start: 12.2009
- Project finished: 05.2011
- Retrieves advisories from 6 independent sources
- Aggregates sources and providing them to VNCP

VNCP
- Project start: 06.2011
- Project finished: -
- Receives information from VMT and provides them to end users
- Provides filters, notifications, monitoring and report functionalities

Goals

- **Automatic collection of security-relevant advisories from multiple sources**
- **Aggregation and processing of advisories**
- **Provision of aggregated advisories to end users by predefined filters**
- **End users use advisories to resolve/prevent security issues**

VMT

- **Automatic collection and persistence of security advisories from various resources**
  - Involves identification of new advisories, their retrieval, parsing, transformation into the common format, and insertion into the database
  - The advisories are in most cases available in the form of Web pages
- **Provides an integrated environment for the management of the collected security advisories**
  - Provides search capabilities based on various advisory attributes as well as keyword search
  - Helps to find related advisories based on the common references
  - Provides the user with a fully integrated workflow for the creation of new security advisories
- **Additional features**
  - Statistics about the collected and created advisories
  - Software product catalog, which can be used for coherent management of the affected software products

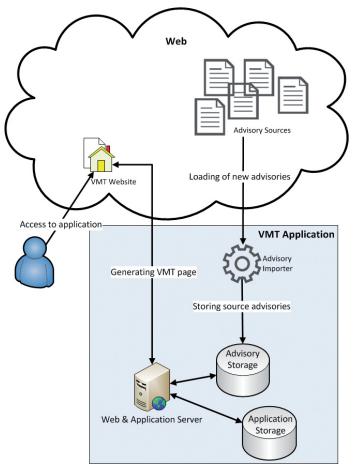


Figure 1: Structure of VMT

VNCP

- **The client-side application to VMT**
- **Regularly retrieves newly created advisories from the VMT application based on the software inventory registered by the customer**
- **Allows the users to browse through the retrieved advisories as well as search by various criteria**
- **Integrates an advanced form of advisory filtering**
  - Registration of assets and the installed software products
  - Creation of roles that can be attached to any number of assets and any number of users. A role can contain a number of user-defined filters that are based on various advisory attributes
  - The user can view the advisories that are related to him based on his associated role and the associated assets
  - The user gets notified about the incoming advisories that are related to him based on the role configuration
- **Additional features**
  - Management of the advisory status separately for each affected asset
  - Reporting services

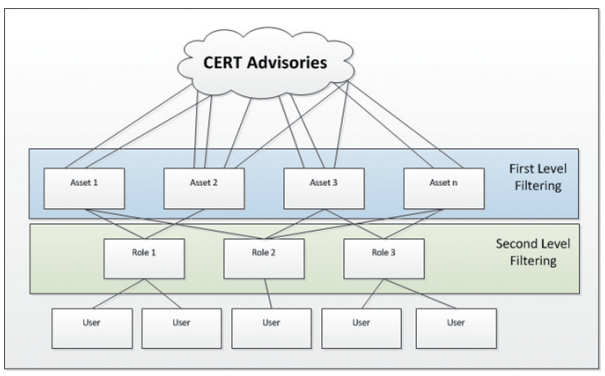


Figure 2: Structure of VNCP

Interactions between VMT and VNCP

VMT
- **Providing aggregated advisories**
- **Assignment of permissions for**
  - Products
  - End users

VNCP
- **Retrieval of products & advisories from VMT**
  - Flexible intervals
  - Dynamic detection and reloading of missed or faulty advisories
- **Authentication of end users in VNCP with settings from VMT**
- **Creation of filters on VNCP side**

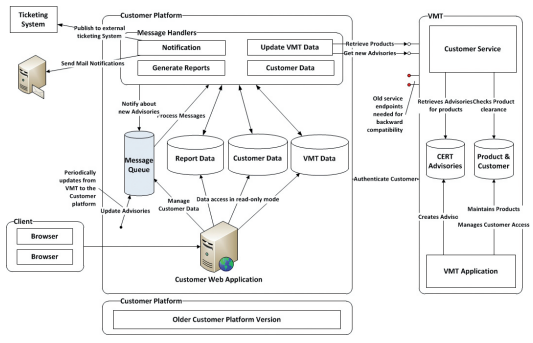


Figure 3: Interactions between VMT and VNCP

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Who is Who:

On Visualizing Organizational Models in Collaborative Systems

Simone Kriglstein, Jürgen Mangler, Stefanie Rinderle-Ma

COMET
Competence Centers for Excellent Technologies
www.ffg.at/comet

secure
sba-research.org

universität wien

Motivation

Organizational structures and, consequently, the organizational models describing them can become very complex, comprising up to thousands of involved entities and relations.
Visualization can help:

- to explore the structure of the organization
- users to build valuable knowledge, which supports them in their decisions

Two visualization approaches were developed (based on the data model depicted in Figure 1) in order to provide optimum support for users in consideration of their preferences and needs.

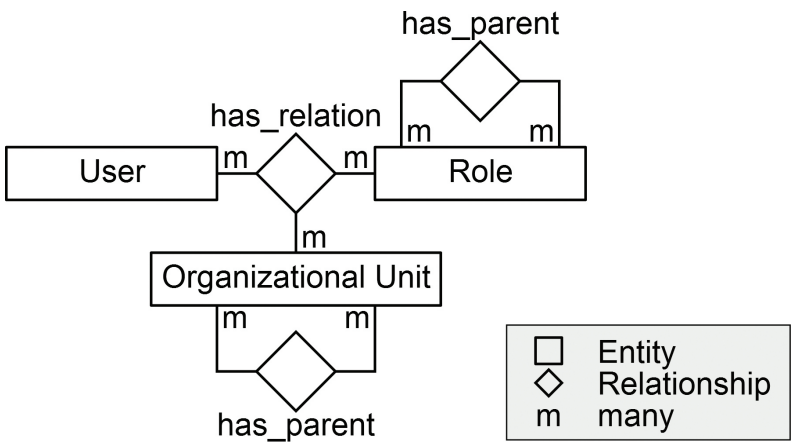


Figure 1: Data model for both visualization approaches.

User Study

The motivation was to detect misinterpretations or unclear elements and to get early feedback. Both approaches were tested with 13 experts.

Following methods are used:

- Observations in combination with thinking aloud:
  - During participants interact with the visualizations in order to fulfill different tasks
- Semi-structured interview
  - Participants were asked about:
    - which visualization approach they preferred with regard to aesthetics and utility
    - the strengths and weaknesses of both visualizations
    - compare them with visualizations which they usually use to analyze the organizational structure

Results:

- The representation of users in an individual view was noted as a good solution
- OrbitFlower was considered more useful to get a first overview
- OrbitList was considered better for answering specific questions

Visualization Design

Color blue:
- Organizational unit nodes
- Relationships between organizational units

Color purple:
- Role nodes
- Relationships between roles

Thickness:
- Relationships between roles and organizational units correspond to the number of assigned users

Size & Color Intensity:
- depends on the number of users assigned to this node

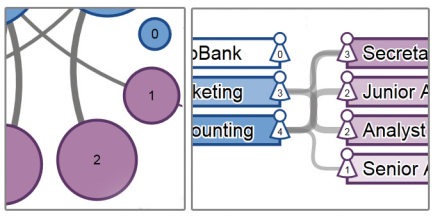


Figure 2: Example for size and color intensity.

OrbitFlower:

- Circular layout that locates nodes on the perimeter of a circle
- Compact shape allows handling a large number of nodes

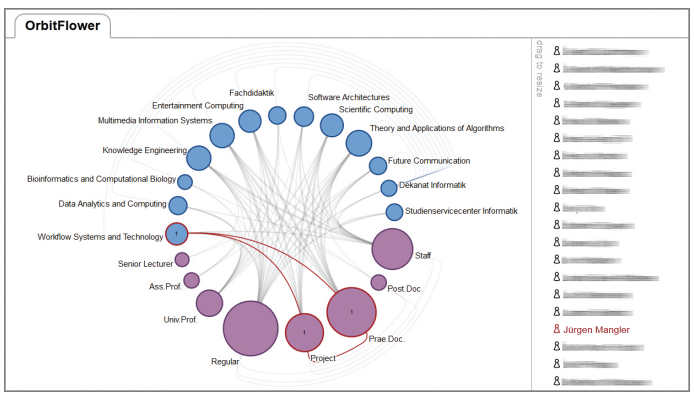


Figure 3: Example shows the assignment of the user "Jürgen Mangler" to his organizational unit and role.

OrbitList:

- Rectangular layout that arranges nodes parallel to the x- and y-axes
- Users generally complete tasks faster

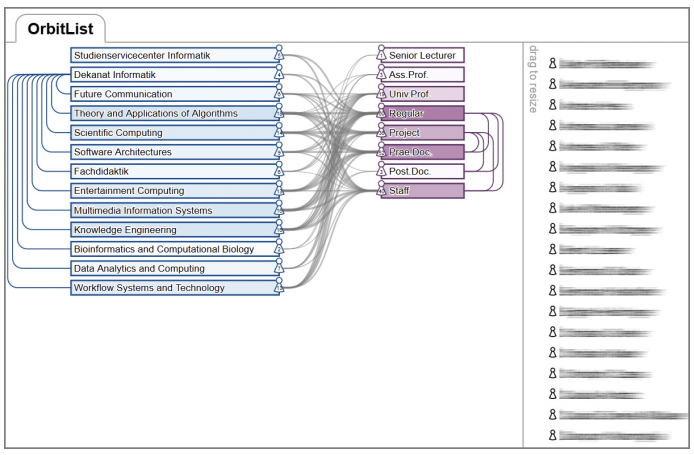


Figure 4: Example shows the relationships for the role "Regular".

Both visualizations show a list of users in a second view.

S. Kriglstein, J. Mangler, S. Rinderle-Ma: "Who is Who: On Visualizing Organizational Models in Collaborative Systems." in 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2012.

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwfj Bundesministerium für Wirtschaft, Familie und Jugend
FFG
wirtschaftsagentur wien zit Die Technologieagentur der Stadt Wien
Christian Doppler Forschungsgesellschaft
FWF Der Wissenschaftsfonds.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

25 Years of Software Obfuscation –
Can It Keep Pace with Progress in Code Analysis?

Sebastian Schrittwieser, Stefan Katzenbeisser, Johannes Kinder, Edgar Weippl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

Survey Motivation

- Code obfuscation has always been a highly controversially discussed research area
- While theoretical results indicate that provably secure obfuscation in general cannot be achieved, many application areas (e.g., malware, commercial software, etc.) show that code obfuscation is indeed employed in practice
- Still, it remains unclear to what extent today's code obfuscation state of the art can keep up with the progress in code analysis and where we stand in the arms race between attackers and defenders

Scenarios

- We present a novel classification of real-life attack scenarios in the context of code obfuscation, derived from a careful analysis of past security incidents involving obfuscated programs
- We first distinguish between various analysis techniques that an attacker is willing to employ during his attack; then we deal with different aims of an attacker.

Code analysis categories	Example
Pattern matching	Malware signatures
Automated static analysis	Heuristic malware detection
Automated dynamic analysis	Malware analysis in the labs of anti-virus vendors
Human-assisted analysis	Reverse engineering

Attacker's aims	Example
Finding the location of data (LD)	Extraction of licensing keys from binary
Finding the location of program functionality in the code (LC)	Finding the location of a copy protection mechanism
Extraction of code fragments (EC)	Extraction of code fragments for rebuilding verification routines for licensing keys
Understanding the program (UC)	Understand a proprietary cipher in order to start cryptanalysis attempts

Table 1: Code analysis categories and attacker's aims

- Combining these two concepts, we arrive at attack scenarios, which are analyzed in the context of various types of code obfuscation.
- As not all combinations are reasonable (e.g., pattern matching provides information on the code but cannot be used for extracting code), a total of 14 scenarios must be considered.

Results

	Patterns		Automated static				Automated dynamic				Human assisted			
Name	**LD**	**LC**	**LD**	**LC**	**EC**	**UC**	**LD**	**LC**	**EC**	**UC**	**LD**	**LC**	**EC**	**UC**
Data obfuscation														
Reordering data	■	▒	▒			▒								
Changing encodings	■	▒	■			▒								
Converting static data to procedures	■	▒	■			▒	▒				▒			
Static code rewriting														
Replacing instructions	■	▒				▒								
Opaque predicates	■	▒	▒	▒	▒	▒			▒	▒				
Inserting dead code	■	▒				▒								
Inserting irrelevant code	■	▒				▒								
Reordering	■	▒												
Loop transformations	■	▒	▒	▒	▒	▒			▒	▒				
Method splitting/recombination	■	▒				▒								
Aliasing	■	▒	▒	▒	■	▒			▒	▒				
Control flow flattening	■	▒	▒	▒	■	▒			▒	▒				
Parallelized code	■	▒	▒	▒	■	■			▒	▒				
Name scrambling	■	▒				■						▒	▒	▒
Removing standard library calls	■	▒	▒	▒	▒	▒			▒	▒		▒	▒	▒
Breaking relations	■	▒			▒	▒			▒	▒		▒	▒	▒
Dynamic code rewriting														
Packing/Encryption	■	▒	■	■	■	■		▒		▒				
Dynamic code modifications	■	■	■	■	■	■		▒	▒	▒				
Environmental requirements	■	■	■	■	■	■	▒	▒	▒	▒	▒	▒	▒	▒
Hardware-assisted code obfuscation	■	■	■	■	■	■	▒	▒	▒	▒	▒	▒	▒	▒
Virtualization	■	■	▒	▒	■	■		▒	▒	▒		▒	▒	▒
Anti-debugging techniques			▒	▒	■	■	■	■	■	■	▒	▒	▒	▒

Figure 1: Analysis of the strength of code obfuscation classes in different attack scenarios (LD = Locating Data, LC = Locating Code, EC = Extracting Code, UC = Understanding Code).

Conclusions

- While, at least in theory, completeness of code analysis seems possible (and most of the analysis approaches introduced in academia indeed work for small and specific examples), large real-world programs can be considered significantly harder to analyze.
- A major limiting factor for code analysis is that the high complexity of analysis problems often exceeds resource constrains available for the analyst, thus making it fail for complex programs.
- Therefore, very simple obfuscation techniques can still be quite effective against analysis techniques employing pattern matching or static analysis, which explains the unbroken popularity of obfuscation among malware writers.
- Dynamic analysis methods, in particular if assisted by a human analyst, are much harder to cope with; this makes code obfuscation for the purpose of intellectual property protection highly challenging.

bmvit Bundesministerium für Verkehr, Innovation und Technologie · bmwf Bundesministerium für Wirtschaft, Familie und Jugend · FFG · wirtschaftsagentur wien zit Die Technologieagentur der Stadt Wien · Christian Doppler Forschungsgesellschaft · FWF Der Wissenschaftsfonds.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Alliance Permanent Access to the Records of Science in Europe Network

Andreas Rauber

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

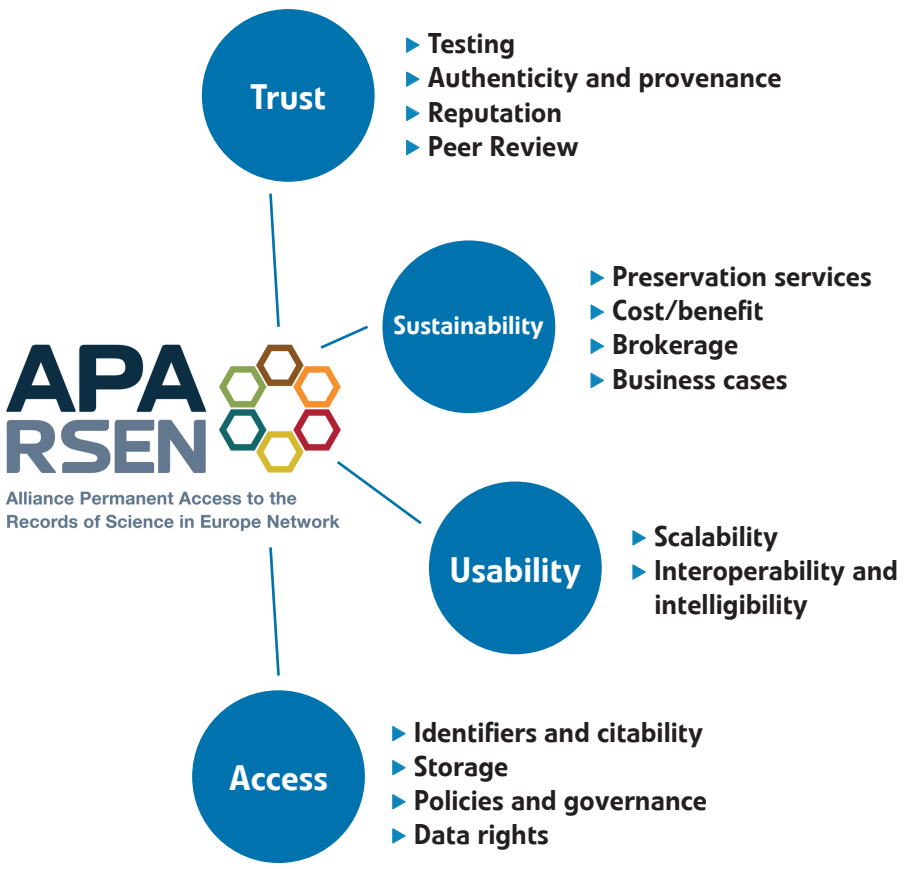
secure sba-research.org

APARSEN Alliance Permanent Access to the Records of Science in Europe Network

Motivation

Digital preservation (DP): Keeping digital resources accessible, understandable and easy to find. Technology advances rapidly and so does hardware, software, and file formats. DP tries to tackle the problems caused by hardware and software obsolescence by preserving the information for the long term.

Key Aspects



Goals

The Alliance Permanent Access to the Records of Science in Europe Network (APARSEN) project

- **was launched in January 2011**
- **aims to create a Virtual Centre of Excellence (VoE) for digital preservation in Europe**
  - no geographic boundaries
  - diverse teams
- **brings together leading commercial partners, academic researchers and libraries**
- **develops technical methods for ensuring long-term access to data and their reusability**
- **deals with legal and economic questions regarding the long-term preservation of data and the resulting costs, administrative overhead, and digital rights management of collected information**
- **raises awareness within and outside the consortium in order to establish new job profiles for data curators and data managers fulfilling formal qualification criteria in the area of digital preservation**
- **is funded under the European Community's Seventh Framework Programme FP7-ICT-2009-6-269977**

SBA Research Areas in APARSEN

- **Authenticity and provenance**
  - Identify and collect evidence to judge the completeness and wholeness of digital data
  - Record the history and evolution of digital objects
- **Secure logging mechanisms**
  - Monitor and log all archive activities and protect this information from intruders and attackers
  - Provide audit trails for fraud detection
- **Data quality and annotation**
  - Reproducible experiments and data reusability
  - Scientific Workflow Management Systems
- **Audit and certification or archives and repositories**
  - compliance with standards and trustworthy preservation of digital material
- **Coordination of common standards**
  - Identify and select common technology standards
  - Promote their use across domain boundaries
- **Training materials**
  - Develop and provide training materials
  - Dissemination activities

www.aparsen.eu

Network of Excellence

ACKNOWLEDGMENT
Part of this work is funded by the European Commission's Seventh Framework Programme (FP7/2007–2013) – ICT-2009.4.1: Digital Libraries and Digital Preservation – under grant agreement No 269977.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Automated Derivation and Comparison of Role Engineering Artifacts

Anne Baumgrass and Mark Strembeck

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org
WU Wirtschaftsuniversität Wien Vienna University of Economics and Business

Problem & Motivation

- Automation of monotonous and error-prone role engineering tasks
- Conformance checks of RBAC models
- Migration from current-state RBAC models (derived via mining techniques) to target-state RBAC models (specified via engineering techniques)

Approach

Method to support the migration and conformance checking of RBAC models via automated derivation and comparison of role engineering artifacts:

- Derivation of current-state RBAC models from process execution histories
- Derivation of target-state RBAC models from process models
- Derivation of a migration guide to migrate a current-state RBAC model to the corresponding target-state RBAC model
- Check if business process executions conform to RBAC models

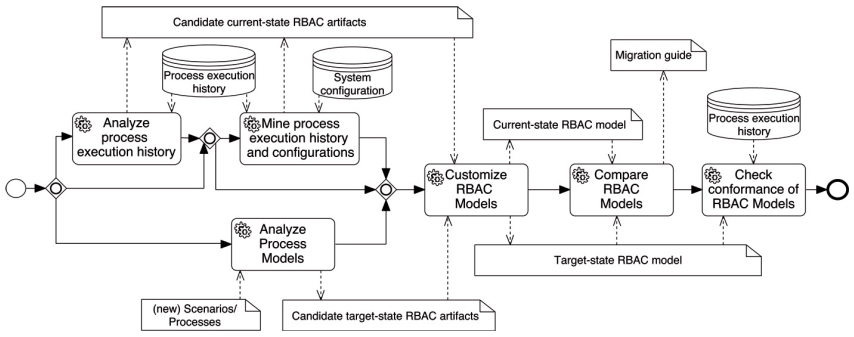


Figure 1: Approach overview: Derivation, comparison, and conformance checking of RBAC models

Derivation of Role Engineering Artifacts

Derive current-state RBAC models from process execution histories

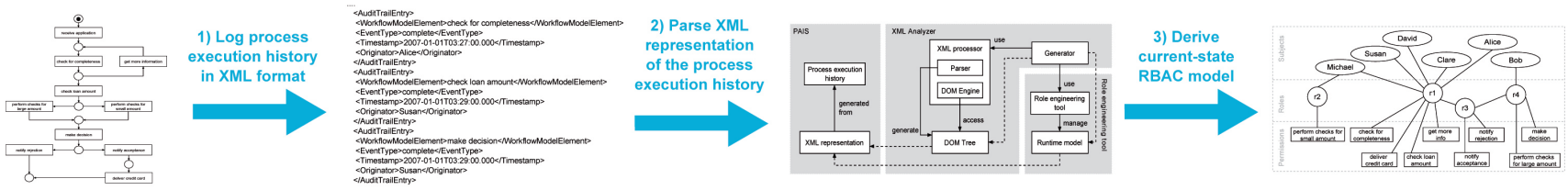


Figure 2: Deriving current-state RBAC models from process execution history

Derive target-state RBAC models from business process models

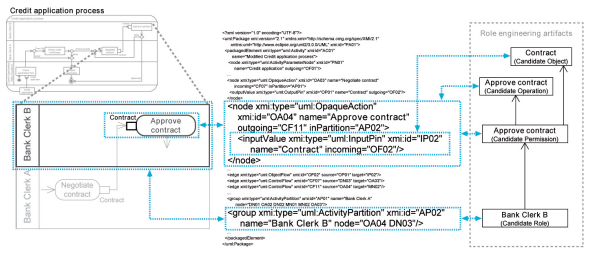


Figure 3: Example of the derivation of role engineering artifacts from UML activity models

Derivation of a Migration Guide

Apply model comparison techniques to identify differences

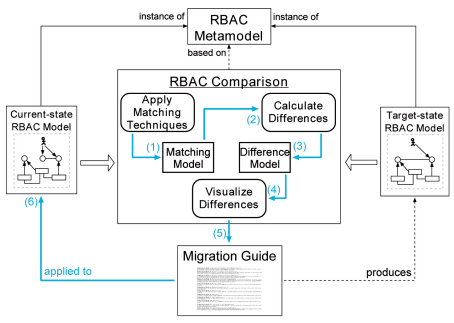


Figure 4: Approach overview: Derivation of migration rules

Conformance Checking of RBAC Models

Check conformance of RBAC Models with process execution history via LTL (Linear Temporal Logic)

- LTL templates define patterns for RBAC model properties
- Transform RBAC models to LTL statements via respective LTL templates
- Check conformance with process execution history

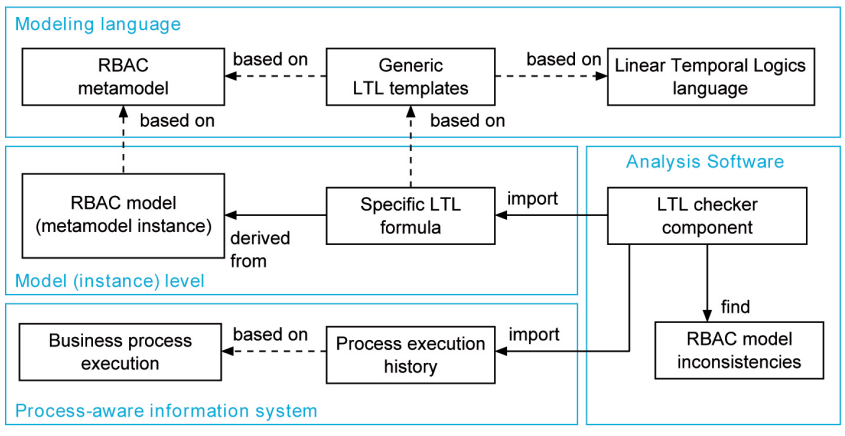


Figure 5: Conformance checking for RBAC models with business process execution via LTL

References

A. Baumgrass, M. Strembeck: An Approach to Bridge the Gap between Role Mining and Role Engineering via Migration Guides, In: Proc. of the 7th International Conference on Availabilty, Reliability and Security(ARES), IEEE CPS, August 2012

A. Baumgrass, S. Schefer-Wenzl, M. Strembeck: Deriving Process-Related RBAC Models from Process Execution Histories, In: Proc. of the 4th IEEE International Workshop on Security Aspects in Processes andServices Engineering (SAPSE), July 2012

S. Schefer-Wenzl, M. Strembeck, A. Baumgrass: An Approach for Consistent Delegation in Process-Aware Information Systems, 15th International Conference on Business Information Systems (BIS), Springer LNBIP, Vol. 117, May 2012.

S. Schefer, M. Strembeck, J. Mendling, A. Baumgrass: Detecting and Resolving Conflicts of Mutual-Exclusion and Binding Constraints in a Business Process Context, In: Proc. of the 19th International Conference on Cooperative Information Systems (CoopIS), Springer LNCS Vol. 7044, October 2011.

A. Baumgrass: Deriving current state RBAC models from event logs, In: Proc. of the International Workshop on Security Aspects of Process-aware Information Systems (SAPAIS), 6th International Conference on Availability, Reliability and Security (ARES), IEEE CPS, August 2011.

A. Baumgrass, M. Strembeck, S. Rinderle-Ma: Deriving Role Engineering Artifacts from Business Processes and Scenario Models, In: Proc. of 16th ACM Symposium on Access Control Models and Technologies (SACMAT), June 2011.

A. Baumgrass, T. Baier, J. Mendling, M. Strembeck: Conformance Checking of RBAC Policies in Process-Aware Information Systems. In: Proc. of the Workshop on Workflow Security Audit and Certification (WfSAC), Springer LNBIP, Vol. 100, August 2011.

M. Strembeck: Scenario-Driven Role Engineering, In: IEEE Security & Privacy, Vol. 8, No. 1, January/February 2010

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwfj Bundesministerium für Wirtschaft, Familie und Jugend
FFG
wirtschaftsagentur wien zit Die Technologieagentur der Stadt Wien
Christian Doppler Forschungsgesellschaft
FWF Der Wissenschaftsfonds.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Evaluating Design Decisions
for Security-related Domain-specific Modeling Languages

Bernhard Hoisl, Mark Strembeck

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

ModSec

WU Wirtschaftsuniversität Wien Vienna University of Economics and Business

Problem & Motivation

- Main issues for the specification and enforcement of process-level security properties:
  - no native language elements for security features in contemporary modeling languages
  - mapping problem: process modeling language different from system modeling language
  - lack of patterns, guidelines, best practices, etc. for specifying security properties in an MDD process

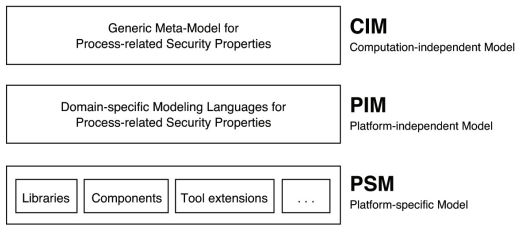


Figure 1: Modeling security properties at different abstraction layers

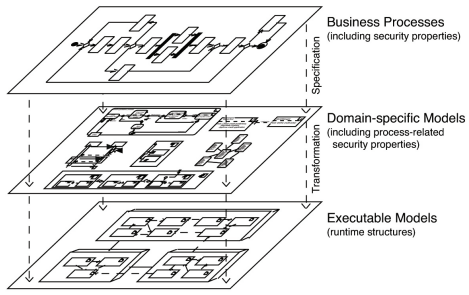


Figure 2: Specification and transformation of process-related security properties

MOF/UML-based Security Extensions

- UML is a de facto standard for software systems modeling
- We conducted 10+ security-related DSML projects based on the MOF/UML in recent years
- Our DSMLs allow to systematically integrate native security properties in UML models

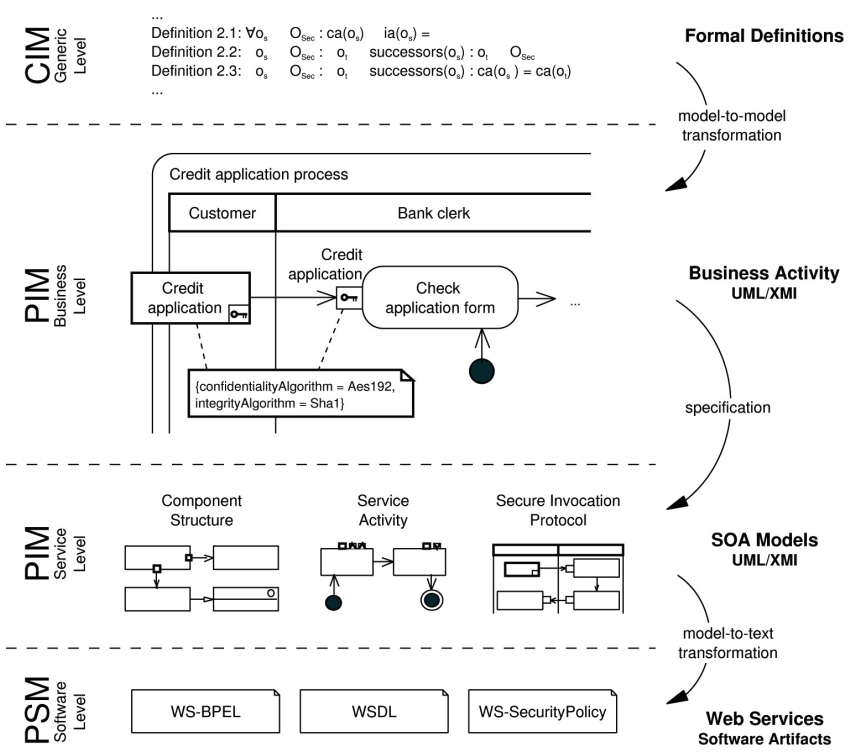


Figure 3: Example DSML: Secure Object Flows

Evaluating Design Decisions

- Systematic documentation of design decisions in a reusable manner via a catalog of structured decision descriptions and their inter-dependencies to guide the decision-making process
- Decision points and options of our own and related DSML projects allow an in-depth evaluation of the decision-making process
- Systematic literature review: evaluation of 2700+ related approaches

#	Decision/Option	P1	P2	P3	P4	P5	P6	P7	P8
D1	**Language model definition**								
O1.1	Textual descriptions	X	X	X	X	X	X	X	X
O1.2	Formal textual models	X	X	X			X	X	
O1.3	Informal diagrammatic models								
O1.4	Formal diagrammatic models	X	X	X			X	X	
D2	**Language model formalization**								
O2.1	M1 structural models								
O2.2	Profile (re-)definition		X				X		X
O2.3	Metamodel extension	X	X	X	X	X	X	X	X
O2.4	Metamodel modification		X					X	X
D3	**Language model constraints**								
O3.1	Explicit constraint expressions	X	X	X	X	X	X	X	X
O3.2	Code annotations								
O3.3	Constraining M2M/M2T transformations						X		
O3.4	Textual annotations	X	X	X	X	X	X	X	X
O3.5	None / Not specified								
D4	**Concrete syntax definition**								
O4.1	Model annotations		X				X		X
O4.2	Diagrammatic syntax extension	X	X	X	X			X	X
O4.3	Mixed syntax (foreign syntax)								
O4.4	Frontend-syntax extension (hybrid syntax)								
O4.5	Alternative syntax								X
O4.6	Reusing diagram symbols		X				X		X
O4.7	None / Not specified					X			
D5	**Behavior specification**								
O5.1	M1 behavioral models		X						
O5.2	Formal textual specification								
O5.3	Informal textual specification		X						
O5.4	Constraining model execution								
O5.5	None / Not specified	X		X	X	X	X	X	X
D6	**Platform integration**								
O6.1	Intermediate model representation	X					X		
O6.2	Generation templates								
O6.3	API-based generators						X		
O6.4	(Direct) model execution	X							
O6.5	M2M transformation								
O6.6	None / Not specified		X	X	X	X		X	X

Table 1: Decision points and options of DSML projects (excerpt)

Future Work

- Extract decision sequences to find patterns of common design paths for security-related DSMLs
- Investigate transferability of findings to non-MOF/UML-based DSMLs

P1: Mark Strembeck and Jan Mendling. Modeling Process-related RBAC Models with Extended UML Activity Models. In: Information and Software Technology, 53(5), 2010.
P2: Sigrid Schefer and Mark Strembeck. Modeling Process-Related Duties with Extended UML Activity and Interaction Diagrams. In Proc. of the International Workshop on Flexible Workflows in Distributed Systems, 2011.
P2, P3: Sigrid Schefer-Wenzl and Mark Strembeck. An Approach for Consistent Delegation in Process-Aware Information Systems. In Proc. of the 15th International Conference on Business Information Systems (BIS), Springer LNBIP, Vol. 117, 2012.
P3: Sigrid Schefer and Mark Strembeck. Modeling Support for Delegating Roles, Tasks, and Duties in a Process-Related RBAC Context. In Proc. of the International Workshop on Information Systems Security Engineering (WISSE). Springer LNBIP, Vol. 83., 2011.
P4: Bernhard Hoisl and Mark Strembeck. Modeling Support for Confidentiality and Integrity of Object Flows in Activity Models. In Proc. of the 14th International Conference on Business Information Systems (BIS). Springer LNBIP, Vol. 87, 2011.
P5: Sigrid Schefer. Consistency Checks for Duties in Extended UML2 Activity Models. In Proc. of the International Workshop on Security Aspects of Process-aware Information Systems (SAPAIS). IEEE, 2011.
P6: Bernhard Hoisl and Stefan Sobernig. Integrity and Confidentiality Annotations for Service Interfaces in SoaML Models. In Proc. of the International Workshop on Security Aspects of Process-aware Information Systems (SAPAIS). IEEE, 2011.
P6: Bernhard Hoisl, Stefan Sobernig, and Mark Strembeck. Modeling and Enforcing Secure Object Flows in Process-driven SOAs: An Integrated Model-driven Approach. In: Software and Systems Modeling, DOI 10.1007/s10270-012-0263-y, 2013.
P7: Sigrid Schefer-Wenzl and Mark Strembeck. Modeling Context-Aware RBAC Models for Business Processes in Ubiquitous Computing Environments. In Proc. of the 3rd International Conference on Mobile, Ubiquitous and Intelligent Computing, IEEE, 2012.
P8: Bernhard Hoisl and Mark Strembeck. A UML Extension for the Model-driven Specification of Audit Rules. In Proc. of the 2nd International Workshop on Information Systems Security Engineering (WISSE). Springer LNBIP, Vol. 112, 2012.
Bernhard Hoisl, Stefan Sobernig, Sigrid Schefer-Wenzl, Mark Strembeck, and Anne Baumgrass. Design Decisions for UML and MOF based Domain-specific Language Models: Some Lessons Learned. In Proc. of the 2nd Workshop on Process-based approaches for Model-Driven Engineering (PMDE), 2012.

More information is available at http://nm.wu.ac.at/modsec and http://nm.wu.ac.at/home/mark/BusinessActivities/.

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwfj Bundesministerium für Wirtschaft, Familie und Jugend
FFG
wirtschaftsagentur wien zit Die Technologieagentur der Stadt Wien
Christian Doppler Forschungsgesellschaft
FWF Der Wissenschaftsfonds.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Integrated Model-driven Security: From Business Processes to Software Services

Bernhard Hoisl and Mark Strembeck

Competence Centers for Excellent Technologies
www.ffg.at/comet

Problem & Motivation

- **Specification and enforcement of process-level security properties**
- **Main problems:**
  - no native language constructs to model security features in current modeling languages
  - process modeling language different from system modeling language → mapping problem

Systematic Approach

- **CIM: Generic metamodels for process-related security properties**
- **PIM: Domain-specific modeling languages (DSMLs) for process-related security properties**
- **PSM: Enforcement of DSML specifications in software systems**
- **Transformations: CIM-to-PIM mapping (model-to-model) and PIM-to-PSM mapping (model-to-text)**

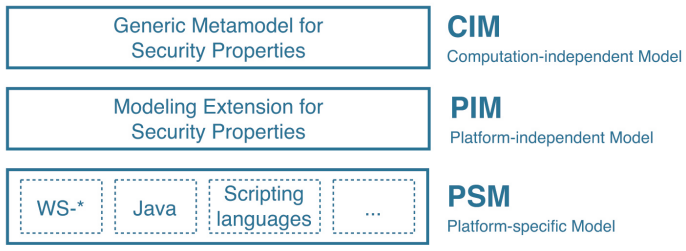


Figure 1: The approach supports all MDD layers

...
Definition 3.2: $\forall t_2 \in dme(t_1)$, $pi \in P_I$: $\forall t_x \in ti(t_2, pi)$, $t_y \in ti(t_1, pi)$: $es(t_x) \cap es(t_y) = \emptyset$
Definition 3.3: $\forall t_2 \in rb(t_1)$, $pi \in P_I$: $\forall t_x \in ti(t_2, pi)$, $t_y \in ti(t_1, pi)$: $er(t_x) = er(t_y)$
Definition 3.4: $\forall t_2 \in sb(t_1)$, $pi \in P_I$: $\forall t_x \in ti(t_2, pi)$, $t_y \in ti(t_1, pi)$: $es(t_x) = es(t_y)$
...

Figure 2: Formal and generic definitions (CIM level)

Example: Secure Object Flows

- **CIM: Generic definition for data confidentiality and integrity**
- **PIM: Integration of secure object flows into the UML**
  - business-level: process view → security-extended UML activity models
  - service-level: SOA views → UML component structure, service activity, and secure invocation protocol
- **PSM: Web Services → WS-BPEL, WSDL, WS-SecurityPolicy**
- **Tool support for**
  - all modeling views (business processes, security properties, software services)
  - automatic model transformations
  - deployment of software artifacts in runtime engine

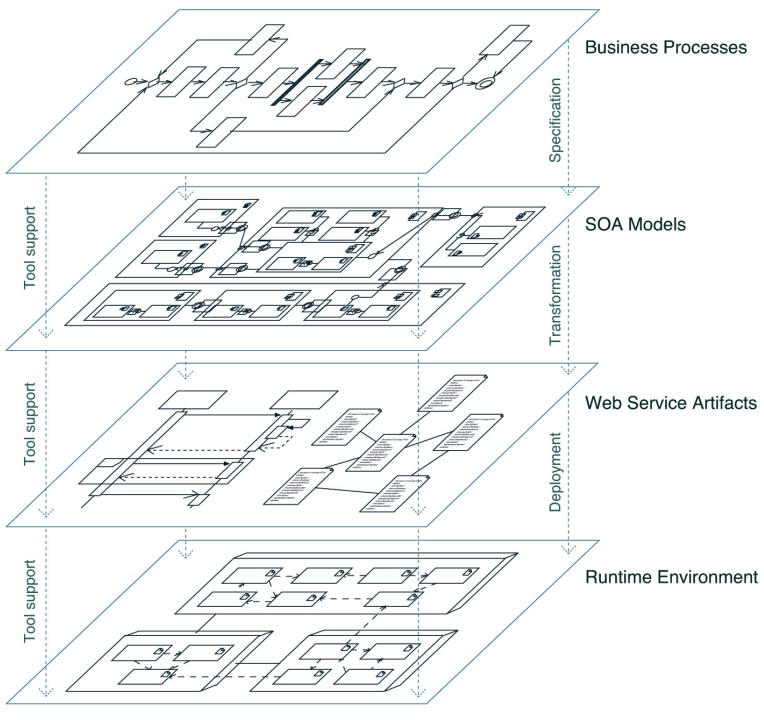


Figure 3: Integrated tool support for the definition and implementation of secure object flows

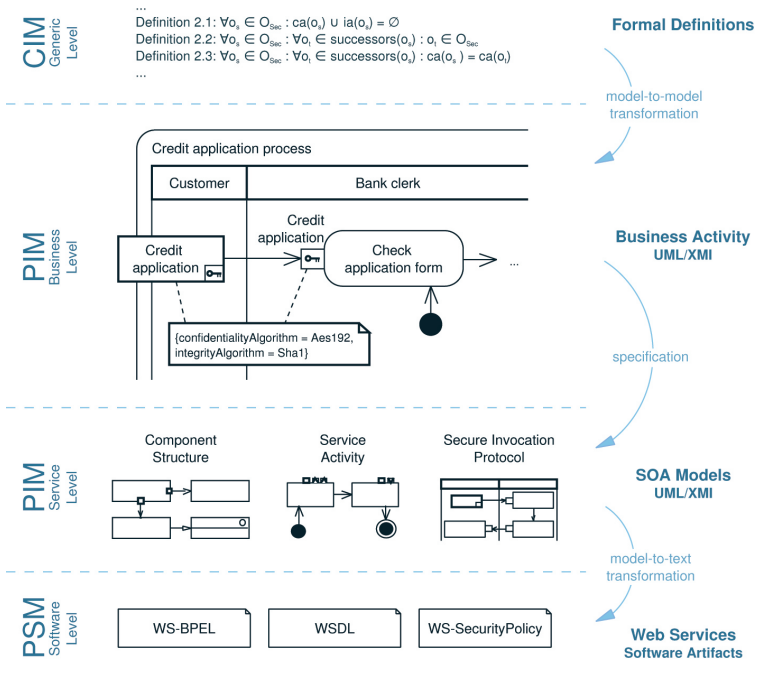


Figure 4: Different modeling levels, views, and transformations

References
B. Hoisl, S. Sobernig, and M. Strembeck: Modeling and Enforcing Secure Object Flows in Process-driven SOAs: An Integrated Model-driven Approach. In: Software and Systems Modeling (SoSyM), Springer, 2012, forthcoming
B. Hoisl, S. Sobernig, S. Schefer-Wenzl, M. Strembeck, A. Baumgrass: Design Decisions for UML and MOF based Domain-specific Language Models: Some Lessons Learned, In: Proc. of the 2nd Workshop on Process-based approaches for Model-Driven Engineering (PMDE), July 2012
B. Hoisl and M. Strembeck: A UML Extension for the Model-driven Specification of Audit Rules. In: Proc. of the 2nd International Workshop on Information Systems Security Engineering (WISSE), Springer LNBIP, Vol. 112, June 2012
B. Hoisl and S. Sobernig: Integrity and Confidentiality Annotations for Service Interfaces in SoaML Models. In: Proc. of the International Workshop on Security Aspects of Process-aware Information Systems (SAPAIS), IEEE CPS, August 2011
B. Hoisl and M. Strembeck: Modeling Support for Confidentiality and Integrity of Object Flows in Activity Models. In: Proc. of the 14th International Conference on Business Information Systems (BIS2011), Springer LNBIP, Vol. 87, June 2011
M. Strembeck and J. Mendling: Modeling Process-related RBAC Models with Extended UML Activity Models. In: Information and Software Technology (IST), Vol. 53, No. 5, May 2011

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Privacy in e-Health

Johannes Heurix and Thomas Neubauer

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

As highly sensitive patient information provides a promising goal for attackers, there is increasing social and political pressure regarding the prevention of health data misuse. Traditional data security and access control mechanisms have their limitations in that they are vulnerable against inside attacks by malicious administrators. The answer to this problem is to let the patient as data owner control the access rights of trusted third parties.

Challenges

- Nowadays, the protection of sensitive data is more important than ever before, because data is stored for longer periods of time and in a centralized way.
- It is the patient's right to demand privacy (e.g., HIPAA, EC Directives, Domestic Acts) as disclosure of medical data can create serious problems for the patient.
- On their own, traditional access control, disassociation, and encryption techniques have their limitations.
- It is necessary to assure the availability of health data for secondary use to improve clinical studies.

Usage Scenarios

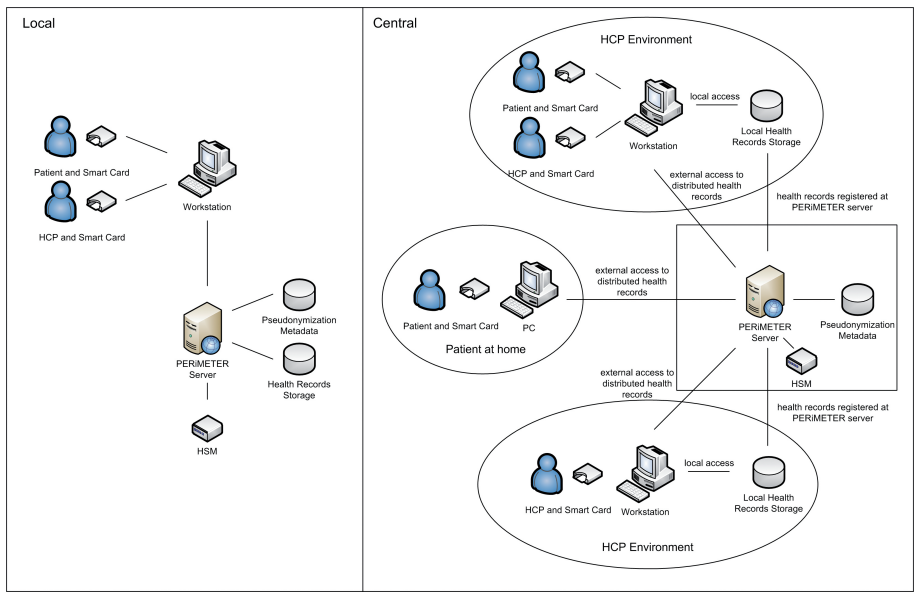


Figure 1: PERiMETER Usage Scenarios

- In the local scenario, PERiMETER pseudonymizes only records stored in the local data repository. Both patient and health professional access the records via the same workstation using personal smart cards as authentication tokens. An optional server-side hardware security module provides cryptographic services with enhanced key protection.
- In the central scenario, PERiMETER is responsible for managing access to multiple records at multiple locations. While the pseudonymization metadata contain only references, the actual health records remain at the individual local storages. Through the PERiMETER server, the data owner can grant trusted persons from other environments access to selected records.

PERiMETER

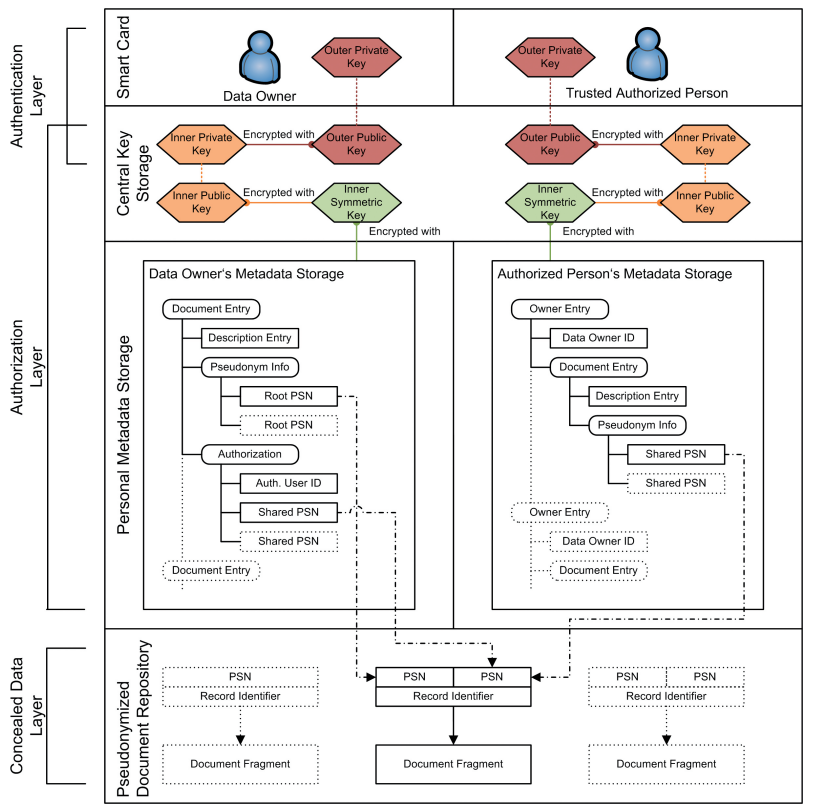


Figure 2: PERiMETER Concept

PERiMETER (Pseudonymization and pERsonal METadata EncRyption) utilizes a pseudonym-based access control mechanism and a layer-based security model with multiple cryptographic keys to grant access only to authenticated and authorized persons. The patient as data owner strictly controls all access rights to personal health data and is able to create access authorizations for trusted persons, while depersonalized and pseudonymized medical information is available for secondary use. Record fragment links are managed by personal encrypted metadata storages that provide privacy-preserving querying mechanisms using an XML Schema-aware searchable encryption scheme.

Pseudonyms

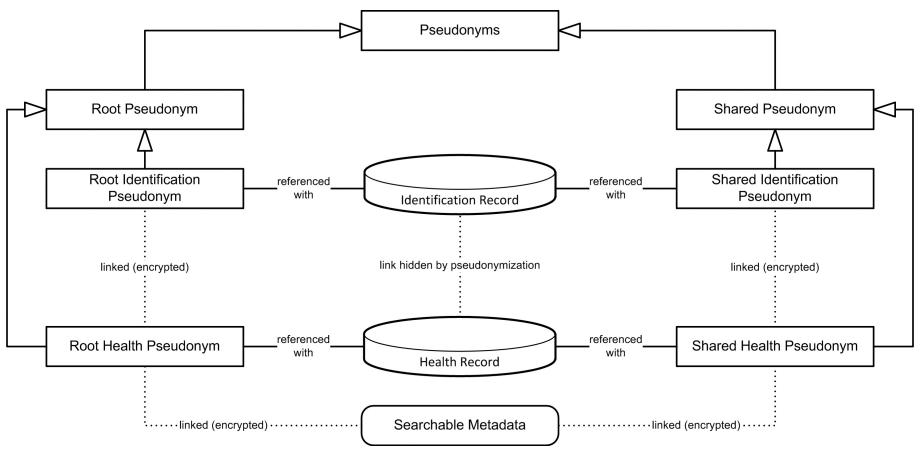


Figure 3: Pseudonymization Data Model

Root pseudonyms are known to the patient as data owner only and are used as references to represent the links between the document fragments. Fragment-specific shared pseudonyms created by the data owner provide trusted persons with this linking information and act as authorization tokens.

T. Neubauer and J. Heurix: "A Methodology for the Pseudonymization of Medical Data" in International Journal of Medical Informatics, Vol. 80/3, 2010.
J. Heurix, M. Karlinger, T. Neubauer: "Pseudonymization with Metadata Encryption for Privacy-Preserving Searchable Documents" in Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS'12), 2012.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Spoiled Onions: Exposing Malicious Tor Exit Relays

Philipp Winter, Richard Köwer, Martin Mulazzani, Markus Huber,
Sebastian Schrittwieser, Stefan Lindskog, Edgar Weippl

COMET
Competence Centers for Excellent Technologies
www.ffg.at/comet

secure
sba-research.org

Problem Description

- The **Tor network** is run by volunteers.
- 4,500 relays and 1,000 exit relays 24/7
- Used by hundreds of thousands of users every day
- Mischief can happen:
  - Man-in-the-middle attacks
  - Active or passive
  - Related work neither longitudinal nor current

Motivation

- Develop new scanners to automatically detect mischief
  - SSL and SSH Man-in-the-middle attacks
  - Plaintext credential sniffing
- Longterm analysis
- Report findings to the Tor project for node removal
- Improve overall user security

New Scanners

exitmap

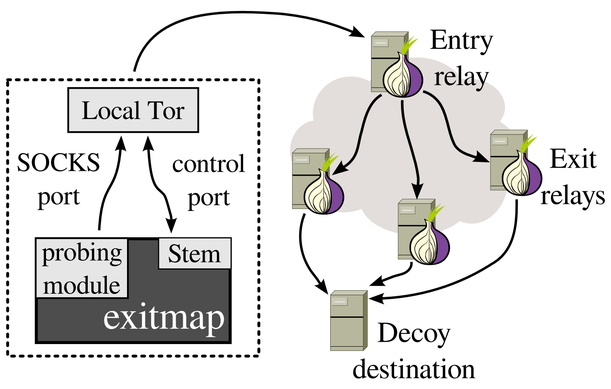


Figure 1: *exitmap* for detecting SSL MitM

HoneyConnector

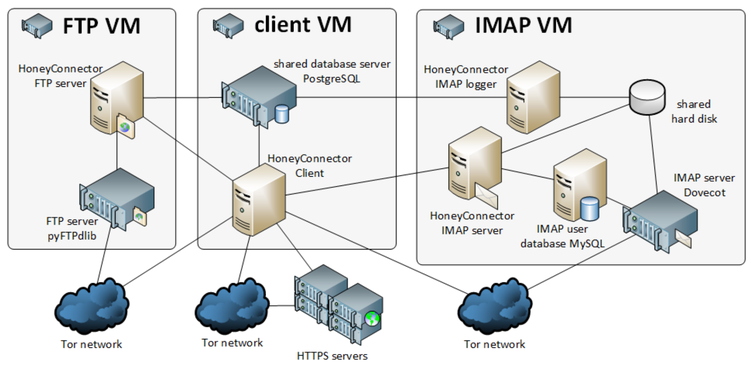


Figure 2: *HoneyConnector* for detecting credential sniffing (FTP, IMAP)

Results

- *exitmap* can scan all exit nodes in 60 seconds
- *HoneyConnector* did more than 50,000 bait connections
- Runtime of both scanners for 5 months
  - **40** malicious relays detected using exitmap
  - **27** malicious relays detected using HoneyConnector
- Russian group of 20 man-in-the-middle relays
- International group of 5 credential re-use relays
- Indian group of 7 credential re-use relays

Log-in Attempts with Sniffed Credentials

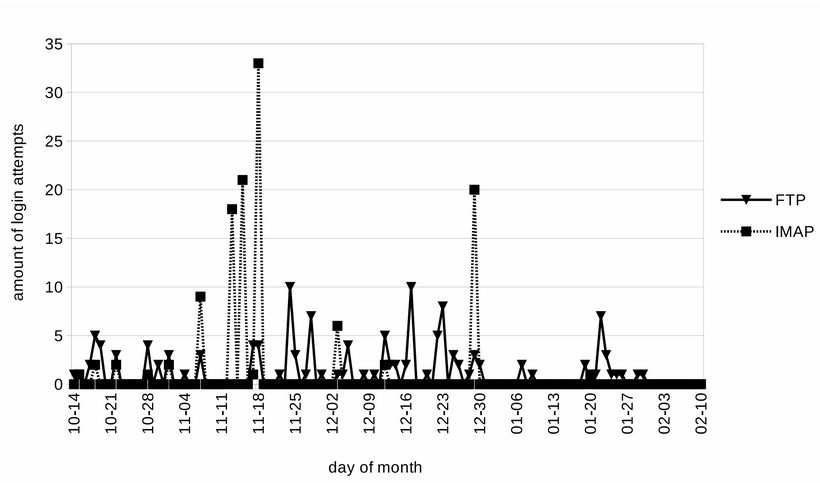


Figure 3: Timeline of log-in attempts

Future Work & Conclusion

Future Work:

- Write additional modules for *exitmap*
- Long-term deployment with the Tor project
- Attack attribution problem

Conclusion:

- Code for both scanners is released here:
  `http://www.cs.kau.se/philwint/spoiled_onions`
- Best to use Tor as recommended: no plaintext protocols
- More long-term experiments necessary

Philipp Winter, Richard Köwer, Martin Mulazzani, Markus Huber, Sebastian Schrittwieser, Stefan Lindskog, and Edgar Weippl. Spoiled onions: Exposing malicious tor exit relays. In *Privacy Enhancing Technologies Symposium (PETS)*, 2014.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFW und das Land Wien gefördert. Das Programm COMET wird von der FFG abgewickelt.

The Hardness of Code Equivalence over Finite Fields and its Application to Code-based Cryptography

Dimitris E. Simos, Nicolas Sendrier

COMET Competence Centers for Excellent Technologies www.ffg.at/comet

secure sba-research.org

Inria

The Code Equivalence Problem

- **Problem specification**
  - Code equivalence depends on the code alphabet and equivalence mapping
  - Linear codes are defined over finite fields and the equivalence mappings are the semi-linear isometries of the Hamming space
- **Three notions of code equivalence**
  - *Permutation Code Equivalence (PCE)*
  - *Linear Code Equivalence (LCE)*
  - *Semi-linear Code Equivalence (SLCE)*
- **Two complexity problems**
  - *Decisional:* Decide whether the codes are equivalent up to a semi-linear isometry
  - Computational: Retrieve the semi-linear isometry

Hardness of Code Equivalence

- **Complexity**
  - PCE is difficult to decide in the worst case
  - Not NP-complete
  - At least as hard as Graph Isomorphism
  - Recent reduction of PCE to the Hidden Subgroup problem (HSP)
- **Related algorithms**
  1. Hypergraph algorithms for PCE, LCE and SLCE
  2. Algebraic algorithms for LCE
  3. Support splitting algorithm (SSA) for PCE
  4. No efficient algorithm for LCE was known

An Extension of SSA

- **Our approach**
  - Reduce LCE or SLCE to PCE
  - Achieved by introducing the closure of a linear code
- **Efficiency of the reduction**
  - The closure reduces LCE to the hard instances of SSA for PCE
  - Exceptions are the ternary and quaternary field
- **Polynomial Extension of SSA**

Algorithm	Field (alphabet)	Random codes (average-case)	Weakly self-dual codes (worst-case)
SSA	F_2	$O(n^3)$	$O(2^k n^2 \log n)$
SSA extension	F_3	$O(n^3)$	$O(3^k n^2 \log n)$
SSA extension	F_4	$O(n^3)$	$O(2^{2k} n^2 \log n)$
SSA extension	F_q, $q \geq 5$	$O(q^k n^2 \log n)$	$O(q^k n^2 \log n)$

- **Conjecture**
  - LCE problem is hard for almost all of the instances, for given $q \geq 5$.

Zero-knowledge Protocols for Code-based Cryptography

- **Zero-knowledge (ZK) protocols**
  - Allow a prover to convince a verifier that it knows a secret without the verifier learning any information about the secret
  - No information can be revealed no matter what strategy a so-called cheating verifier, or cheater, follows when interacting with the prover
- **Code-based cryptography (CBC)**
  - The underlying hard problems do not seem so far to be susceptible to attacks mounted by quantum computers
  - Designed cryptosystems are candidates in a post-quantum era
- **ZK protocols for CBC**
  - Using error-correcting codes for identification schemes

An Improved Version of Girault's ZK Protocol

- **Girault's identification scheme**
  1. Three-pass
  2. Cheating probability of 1/2
  3. Has to be repeated t times to reach a security level of $1 - (1/2)^t$
  4. Computations are performed on the standard model
- **Security assumptions**
  - Hardness of decoding in a linear code
  - Hardness of PCE [broken by SSA for almost all of the instances]
- **Our contribution**
  1. Repair the protocol by using LCE instead of PCE
  2. The scheme is again usable in the standard model

Code Equivalence and Quantum Fourier Sampling

- **Implications of the reduction of PCE to HSP**
  - McEliece-type cryptosystems resist precisely the attacks to which the RSA and ElGamal cryptosystems are vulnerable (i.e., those based on generating and measuring coset states)
  - Thus strong Fourier sampling, on which almost all known exponential speedups by quantum algorithms are based, offers no advantage
- **Our contribution**
  1. We showed that the instances of codes that are HSP-hard for PCE remain HSP-hard for LCE
  2. Opens the path for the design of McEliece-type cryptosystems based on LCE

N. Sendrier and D. E. Simos: "The hardness of code equivalence over Fq and its application to code-based cryptography," in PQCrypto '13: Proceedings of the 5th International Conference on Post-Quantum Cryptography, Lecture Notes in Computer Science, vol. 7932, pp. 203–216, 2013.
N. Sendrier and D. E. Simos: "How easy is code equivalence over Fq?," in WCC '13: Proceedings of the 8th International Workshop on Coding and Cryptography, pp. 80–92, 2013.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

TIMBUS
Timeless Business Processes and Services

Andreas Rauber

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

TIMBUS TIMELESS BUSINESS

Motivation

Objective: enlarge understanding of Digital Preservation (DP) to specifications of service, software and their dependencies for the preservation of BPs

- **Business Processes** (BP): processed, analyzed, transformed and rendered data – e.g., civil engineering, aerospace, medical data, scientific workflow (e.g., LHC)
- Companies have to guarantee BP persistence for a **long time** (5,10,..., 50 years)

TIMBUS

- analyzes and recommends which BP aspects should be preserved and how
- based on feasibility and cost-benefit analysis
- delivers methodologies and tools to capture and formalize existing BPs on technical/organizational levels
- aligns DP with Enterprise Risk Management (ERM) & Business Continuity Management (BCM)

Phases

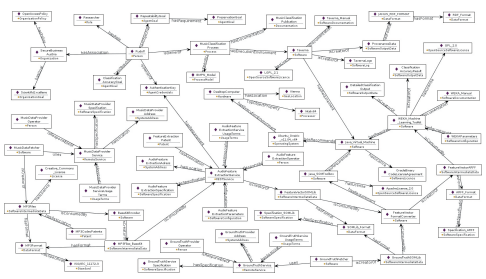
BP Preservation can be broken down into:

1. **Planning**
   - perform enterprise risk analysis
   - determine requirements for preserving relevant BPs
   - capture and define relevant context and dependencies
2. **Preservation**
   - perform required preservation actions (e.g., emulation of external services and migration of data)
3. **Redeployment**
   - reactivates and reruns BPs in executing environment
   - verification of performance and behavior

SBA Research Topics

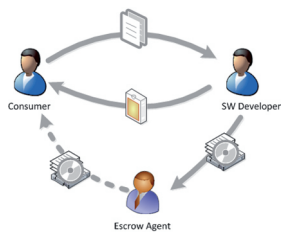
Determine process context

Document dependencies and environmental factors that influence processes



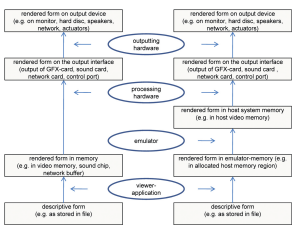
Software escrow – technical and legal framework

Semi-automatic audit for depositing artifacts for software escrow



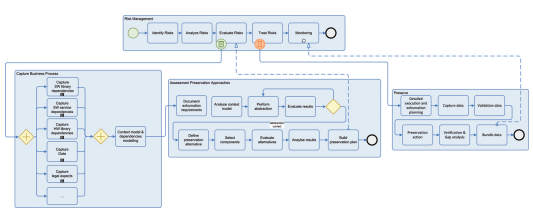
Validation of preserved business processes and verification of redeployed processes

Validate processes for preservation and verify the performance and behavior of redeployed processes in new execution environments



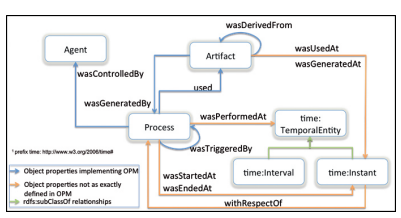
Processes for DP of BPs

Process framework to preserve BPs across different industrial domains



Provenance and authenticity

Aims towards trusted preservation of BPs, documents the history of data and processes



Compliance issues of business processes

Define legal aspects for preserving business processes

ACKNOWLEDGMENT: Part of this work is funded by the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement No 269940.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

A Novel Approach to Software Testing via Combinatorial Designs

Dimitris E. Simos, Aleksandar Hudic, Severin Winkler, Andreas Bernauer

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

Software Testing

- Problem specification
  - Testing is an important but expensive part of the software development process
  - The problem is to design a test plan for a software system
- Challenges
  - We cannot test everything
  - Exhaustive search of search space increases time needed exponentially
- Test plans for software testing
  - To design a test plan, the tester identifies possible output values from each of the stages of the software system
  - It is important to find a test plan that is not too large, yet tests for most of the interactions among the possible outputs in the modules of a software system

Combinatorial Testing

- Motivation
  - Select few tests and still achieve good coverage
  - Software developers have begun using combinatorial designs to test for interactions of the system
- Combinatorial test design process
  1. Model the input space. The model is expressed in terms of stages and stage values
  2. The model is input into a combinatorial design procedure to generate a combinatorial object that is simply an array of symbols
  3. Every column of the generated array is used to output a test plan of the software system
- Benefit
  - Steps 2 and 3 can be automated

Combinatorial Testing

- Challenges
  - Two to three-way combinations reach 100 percent detection
  - Generating test suites to cover all t-way interactions is a difficult mathematical problem studied for nearly a century

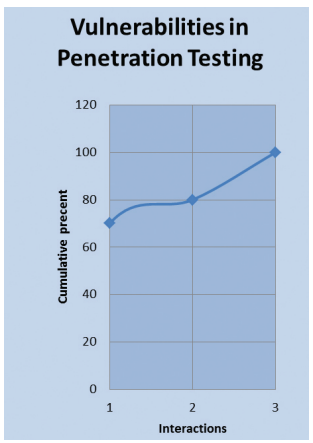


Figure 1: Coverage vs interactions in penetration testing

Mobsetip Project

- Research problems related to penetration testing
  - Generate test plans
  - Characterize vulnerabilities
  - Automated detection of such vulnerabilities
- Current approach
  - Employ mixed-level covering arrays (class of combinatorial designs)
  - Vulnerabilities are caused by two to three-way interactions

Design Test Plans for Penetration Testing

- A toy example
  1. User input can be in capital or lower-case letters and quotes
  2. Validation for SQL injection with values yes and no
  3. User database interaction with values true and false
  4. Validation for cross-site scripting (XSS) with values yes and no
- Analysis
  - We have three binary stages and one with three stage values, i.e., a total of $3 \times 2^3 = 24$ different scenarios
- Goal
  1. Reduce the number of test scenarios
  2. Still test all two-way interactions (user input, validation for SQL injection)

Test plans from Covering Arrays

- Test scenarios generated from MCA(2,4,(2,2,2,3))

User Input	0	1	2	0	1	2
SQL Injection	0	1	0	1	0	1
User DB Interaction	0	0	1	1	1	0
XSS	0	1	1	1	0	0

- Test configurations

User Input	caps	small	quotes	caps	small	quotes
SQL Injection	no	yes	no	yes	no	yes
User DB Inter.	false	false	true	true	true	false
XSS	no	yes	yes	yes	no	no

- Achieve a 65 percent reduction on test plans

Highlights and Future Research

- Automated test plans for software systems
- Combinatorial design approach
- Implementation of a test suite

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Automated Analysis and Clustering of Windows Shellcodes

Georg Merzdovnik, Paolo Milani Comparetti

COMET
Competence Centers for Excellent Technologies
www.ffg.at/comet

secure
sba-research.org

Motivation

- New kinds of shellcodes are released into the wild every day
- Impossible to analyze all samples manually
- Most available tools rely on a high degree of user interaction
- Accessing these tools is often tedious

Goals

- Provide a system that is able to analyze shellcode automatically
- Since most shellcodes use self-decryption routines, make use of dynamic analysis to obtain unencrypted sample for further analysis
- Automatic generation of report for malware analysts
- System for further analysis of the shellcodes to detect similarities

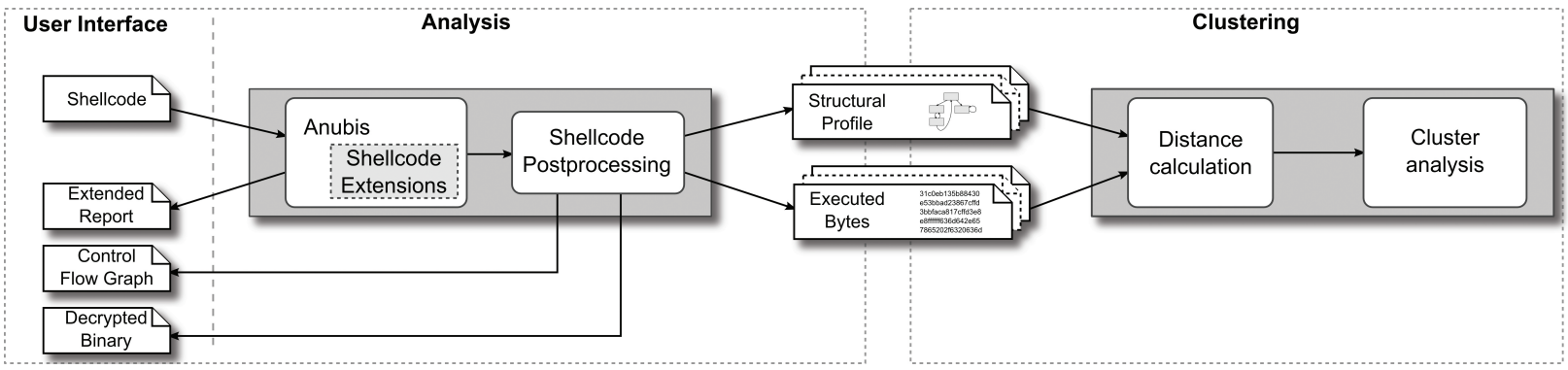


Figure 1: System overview

Approach

- Extend the existing Anubis environment for analyzing unknown binaries to allow the processing of shellcodes
- Collect samples to test clustering based on different distance metrics

Sample Analysis

- Extension of Anubis' underlying qemu to allow a fine-grained dynamic analysis at instruction level (logging of information about the shellcode's execution and memory accesses)
- Static processing of the logs to extract information about the shellcode's internals
  - Control flow graph
  - Decrypted shellcode version
  - Structural profile
  - Executed bytes

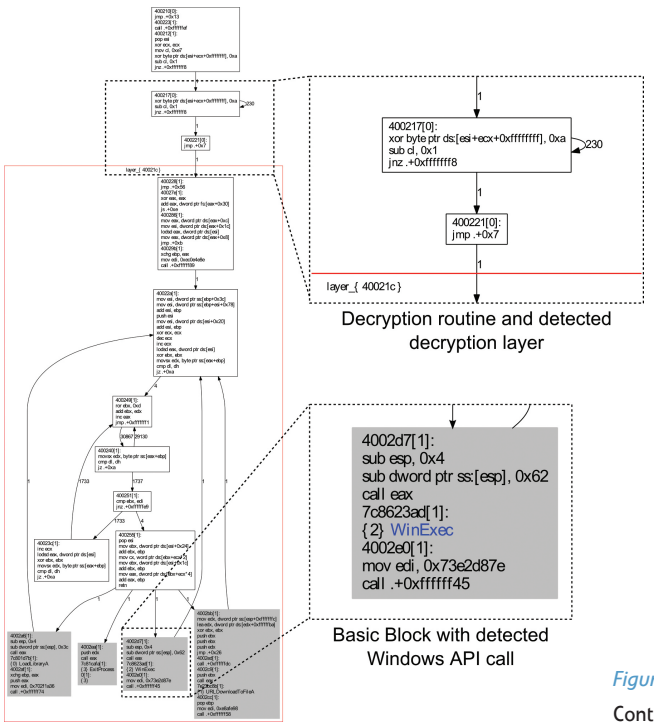


Figure 2: Example of a generated Control Flow Graph (CFG)

Evaluation

Sample Analysis

- Evaluation of successful execution: Check if they did a task like bind or download & execute
- Majority of collected samples showed a download & execute behavior (i.e., the shellcode loaded another binary that was then executed)

Clustering

- Suitability test of distance metrics for clustering shellcodes
- Test sample set containing a variety of shellcodes
- Encoded with different techniques

	original	msf-call4	msf-countdown	msf-fstenv	nops	Tapion
addUser	0	1	2	3	4	5
download-exec	6	7	8	9	10	11
exec	12	13	14	15	16	17
messagebox	18	19	20	21	22	23
shell-bind-tcp	24	25	26	27	28	29

Table 1: Mapping of encoder samples to dendrogram sample

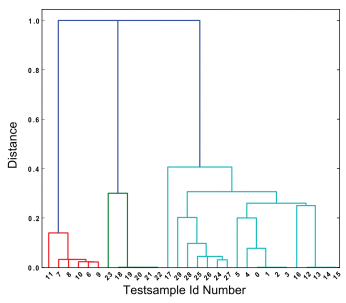


Figure 3: Structural distance dendrogram of encoder samples

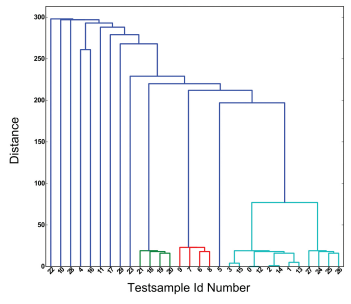


Figure 4: Exedit distance dendrogram of encoder samples

Conclusion

- Implementation of easy-to-use shellcode submission system
- Generates high and low-level information about the shellcode
- Distance based on structure of the shellcode is less prone to error than the distance based on executed bytes

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwfj Bundesministerium für Wirtschaft, Familie und Jugend
FFG
wirtschaftsagentur wien zit Die Technologieagentur der Stadt Wien
Christian Doppler Forschungsgesellschaft
FWF Der Wissenschaftsfonds.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Combinatorial Testing for Web Application Security

Dimitris E. Simos, Severin Winkler, Bernhard Garn, Ioannis Kapsalis,
Andreas Bernauer, Peter Aufner

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

The Best of Both Worlds: Combinatorial Security Testing

Model-based Security Testing in Practice

- **Research Problems**
  - Generate test cases
  - Characterize vulnerabilities
  - Automated detection of such vulnerabilities
    - Cross-Site Scripting (XSS)
    - SQL Injection (SQL-I)
- **Current approach**
  - Employ mixed-level covering arrays (class of combinatorial designs)
  - Vulnerabilities are caused by 2- to 4-way interactions

Combinatorial Testing

- **Motivation**
  - Select few tests and still achieve good coverage
  - Software developers have begun using combinatorial designs to test for interactions of the software system
- **Combinatorial test design process**
  1. Model the input space; the model is expressed in terms of stages and stage values
  2. The model is input to a combinatorial design procedure to generate a combinatorial object which is simply an array of symbols
  3. Every column of the generated array is used to output a test plan of the software system
- **Benefit**
  - Steps 2 and 3 can be automated

An (Automated) XSS Testing Framework

- **Modelling Phase**
  - Discretizing the search space // designer
  - Devise payload grammars // black-box combinatorial testing
- **Test Generation Phase**
  - Generate CAs from a combinatorial test design tool // ACTS automation
  - Translate abstract tests to XSS attack vectors // bash scripts
- **Test Execution Phase**

  Preprocessing **urls**:=Spider(webpage) // i.e. spider automation

  Injection XSSinjector(**urls**,attack vectors) // python injector

  Oracle Check whether an attack vector is reflected on webpage

Case Study

- **Systems Under Test (SUTs)**
  - Training applications
    - Webgoat - version 5.4
    - Mutillidae II - version 2.6.3.1
    - Damn Vulnerable Web Application (DVWA) - version 1.8
  - Realistic, intentionally vulnerable applications
    - Gruyere - version 201-07-15
    - Bodgeit - version 1.3
- **Penetration Testing Tools**
  - Burp Suite
  - Zed Attack Proxy (ZAP) Project

Evaluation

- **Penetration Testing**
  - Hacked 18 out of 20 input field parameters
  - Different security levels
  - Combinatorial strength increases test coverage
- **Combinatorial Testing**
  - Reduction of 99.93% of search inputs
  - Test all 2-way interactions with 114 inputs out of all 158,799 possible inputs
  - While still being able to penetrate the SUTs

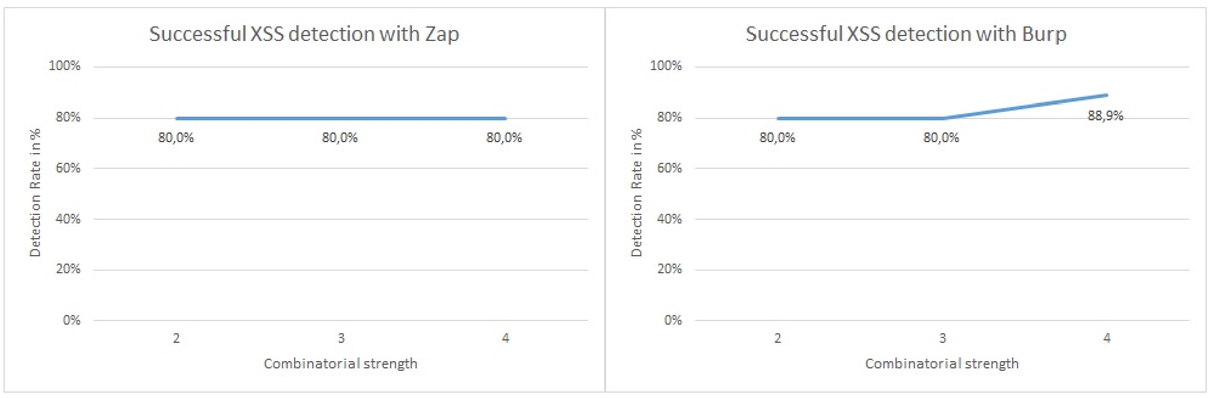


Figure 1: Comparison of XSS detection rate with different combinatorial strength

Conclusion

Highlights

- Combinatorial modelling of vulnerabilities
- Automated test cases for penetration testing
- Reduction of search space

Work in Progress

- Subgrammars for XSS detection
- Combinatorial security testing of web application scanners
- Implementation of combinatorial penetration testing framework

A. Bernauer, J. Bozic, D. E. Simos, S. Winkler, and F. Wotawa. Retaining consistency for knowledge-based security testing. In *IEA/AIE '14: Proceedings of the 27th International Conference on Industrial, Engineering & Other Applications of Applied Intelligent Systems, Lecture Notes in Computer Science, to appear*.
J. Bozic, D. E. Simos, and F. Wotawa. Attack pattern-based combinatorial testing. In *AST '14: Proceedings of the 9th International Workshop on Automation of Software Test, ICSE '14: 36th ACM/IEEE International Conference on Software Engineering*, pages 1--7, 2014.
B. Garn and D. E. Simos. Eris: A tool for combinatorial testing of the linux system call interface. In *IWCT '14: Proceedings of the 3rd International Workshop on Combinatorial Testing, ICST '14: 7th IEEE International Conference on Software Testing, Verification and Validation*, pages 58--67, 2014.
D. E. Simos and S. Winkler. An approach to penetration testing via combinational designs. In *ASQT '13: Proceedings of the 11th User Conference for Software Quality, Test and Innovation, Austrian Computer Society (OCG), to appear*.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFW und das Land Wien gefördert. Das Programm COMET wird von der FFG abgewickelt.

Covert Computation

Sebastian Schrittwieser

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

Static Malware Detection

- Today's static malware detection systems (i.e., virus scanners) mainly rely on signatures of malware samples and thus work on the syntactical level only
- Recently, the concept of semantics-aware malware detection was introduced. Here, the maliciousness of software is evaluated based on a semantic analysis of the program: templates that define malicious behavior are matched against the software

Problem Description

- The evaluation of a program's maliciousness is based on a model of the underlying hardware
- Models are an abstract representation of the real world and are not strong enough to map the entire functionality of the hardware
- Threat: By exploiting this knowledge gap, hidden functionality can be implemented

Evaluation

- Today's semantics-aware malware detection approaches have very weak models of the hardware and thus do not identify functionality hidden in side effects. The complexity of the analysis is moved to a layer below semantics
- The average increase of binary size is moderate
- The concept suffers from performance slowdowns. However, for certain types of malware (e.g., slow spreading worms), performance is not the primary concern

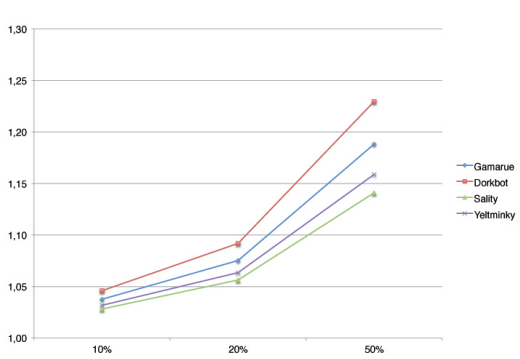


Figure 3: Space overhead

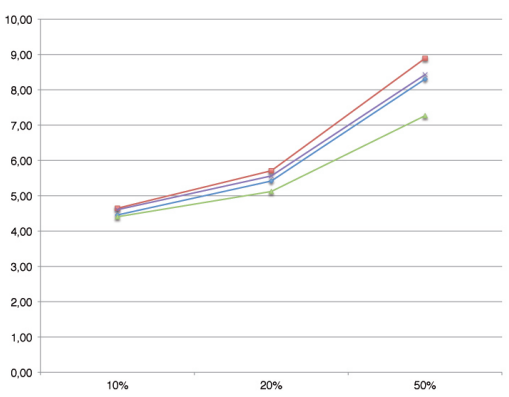


Figure 4: Complexity overhead

Malware Obfuscation Techniques

- Previous approaches implemented the concept of hiding code in data:
  - Encryption
  - Packers
  - "Mimimorphism" (Wu et al., CCS 2010)
- We aim to *hide code in code*

Concept

- "Covert computation" – exploiting side effects of microprocessors in order to hide functionality
- Side effects can be used to hide malicious functionality inside harmless-looking code

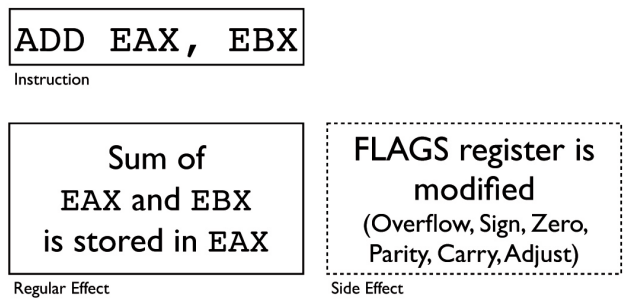


Figure 1: Sideeffects of the AND instruction

- Example: FLAGS Register of the x86 architecture
  - Rotation instructions (RCL, RCR) move bits of the input register into the Carry Flag (CF)
  - Two conditional jumps can be used to rebuild logical operations such as XOR

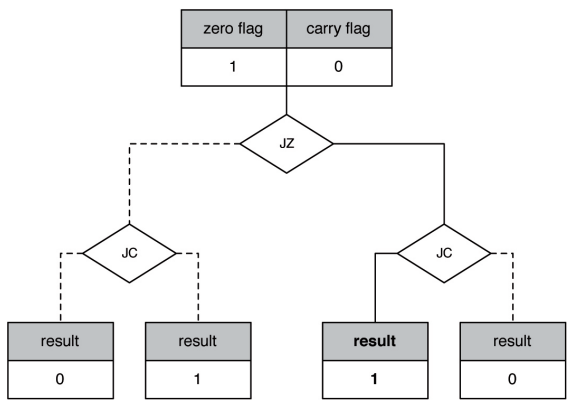


Figure 2: XOR (implemented in side effects)

Conclusion

- Today's microprocessor architectures are highly complex
- Side effects are difficult to map with machine models
- This knowledge gap can be exploited for hiding small code portions in larger ones

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Defense-side Reconnaissance:
Preliminary Surveying of an Attacker's Profile

Peter Frühwirt, Sebastian Schrittwieser, Edgar Weippl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

Motivation

Attackers have as much time as they want to gain information about the targeted system. In order to create appropriate defense strategies, the defender has to know more about the intruder than IDS can deliver in a short amount of time.

Intrusion detection systems (IDS) use different mechanisms

- **signature-based**
  - static and limited
  - can be easily bypassed by the intruder
  - needs security experts to create signatures
- **behavior-based**
  - high false positive rate
  - often not applicable to complex systems

In conclusion these systems have to deal with different problems:

- Stale signatures are easily bypassed by attackers
- High complexity of systems and attacks
- Dedicated domain knowledge needed for IDS rule creation

System design and implementation

Our approach uses machine learning for classification, which is transparent to the user. Traffic is preprocessed by adding attributes and metadata to each connection. Our system automatically decides which machine-learning algorithms are used by evaluating on a training set. New traffic is classified by using these optimized models.

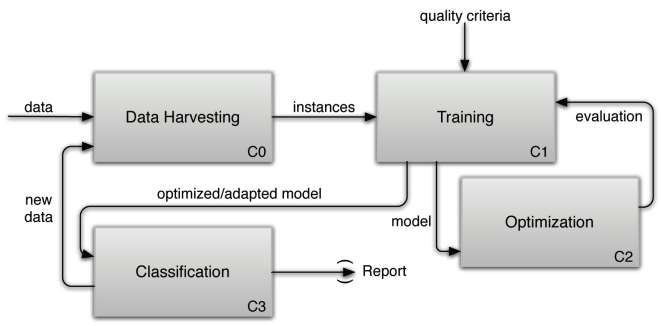


Figure 1: learning and adoption process

Optimization

New approach to reduce aberrations: Classification voting

- Using different classification algorithms
- Clever majority voting to determine a common result

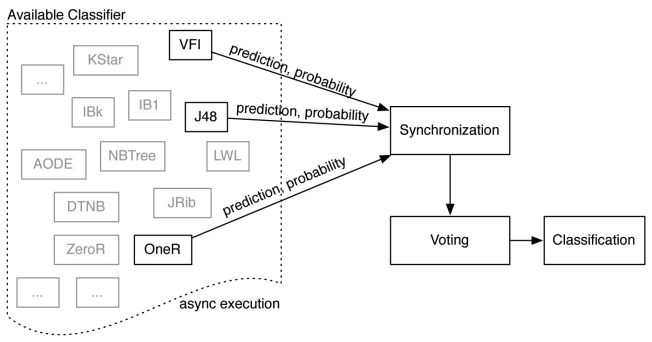


Figure 2: Classification voting

Evaluation

Feasibility: Implementation of a prototype

- Automated learning, optimization and classification

UCSB iCTF 2011 traffic dump (about 246 GB traffic). Detection of automated behavior

- penetration testing tools (simple, static signature)
- scorebot (complex, obfuscated, changing signature)

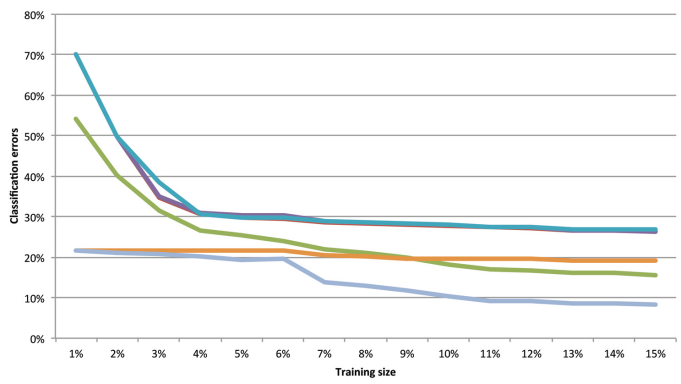


Figure 3: classification performance

Conclusion and future work

- New approach of intrusion detection
- Using machine learning to classify traffic
- Classification voting for better results
- Network forensic analysis possible
- Prediction of attack's next steps
- Traffic clustering
- Generation of attackers' profiles

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Detecting Environment-Sensitive Malware

Martina Lindorfer, Clemens Kolbitsch and Paolo Milani Comparetti

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org
iseclab

Problem Outline

- Thousands of new malware samples surface every day
- Automation of analysis is necessary → Dynamic malware analysis
- Sample is executed in a monitored environment (emulator, virtual machine)
- Secure Systems Lab developed Anubis ("Analyzing Unknown Binaries")
- Public malware analysis sandbox: http://anubis.iseclab.org/
- **BUT:** Malware can discover that it is being analyzed
- Environment-sensitive malware checks for characteristics of the sandbox: CPU bugs, timing, Windows product ID, username, hardware serials, ...
- Malware exhibits no malicious activity in the sandbox ("analysis evasion")

→ **How can we detect analysis evasion?**

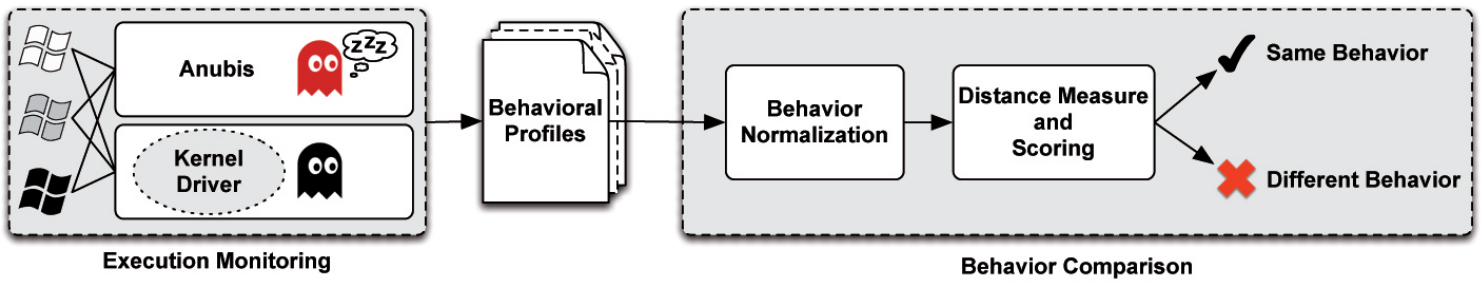


Figure 1: System Overview

Approach

- Build a verification system for Anubis to uncover evasion techniques

Execution Monitoring

- Windows kernel driver intercepts and logs system calls on a real host
- Logs are converted to behavioral profiles:
  Malware behavior as a set of operations on operating system resources

```
file|C:\foo.exe|write:1
process|C:\Windows\foo.exe|create:0
network|tcp_conn_attempt_to_host|www.foobar.com
registry|HKLM\System\CurrentControlSet\Services|set_value('xy'):1
```

Behavior Comparison

- Comparison of behavior in Anubis and on real host with driver
- Different Windows installations → normalize behavior
  1. Remove noise
  2. Generalize username
  3. Generalize environment (hardware, language)
  4. Randomization detection
  5. Repetition detection (file infectors)
  6. Filesystem and registry generalization (ignore missing resources)
- 3 executions in each sandbox (Anubis and real host)
- Intra-sandbox distance = variations between executions
- Inter-sandbox distance = variations between sandboxes
- Inter-sandbox distance – Intra-sandbox distance = evasion score [0,1]
- If evasion score ≥ threshold → different behavior; else same behavior
- Use findings to improve Anubis and prevent analysis evasion

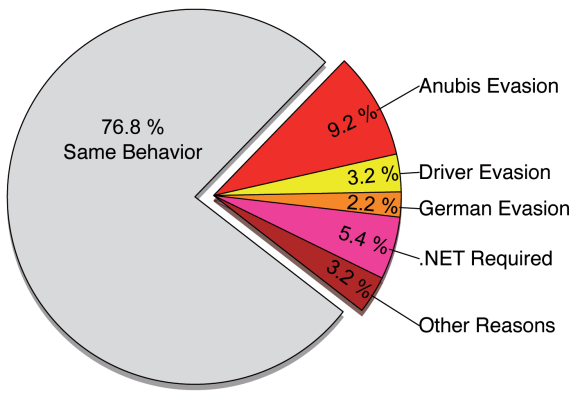


Figure 2: Manual classification of samples in the training dataset

Evaluation

Experiments with 4 different sandboxes

→ Anubis, Driver with Anubis image, Driver with German image, Driver with other image (different user, .NET, ...)

Training Dataset

- 185 malware samples
- Used to optimize normalization and scoring
- Manual classification
- Reached 99.5% accuracy @ threshold 0.4

Test Dataset

- 1686 malware samples
- Used to verify our system
- 25.56% samples above threshold
- Spot tests to find reasons for evasion

→ **Several new Anubis evasion techniques detected**
→ **Configuration flaws and missing software in Anubis (.NET, JRE, Microsoft Office, etc.)**
→ **Driver vulnerable to bypassing, but we can fix it**
→ **We can use these results to improve Anubis in order to observe a wider variety of malware behavior and thwart evasion!**

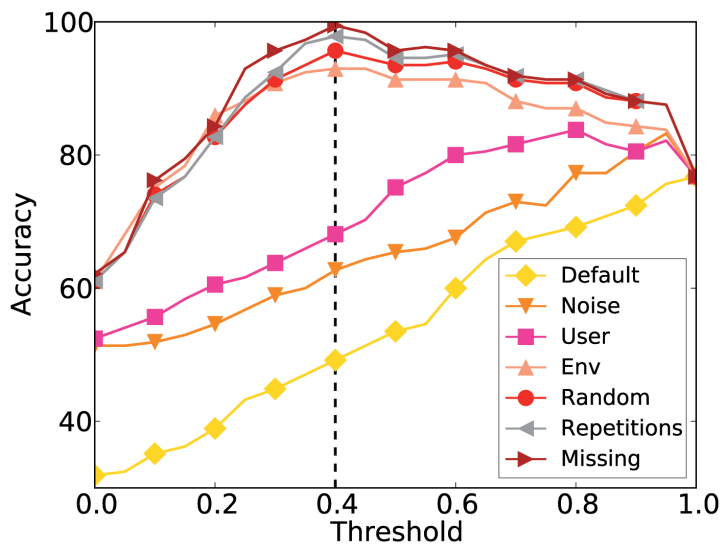


Figure 3: Efficiency of behavior normalization measured by result accuracy

Reference
M. Lindorfer, C. Kolbitsch, Paolo M. C.: "Detecting Environment-Sensitive Malware" in International Symposium on Recent Advances in Intrusion Detection (RAID 2011), 2011

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Enter Sandbox: Android Sandbox Comparison

Sebastian Neuner, Victor van der Veen, Martina Lindorfer, Markus Huber, Georg Merzdovnik, Martin Mulazzani and Edgar Weippl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

Motivation

- 1 Billion Android devices in 2017
- SMSZombie: 500.000 infections
- Too many sandboxes out there: unsufficient, no comparison
- No survey of current state-of-the-art Android malware detection techniques

Contributions

- Discussion of methods to detect and fingerprint dynamic analysis sandboxes
- Comparison of 16 dynamic analysis platforms for Android regarding their features:
  - Level of introspection
  - Functionality
  - Interdependencies
- Evaluation of the effectiveness of eight of these dynamic sandboxes: publicly available malware corpora and Master Key vulnerabilities

Methodology

Selected Malware Samples

- **Obad:** Kaspersky Lab: "one of the most sophisticated mobile malware to date"
- **Geinimi:** Malware Genome Project, sends SMS and reads sensitive data
- **DroidKungFu:** sophisticated privilege escalation attacks
- **Basebridge/Nyleaker:** invalid manifest files to evade Androguard
- **MasterKey:** weaknesses in Androids ZIP format handling

Fingerprinting

Creation of APK files with different API levels to detect undocumented information:

- Joe Sandbox: API level 15
- ForeSafe: not possible
- VisualThreat: not possible

Interdependency

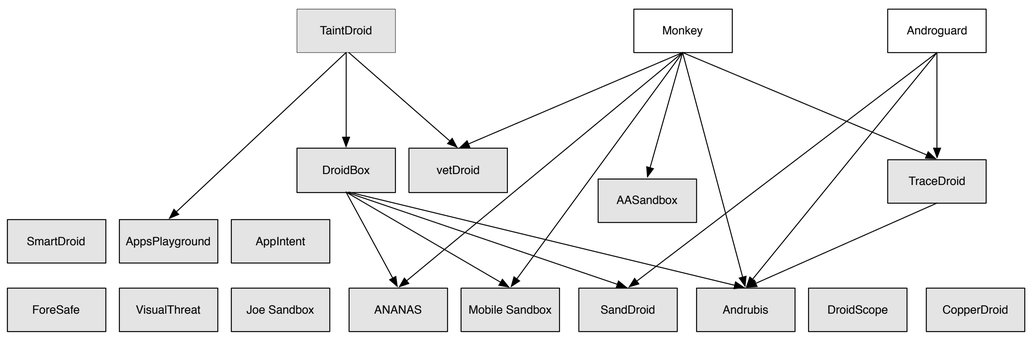


Figure 2 : Framework interdependency

Results

Framework	Implementation Details		Analysis Type			Analyzed Features			
	Android Version	Inspection Level	Static	Tainting	GUI Interactions	File	Network	Phone	Native Code
AASandbox	---	Kernel	✓		✓	✓	✓	✓	
AppIntent	2.3	Kernel	✓	✓	✓				
ANANANS	2.3-4.2	Kernel	✓		✓	✓	✓	✓	✓
Andrubis	2.3.4	QEMU & Dalvik	✓	✓	✓	✓	✓	✓	✓
AppsPlayground	---	Kernel	✓	✓	✓				
CopperDroid	2.2.3	QEMU	✓		✓	✓	✓	✓	✓
DroidBox	2.3-4.1	Kernel		✓		✓	✓	✓	
DroidScope	2.3	Kernel & Dalvik		✓		✓	✓	✓	✓
ForeSafe	?	?	✓		✓	✓	✓		
Joe Sandbox	4.0.3 / 4.0.4	?	✓		?	✓	✓	?	?
Mobile Sandbox	2.3.4	Dalvik	✓	✓	✓		✓	✓	✓
SandDroid	?	?	✓	✓	?	✓	✓	?	?
SmartDroid	2.3.3	Kernel	✓	✓	✓	✓	✓	✓	
TraceDroid	2.3.4	Dalvik	✓		✓	✓	✓	✓	
vetDroid	2.3	Kernel & Dalvik	✓	✓	✓	✓	✓	✓	
VisualThreat	?	?	✓			✓	✓	✓	✓

Table 1 : Table of results; ("---" means: installable on any Android version. "?" means: not possible to determine.)

Framework	Obad	Geinimi	DroidKungFu	Basebridge/ Nyleaker
Andrubis	✓/ ✓	✓/ ✓	✓/ ✓	✓/ ✗
CopperDroid	- / -	✓/ -	- / ✓	- / -
ForeSafe	✓/ ✓	✓/ ✓	✓/ ✓	✓/ ✓
Joe Sandbox	✓/ ✓	✓/ ✓	✓/ ✓	✓/ ✓
Mobile Sandbox	- / -	- / -	- / -	- / -
SandDroid	- / -	- / -	- / -	- / -
TraceDroid	✓/ ✓	✓/ ✓	✓/ ✓	✓/ ✓
VisualThreat	✓/ -	✓/ ✓	✓/ ✓	✓/ ✓

Table 2 : Analysis online sandboxes: two samples per malware family; (''✓'' means: detected. ''✗'' means: not detected. ''-'' means: analysis error.)

Framework	Bug 8219321	Bug 9695860	Bug 9950697	Python ZIP Bug
Andrubis	✓	-	-	✓
CopperDroid	-	-	-	-
ForeSafe	✓	✓	✓	✓
TraceDroid	✓	-	-	✓
VisualThreat	✓	✓	-	✓

Table 3 : Evaluation Master Key samples; ("✓" means: successfully executed. "-" means: sandbox was not able to execute the sample.)

Sebastian Neuner and Victor van der Veen and Martina Lindorfer and Markus Huber and Georg Merzdovnik and Martin Mulazzani and Edgar Weippl, ''Enter Sandbox: Android Sandbox Comparison''; Proceedings of the IEEE Mobile Security Technologies Workshop (MoST). IEEE, 2014.

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwfw Bundesministerium für Wissenschaft, Forschung und Wirtschaft
FFG
wirtschaftsagentur wien zit Die Technologieagentur der Stadt Wien
Christian Doppler Forschungsgesellschaft
FWF Der Wissenschaftsfonds.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFW und das Land Wien gefördert. Das Programm COMET wird von der FFG abgewickelt.

InnoDB Database Forensics

Enhanced Reconstruction of Data Manipulation Queries from Redo Logs

Peter Frühwirt, Peter Kieseberg, Sebastian Schrittwieser,
Markus Huber, Edgar Weippl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

Motivation

The InnoDB storage engine is one of the most widely used storage engines for MySQL. Every executed SQL statement leaves traces for forensic analysis in different places:

- data files [1]
- database index trees [2]
- log files

Database forensic analysis can be used to

- reconstruct executed SQL queries
- create a timeline of activities
- recover deleted / manipulated data

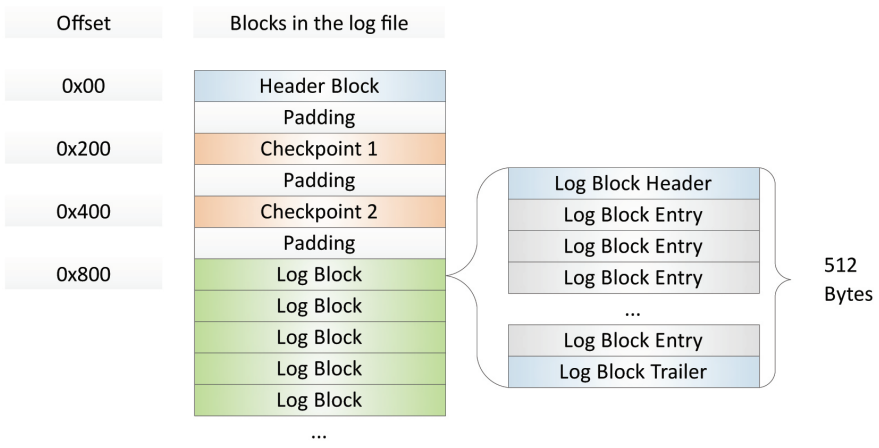


Figure 1: Structure of the log files

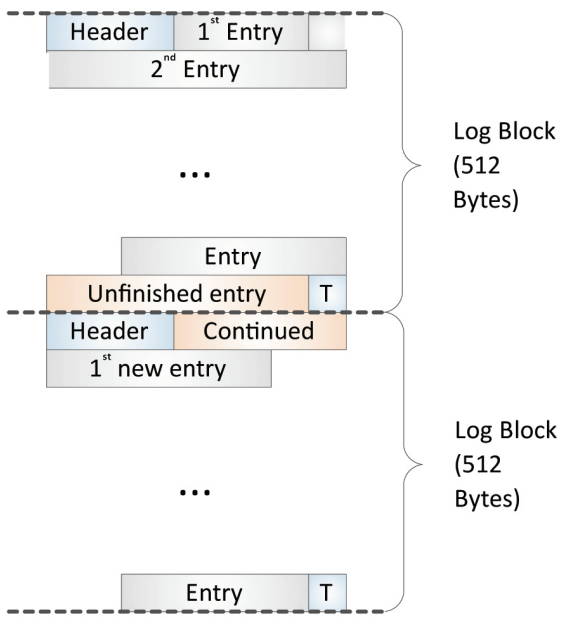


Figure 2: Log blocks with log entries

Query reconstruction

Log blocks contain different types of log entries. Every change of files will create at least one log entry. The log file is needed for transaction rollbacks and crash recovery. Depending on its type, a log entry can contain information about

- transactions
- inserted / modified / removed data
- primary keys
- metadata
- internal pointer

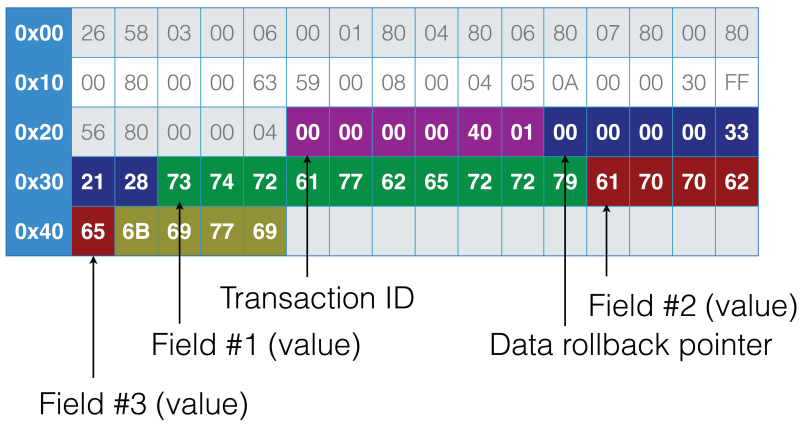


Figure 3: Query reconstruction

Evaluation

Feasibility: Prototype implementation

Challenges

- Missing documentation
- Unknown data
- Fault tolerance

Conclusion and future work

- Reconstruction of executed queries
- Deeper understanding of InnoDB internals
- Various methods of forensic analysis
- Combination of data from different locations
- Further research on InnoDB index trees

[1] Frühwirt P., Huber M., Mulazzani M., Weippl E. Innodb database forensics. In: Proceedings of the 24th international conference on Advanced Information Networking and Applications (AINA 2010); 2010.
[2] Kieseberg P., Schrittwieser S., Mulazzani M., Huber M., Weippl E. Trees cannot lie: using data structures for forensics purposes. In: Intelligence and Security Informatics Conference (EISIC), 2011 European. IEEE; pp. 282-285.

P. Frühwirt, P. Kieseberg, S. Schrittwieser, E. Weippl: „InnoDB Database Forensics: Enhanced Reconstruction of Data Manipulation Queries from Redo Logs," in Information Security Technical Report (ISTR), Special Issue: ARES 2012.
P. Frühwirt, P. Kieseberg, S. Schrittwieser, E. Weippl: „InnoDB Database Forensics: Reconstructing Data Manipulation Queries from Redo Logs," in The Fifth International Workshop on Digital Forensics (WSDF), 2012.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Lines of Malicious Code
Insights Into the Malicious Software Industry

Martina Lindorfer, Alessandro Di Federico, Federico Maggi, Paolo Milani Comparetti, Stefano Zanero

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

iseclab

Problem Outline

- Emergence of an underground economy of cybercrime: spam, identity theft, DoS, Fake AV scams
- Arms race of malware developers against security researchers
- Professional development of malware with incremental updates
  - of functionality
  - to evade AV detection
- Researchers have limited analysis resources
- Need to highlight only significant changes as focus analysis efforts

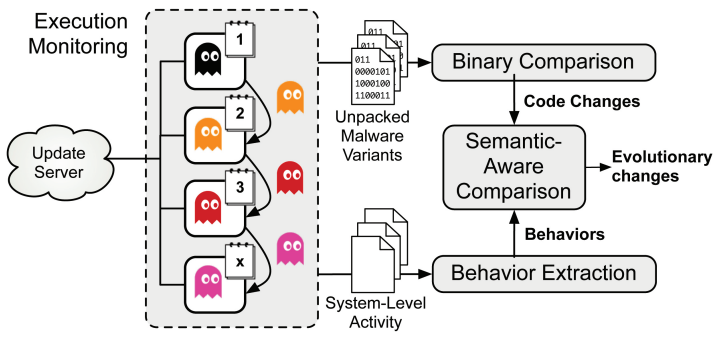


Figure 1: System overview of BEAGLE

Approach

- Identify focus of development effort of malware authors
- Take advantage of auto-update functionality in malware
- Collect subsequent updates of malware variants
- Perform combination of static and dynamic analysis to
  - Identify code changes between versions
  - Identify evolution of functional components e.g. spam, Fake AV
- Implement approach in a system called BEAGLE

Workflow of BEAGLE:

1) Run samples in dynamic analysis sandbox
2) Simulate long-term infection by keeping/restoring analysis state
3) Let samples connect to the C&C server to update
4) Find differences in binary code through static analysis
5) Map differences in binary code to dynamically observed behavior
6) Identify peaks of changes in functionality

System Details

Step 1: Execution Monitoring

- Run samples in stateful sandbox
- Dump memory to unpack samples
- Log call stack for each system call

Step 2a: Binary Comparison

- Compare memory dumps of updated malware versions
- Whitelist benign library code
- Find common subgraphs in the CFG
- Calculate code similarity based on shared/added/removed basic blocks

Step 2b: Behavior Extraction

- Express behavior as graph of system-level events connected by data flow
- Define rules for system call sequences + arguments to detect high-level behaviors

Step 3: Semantic-Aware Comparison

- Locate functions for call stack addresses
- Expand with code path between calls
- Tag functions with behavior labels

➔ Identify changes in functional components

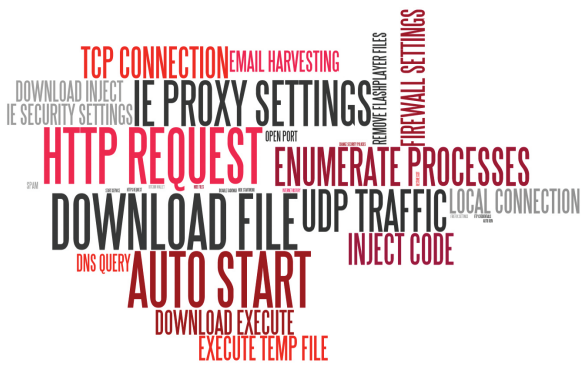


Figure 2: Behavior labels in the evaluation dataset

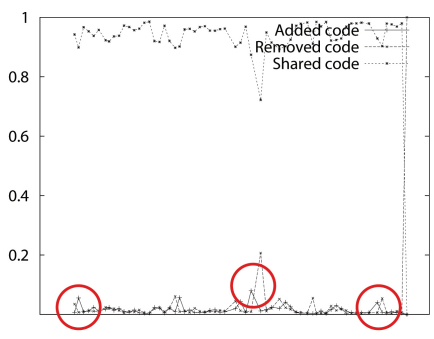


Figure 3: Amount of added/removed/shared code for a ZeuS variant with peaks of new code

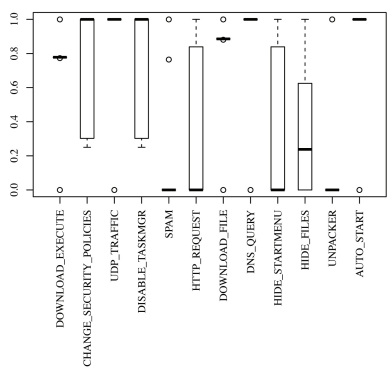


Figure 4: Behavior variability for a sample from the Gamarue family (boxes show the variance, circles represent outliers)

Evaluation Results

- Based on 16 samples from 11 different families (including 6 ZeuS banking trojans)
- One execution per sample/day from September 2011 to April 2012
- Insights:
  - Some families more actively developed than others
  - Incremental updates reuse most of the code
  - Observed peaks of new code
- We can pinpoint changes for one family over individual behaviors
- We can pinpoint changes in the malware landscape over the whole dataset

M. Lindorfer, A. Di Federico, F. Maggi, P. Milani Comparetti, S. Zanero: "Lines of Malicious Code: Insights Into the Malicious Software Industry", in Annual Computer Security Applications Conference (ACSAC), Orlando, Florida, 2012.

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwf Bundesministerium für Wirtschaft, Familie und Jugend
FFG
wirtschaftsagentur wien zit Die Technologieagentur der Stadt Wien
Christian Doppler Forschungsgesellschaft
FWF Der Wissenschaftsfonds.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Quantifying Windows File Slack in Size and Stability

Martin Mulazzani, Sebastian Neuner, Peter Kieseberg, Markus Huber,
Sebastian Schrittwieser, Edgar Weippl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

Slack Space Basics

- NTFS, e.g., with 4k cluster size, 512b sector size
  - 4 sectors per cluster
  - Approx. 700 bytes file in picture
  - Windows pads until 1024 byte

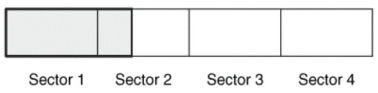


Figure 1: NTFS Slackspace Example

Slack Space: Problems

- 3TB drives are commodity hardware
- A lot of slack space
- Worse if larger cluster size
- Stable as long as not re-written

Contribution

- Quantify file slack in different versions of Windows
- Evaluate stability with regard to system updates
- Formula that estimates slack space

$$S_{(n,s,k)} = n \cdot s \cdot \mathbb{E}(X) = n \cdot s \cdot \sum_{x=1}^{k-1} x \cdot \frac{1}{k} = n \cdot s \cdot \frac{1}{k} \cdot \frac{(k-1)k}{2} = n \cdot s \cdot \frac{k-1}{2}$$

Figure 2: Contributed Formula

Experiment Design

- Different Windows versioned VM's
- Patching…Patching
- Selecting hard drive state after every reboot (update installation)
- Use of tools by fellow researchers (Garfinkel et. al) to get XML
- Measure file slack
- Detect file change by different SHA-1 hash

Results

- An average final slack space of 120MB
- Top value: Windows 7 with 450MB slack space
  - Hide passwords
  - Hide videos
  - Hide your own operating system

Operating System	Initial Slack	Final Slack	Stability
Windows XP Pro.	22.36 MB	36.97 MB (165%)	7.09 MB/31.7%
Windows XP Pro. SP2	26.31 MB	29.49 MB (112%)	16.49 MB/62.7%
Windows XP Pro. SP3	18.72 MB	23.15 MB (124%)	14.21 MB/75.9%
Vista Business	52.70 MB	147.13 MB (279%)	19.34 MB/36.7%
Vista Business SP1	66.49 MB	119.89 MB (180%)	50.77 MB/76.4%
Vista Business SP2	50.89 MB	82.99 MB (163%)	48.13 MB/94.7%
Vista Ent. SP1	66.51 MB	140.35 MB (211%)	50.82 MB/76.4%
Vista Ent. SP2	71.73 MB	113.76 MB (159%)	67.36 MB/93.9%
Windows 7 Pro.	63.71 MB	115.16 MB (181%)	46.96 MB/73.7%
Windows 7 Pro. SP1	65.03 MB	77.80 MB (120%)	60.73 MB/93.4%
Windows 7 Ent.	83.33 MB	454.62 MB (546%)	60.74 MB/72.9%
Windows 7 Ent. SP1	65.10 MB	381.56 MB (586%)	60.77 MB/93.3%
Windows 8 RC	86.40 MB	87.06 MB (101%)	65.10 MB/75.3%
Server 2003 R2 Std. SP2	24.42 MB	33.90 MB (140%)	20.13 MB/82.4%
Server 2003 R2 Ent. SP2	16.55 MB	35.13 MB (212%)	15.20 MB/91.8%
Server 2008 R2 Std.	75.16 MB	146.80 MB (195%)	57.43 MB/76.4%
Server 2008 R2 Std. SP1	69.82 MB	73.03 MB (105%)	69.19 MB/99.1%
Server 2012 RC	70.16 MB	70.58 MB (101%)	70.01 MB/99.8%

Figure 3: Result Table

Outcome

- OS files are quite static
- An average of 44MB persists after every possible update
  - That is an average of 78%
- Top values
  - Vista SP2: 67MB persist (90%)
  - Windows 7: 60MB persist (90%)
- YES: It's worth hiding!

Increasing Complexity - Increasing Files - Increasing Slack Space

Gathering Complexity: Service Packs

- E.g., Windows Vista from 35k files
  - ➔ 90k files
- So: more slack space (possibly)

Gathering slack space…

- Bigger cluster size (bigger than 4k) results in more slack space
- MORE in example:
  - 90k files: 150MB with 4k cluster size
  - 90k files: 1.25GB with 32k cluster size
- Windows Vista/7 supports up to 64k cluster size

File Type Distribution

XP Pro SP2		Windows 7 Pro		Server 2008 R2	
.dll	4414	.dll	6302	.dll	7303
.exe	1106	.mui	3906	.cat	6752
.sys	793	.est	3190	.est	4204
.inf	692	.inf	1352	.mui	3907
.pnf	674	.gpd	1303	.exe	1364
.chm	317	.exe	1067	.gpd	1303
.htm	233	.png	1051	.inf	1160
.nls	192	.cat	945	.mum	909
.jpg	186	.pnf	914	.ppd	806
…	…	…	…	…	…
∑ **11723**	**8607**	∑ **29561**	**20030**	∑ **36394**	**27708**

Figure 4: File Type Distribution

Limitations

- No user interactions
- No user software installed in VM's
  - ➔ WITH user software AND interaction:
  - ➔ More slack space (most likely)
- Only 4k cluster sizes considered

Future Work

- Survey of slack space on deployed installations
- Include other operating systems in survey
- Include other cluster sizes

M. Mulazzani, S. Neuner, P. Kieseberg, M. Huber, S. Schrittwieser, E. Weippl: "Quantifying Windows File Slack in Size and Stability," in Ninth Annual IFIP WG 11.9 International Conference on Digital Forensics, 2013.

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwfj Bundesministerium für Wirtschaft, Familie und Jugend
FFG
wirtschaftsagentur wien zit Die Technologieagentur der Stadt Wien
Christian Doppler Forschungsgesellschaft
FWF Der Wissenschaftsfonds.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Towards a Unified Penetration Testing Taxonomy

Aleksandar Hudic, Lorenz Zechner, Shareeful Islam, Christian Krieg, Severin Winkler, Richard Hable and Edgar R. Weippl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

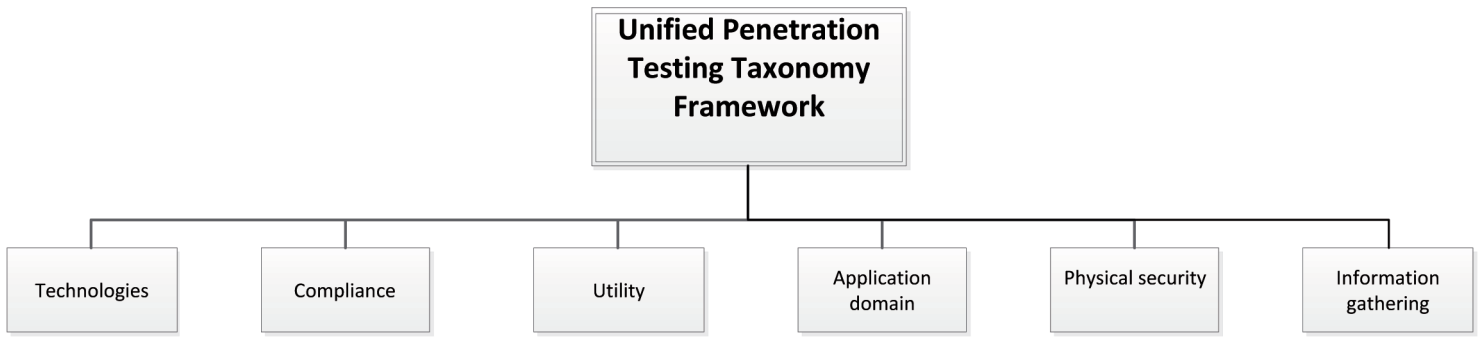


Figure 1: Unified Penetration Testing Taxonomy Framework

Framework depicts an efficient taxonomy of widespread aspects that cover the penetration testing process. It encompasses not only the technical side, but also non-technical aspects such as standards, certificates, guidelines, methodologies, etc. The framework, which is based on a tree structure, is decomposed through the subclasses (categories), which are depicted as independent trees. First, we depict the fundamental two-level structured tree, as shown in Figure 1. We developed and organized the framework and its subclasses to cover areas that relate to the penetration testing process, methodologies, standards that support the process, guidelines that instruct and conduct the testing process, certificates that enhance quality and bring trustworthiness, legal regulations that affect technology, which can all be used to provide penetration testing reports. UPTTF, shown in Figure 1, encompasses the following subclasses:

1. Technologies,
2. Compliance,
3. Utility,
4. Application domain,
5. Physical security,
6. Information gathering.

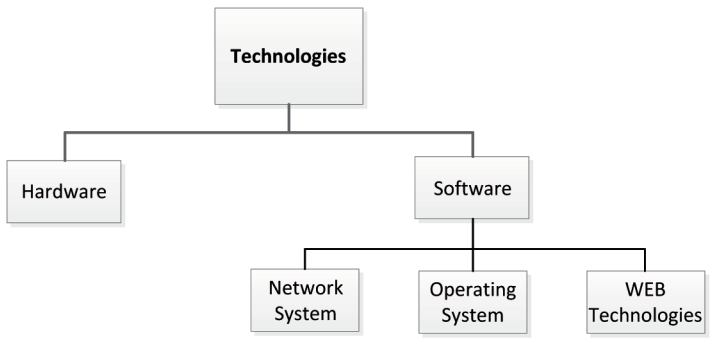


Figure 2: Technologies

The technology subclasses are a fundamental element of the penetration testing process. We distinguish two main categories: hardware and software. The technology subclass uniformly covers the taxonomy of technical (hardware and software) and non-technical areas (standards, guidelines, certificates, reporting, methodologies, etc.). The software category evaluates the taxonomy of software in detail through the tree subcategories: network system, operating system and Web technologies.

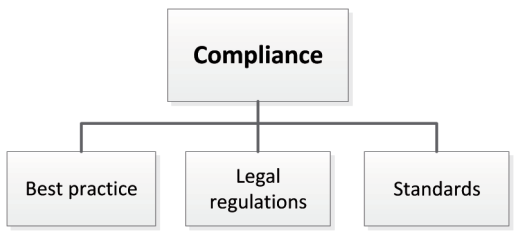


Figure 3: Compliance

The compliance subclass shows what impact different legal regulations, standards, certificates, and technical guidelines have on technological domains and demonstrates their use with different penetration testing methodologies. Furthermore, it is possible to see how one legal regulation, standard, guideline or certificate encapsulates or uses some part of another.

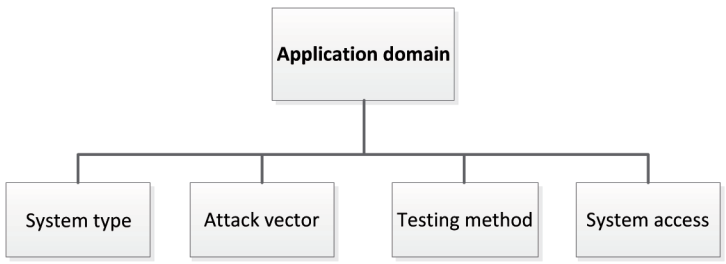


Figure 4: Application Domain

The application domain subclass reveals the form of impact (e.g., internal or external attack), type of system affected (e.g., isolated or distributed), applied methods (black-box, gray-box and white-box) and emphasize the system access point (local, adjacent or remote). Unfortunately, in most cases, it is hard to reveal the type of the system under attack, especially if it is attacked from the outside using black-box methodology.

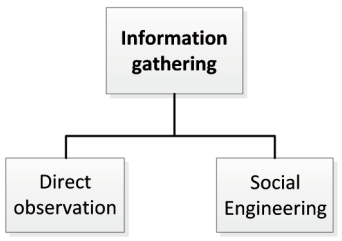


Figure 5: Information gathering

Information gathering is a crucial starting point of the penetration testing process. Before even beginning to apply any kind of test/attack, it is necessary to gather information about the system. Depending on the applied testing methodology (e.g., black-box, gray-box or white-box) the information can be revealed by the customer themselves. In this case, we are dealing with direct observation and information gathering.

Conclusion

Penetration testing is an effective way of discovering and verifying vulnerabilities present in such an information system and its overall organizational infrastructure. However, due to the inherently complex nature of the tests, it is necessary to use a systematic methodology that evaluates every possible area that presents potential vulnerabilities within the organization. Our approach presents a comprehensive unified penetration testing taxonomy focusing on issues from both the technical and the non-technical dimensions.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

AppInspect

Large-scale Evaluation of Social Networking Apps

Markus Huber, Martin Mulazzani, Sebastian Schrittwieser, Edgar Weippl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

Social networking apps

- Apps used by hundreds of millions of social networking users
- Games, horoscopes, quizzes, etc. request access to sensitive personal information (birthday, photos, email address, personal messages, etc.)
- Access to information of application user's friends

Modus operandi of apps

- Social networks simply act as proxies (iframes)
- Personal information is transferred to developers
- Developers rely on analytics & advertising products
- Custom hosting infrastructures

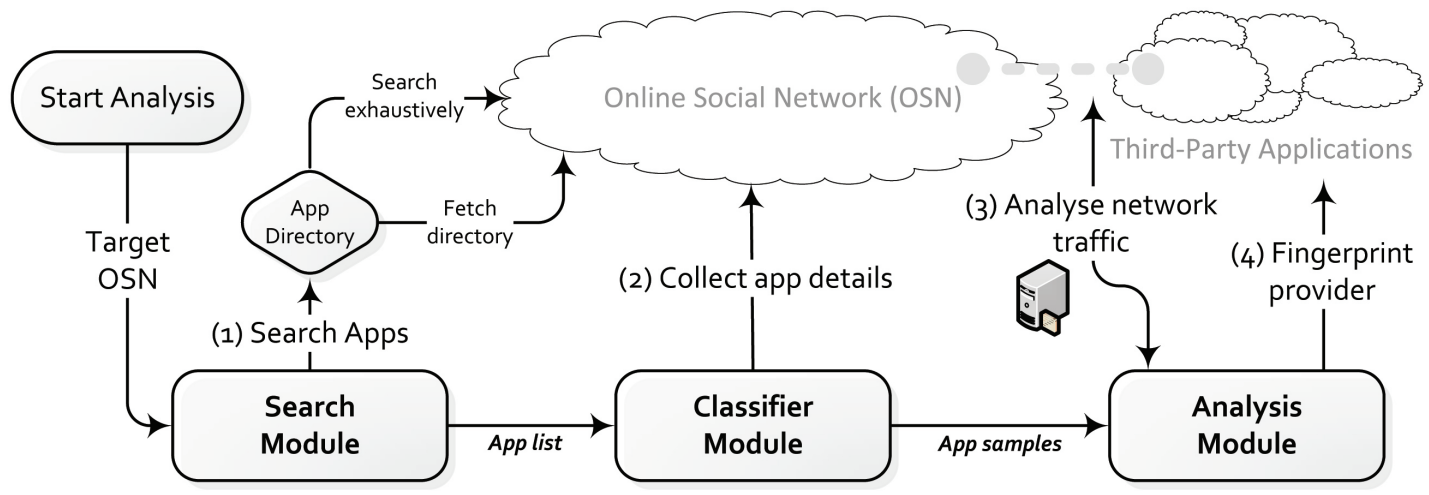


Figure 1: AppInspect, a framework for automated security and privacy analysis of social network ecosystems

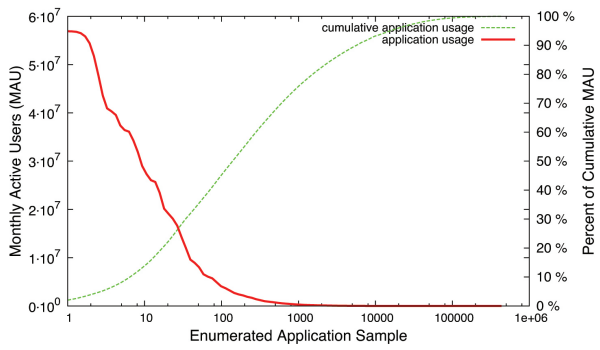


Figure 2: Sample of 434,687 unique applications (06/2012)

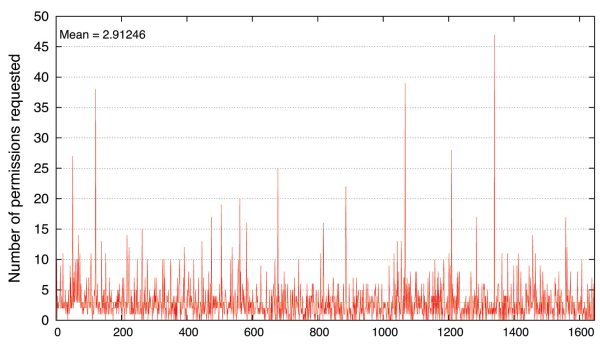


Figure 3: : Requested permissions per app provider

1 Search module

- Facebook
  - Majority of apps not in directories
  - Numeric identifier brute force not feasible (1014)
  - Exhaustive search: letter trigrams, keywords, etc.

2 Classifier module

- Application properties
  - rating, popularity, permissions, type
  - Web scraping /redirection behavior

3 Analysis module

- Traffic collection
  - Applications are installed on test accounts
  - HTTP(S) proxy collects network traffic
- Web tracker identification
  - Detection of analytics and advertising products
- Information leaks
  - Leakage of personal data, auth tokens
- Hosting infrastructure fingerprint
  - Fingerprint the underlying hosting infrastructure
    Detected services against vulnerability database

4 Results

- Facebook prototype on 4,747 apps
  - 139 different Web tracking and advertising products
  - 315 apps transferred personal information
  - 51 apps leaked personal information/tokens
  - Reported our findings to Facebook in November 2012
- Hosting
  - Number of hosts possibly vulnerable
  - FTP/SSH brute force
- Implications
  - 60% of application developers request email address
  - Social phishing, context-aware spam
  - Users trackable with real name

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwfj Bundesministerium für Wirtschaft, Familie und Jugend
FFG
wirtschaftsagentur wien zit Die Technologieagentur der Stadt Wien
Christian Doppler Forschungsgesellschaft
FWF Der Wissenschaftsfonds.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Cloudoscopy: Services Discovery and Topology Mapping

Amir Herzberg, Haya Shulman, Johanna Ullrich, Edgar Weippl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

Motivation

Cloud computing services allow scalable and efficient sharing of resources. Resources like computing or networking are allocated when needed on a pay-per-use basis. This advantage is predominant for its growing popularity. Thereby, placement of virtual instances in clouds and resource sharing raises security and trust concerns. We focus on aspects related to security threats which stem from network sharing among tenants:

- Scouting the cloud's topology,
- discovery of services resident in clouds, and
- address deanonymization.

We evaluated these security threats on four leading commercial clouds: *Amazon EC2*, *Rackspace Cloud*, *Microsoft Azure* and *Google Compute Engine*.

Hop Count Measuring

Native diagnosis tools, e. g. *traceroute*, are typically disabled in cloud environments for camouflage. We have shown that the reconstruction of the path between the attacker and the victim is nevertheless feasible:

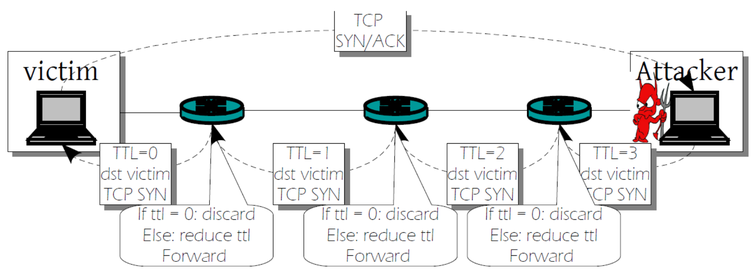


Figure 1 : Hop Count Measuring via TTL-based Scan

E-Mail Server Discovery

Some protocols enable specific address deanonyimzation:

- *Internal Address Block Scan:* The attacker sends e-mails to external addresses from a cloud-based instance and awaits responses. Limitation:
- *External Server-Bounce Scan:* E-mails are sent to random e-mail addresses from an external instance, but the sender address is spoofed. Due to undeliverability, ''bounce'' messages are returned to the spoofed address -- an internal e-mail server.

Address Deanonymization

Background

NICs generate interrupts to notify the kernel of packet arrival:

- Suspension of current task in exchange for interrupt handling
- Processing received packet and invoking respective protocol
- Significant CPU overhead due to context switching
- Other tasks reach starvation during high traffic load

Attack Scenario

Address deanonymization means the correlation of an instance's public address with its private one. By probing the victim's internal address, patterns are introduced into the communication flow. The attacker is looking for these patterns at the victim's external address.

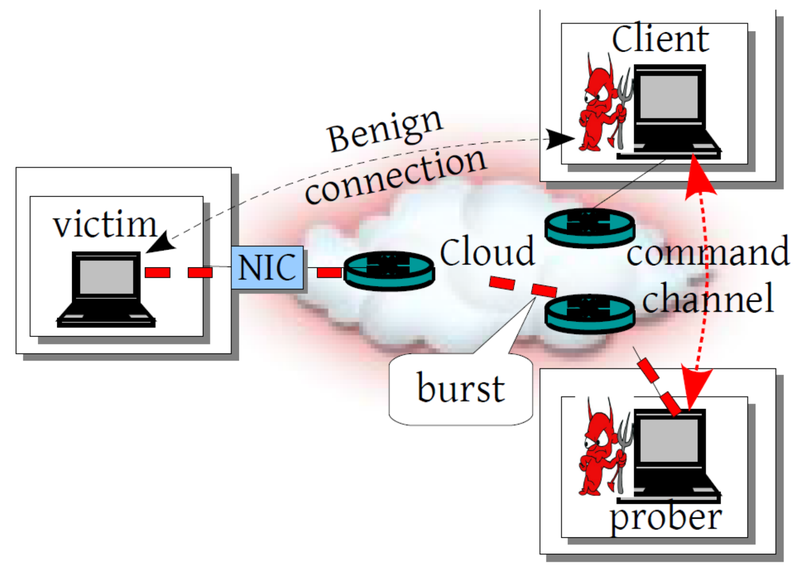


Figure 2 : Attack Scenario

Results

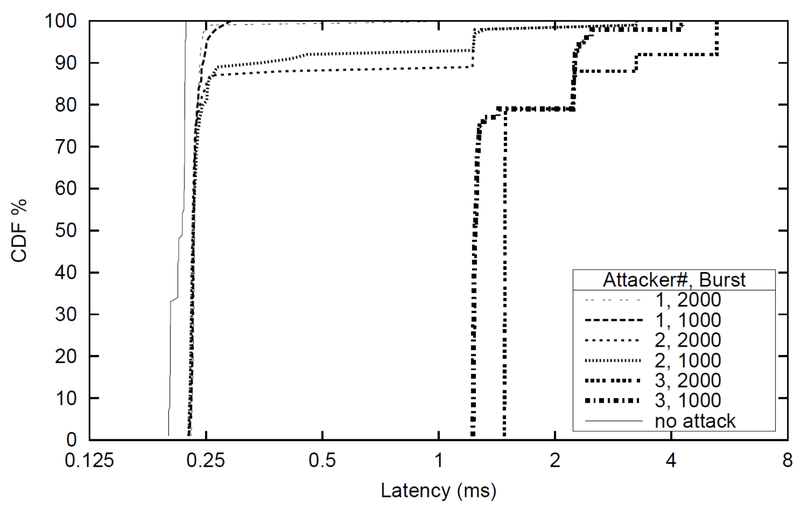


Figure 3 : Latency Caused by Bursts

Conclusion

- Resource sharing provides attack surface in cloud environments.
- Private addresses can be inferred from public ones by exploiting hardware interrupt processing or protocol-specific functionality.
- Camouflaging like prohibiting *traceroute* can be circumvented.

Due to exploiting functionality inherent to networking, mitigation is not easy, but *Blocking cloud-internal traffic*, *the provision of a dedicated NIC per virtual instance* or *rate limiting* are able to prevent some of the proposed attacks.

Amir Herzberg, Haya Shulman, Johanna Ullrich, and Edgar R. Weippl. Cloudoscopy: Services discovery and topology mapping. In *Proceedings of the ACM Cloud Computing Security Workshop (CCSW) at ACM CCS 2013*, 11 2013.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFW und das Land Wien gefördert. Das Programm COMET wird von der FFG abgewickelt.

Dark Clouds on the Horizon: Attacks on Cloud Storage Systems

Martin Mulazzani

Competence Centers for Excellent Technologies
www.ffg.at/comet

secure
sba-research.org

Cloud Storage & Efficiency

- **Naïve approach for cloud storage: data deduplication**
  - Client-side data duplication: no need to upload popular files, saves bandwidth
  - Server-side data deduplication: only store a single copy of each file
- **Can save a lot of storage capacity & bandwidth**
- **Novel attack vector if not properly implemented**
- **Dropbox as well-known service in particular was vulnerable**
  - Operates on Amazon Simple Storage
  - 50 million+ users
  - Billions of files

Attack No.1: Hash-in-the-Middle Attack

- **Local hash computation manipulated**
- **Can result in unauthorized file access if hash value is known**
- **Can be used for stealth data exfiltration or highly efficient P2P data transfers**

Attack No.2: Online Slack Space

- **Hide data without linking to any account by reversing the communication protocol**
- **Can allow attacker to use unlimited storage space**
- **Could be used to counter forensic investigations, no local data traces**

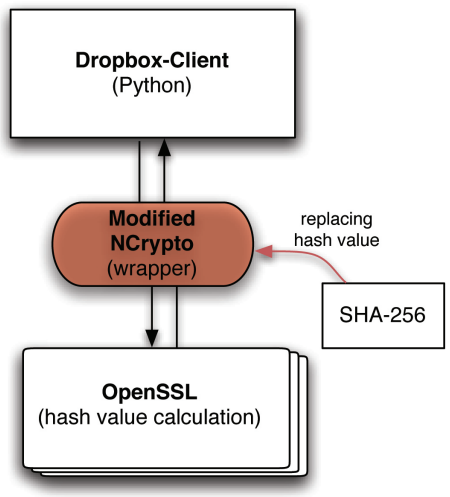


Figure 1: Hash Value Manipulation Attack

Evaluation

- **Evaluated if popular files from BitTorrent are stored on Dropbox**
  - Checked for top 100 from thepiratebay.org as of middle of Sept. 2010
  - Approx. 97% of files were stored on Dropbox
- **Evaluated how long files are stored in Online Slack Space**
  - Half of all files that were uploaded without linking survived > 3 months
- **Measure the time span for file undeletion**
  - Files that were linked to an account were not deleted for > 6 months

Category	Quantity
Application	3
Game	5
Movie	64
Music	6
Series	29
Sum	107

Table: Categories of .torrents

File	$h(f)$	Hitrate	Hitrate rel.
.torrent:	107	106	99%
.nfo:	53	49	92%
others:	208	201	97%
In total:	368	356	97%

Table: Files found on Dropbox

Countermeasures

- **Client cannot be trusted for hash value calculation**
  - Simple fix: upload every file, no client-side data deduplication
- **Cryptographic or interactive probabilistic data possession protocols**
- **Interactive protocol:**
  - Multiple challenge-response rounds
  - Clients are challenged by the server
  - Calculate, e.g., hash values of random subsets
- **Dropbox was notified and vulnerabilities were fixed**

Future Work

- **Compare and evaluate data possession proof protocols & methods**
- **Find the most efficient scheme in terms of communication and computational overhead**
- **Check other popular services for hash manipulation vulnerability**

M. Mulazzani, S. Schrittwieser, M. Leithner, M. Huber, E. Weippl: "Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space," in USENIX Security, 2011.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Browser Identification with Javascript Engine Fingerprinting

Martin Mulazzani

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

Problem Description

- UserAgent string is used to identify browser version
- Can be easily manipulated, not a security feature
- Web page appearance and malware rely on UserAgent anyway
- Motivated by nmap for operating systems (TCP/IP fingerprinting)

Javascript Engine Fingerprinting

- Employ Javascript conformance test for ECMAScript 5.1: test262
- More than 11,000 test cases
- Testset used to distinguish a browser from others
- Calculate minimal fingerprint to accurately identify browser

Web Browser	15.4.4.4-5-c-i-1	13.0-13-s	S15.2.3.6_A1	10.6-7-1	S10.4.2.1_A1
Opera 11.61	✓	✗	✗	✗	✗
Firefox 10.0.1	✓	✗	✗	✓	✗
Internet Explorer 9	✗	✓	✗	✗	✓
Chrome 17	✗	✗	✓	✗	✓
Uniqueness u	2	1	1	1	2

Figure 1: Browsers fail in different test262 test cases

Building a Decision Tree

- Most efficient way to test unknown user's browser
- Can be in O(log n) instead of O(n) for even further performance enhancements
- Collected more than 150 browser & operating system combinations for fingerprinting
- More than 95% of most popular Web browsers of the last three years covered

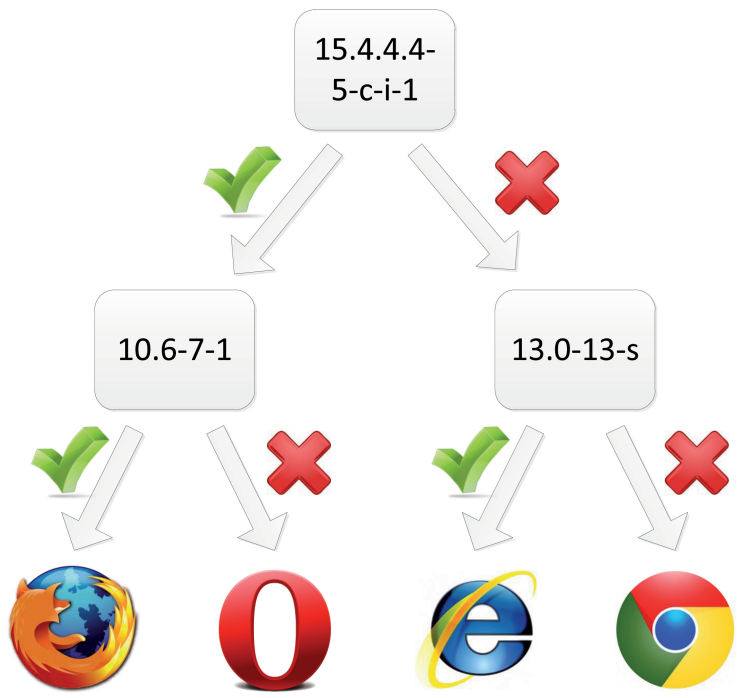


Figure 2: Exemplary Decision Tree for Current Browsers

Evaluation

- Survey with 190 participants
- Testset consisted of the four most common browsers
- 100% detection rate within the testset, no false positives
- 90ms on average for PCs, 200ms for smartphones

Future Work

- Expand experiments to mobile browsers as they become more common
- Assess if advertisement companies /malware already use Javascript fingerprinting
- Build a detection environment as browser extension or proxy server

Conclusion

- Previous work relied on normalized time pattern
- Our method is three orders of magnitude faster
- Could be used to enhance session security (with or without SSL)

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Guess Who's Texting You?

Evaluating the Security of Smartphone Messaging Applications

Sebastian Schrittwieser

COMET
Competence Centers for Excellent Technologies
www.ffg.at/comet

secure
sba-research.org

Mobile Messaging Applications

- Aim at replacing traditional text messaging (SMS) and GSM/3G calls
- Free phone calls and text messages over the Internet
- Novel authentication concept
- Phone number used as single authenticating identifier
- We tested nine applications for Android and iOS (e.g., WhatsApp)

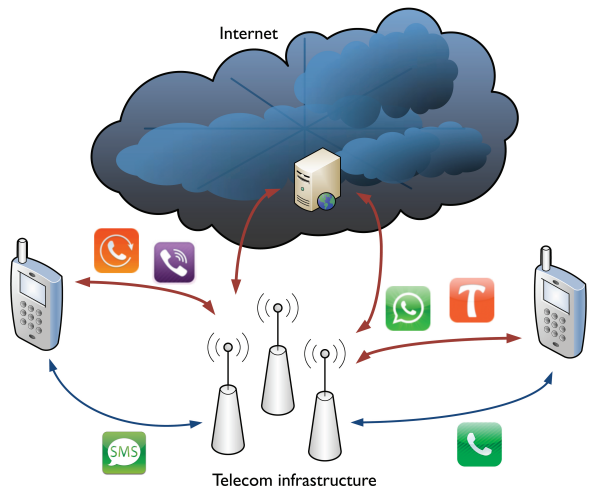


Figure 1: Traditional SMS_talk (blue) vs. Mobile Messengers (red)

Motivation

	Traditional SMS/talk	Mobile messengers
Protocol	proprietary	HTTP(S), XMPP
Security	cryptographically sound authentication (SIM card)	depends on application; much weaker authentication (phone number, IMSI, UDID)
Users' perception	SMS/talk	

Methodology

- Authentication mechanism and account hijacking
- Sender ID spoofing / message manipulation
- Unrequested SMS / phone calls
- User enumeration
- Modifying status messages

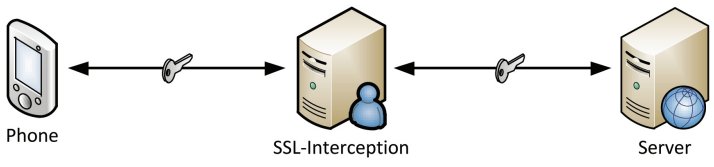


Figure 2: Experimental Setup

Experimental Setup

- Samsung Nexus S running Android 2.3.3 and Apple iPhone 4 running iOS 4.3.3
- SSL proxy to read encrypted HTTPS traffic
- Used to understand the protocol, not for the actual attack (i.e., man-in-the-middle between victim and server)!

	Account Hijacking	Spoofing/ Manipulation	Unrequested SMS	Enumeration	Other Vulnerabilities
WhatsApp	yes	no	yes	yes	yes
Viber	no	no	yes	yes	no
eBuddy XMS	no	no	yes	yes	no
Tango	yes	no	yes	yes	no
Voypi	yes	yes	yes	yes	yes
Forfone	no	yes	yes	yes	no
HeyTell	yes	no	no	limited	no
EasyTalk	yes	no	yes	yes	no
Wowtalk	yes	no	yes	yes	yes

Figure 3: Results

Results for WhatsApp

- **Account Hijacking**
  - SMS verification used to validate phone number
  - Code is generated on the phone and can be intercepted with SSL proxy
  - Allows hijacking of arbitrary WhatsApp accounts
- **Status Messages**
  - No authentication required for updating status message
  - Allows changing the status message of arbitrary WhatsApp accounts
- **User Enumeration**
  - Application uploads the user's address book to the server
  - Server compares the contained phone numbers to already registered phone numbers
  - Server returns a subset list containing only phone numbers that are registered
  - User base enumeration possible by uploading the entire number range

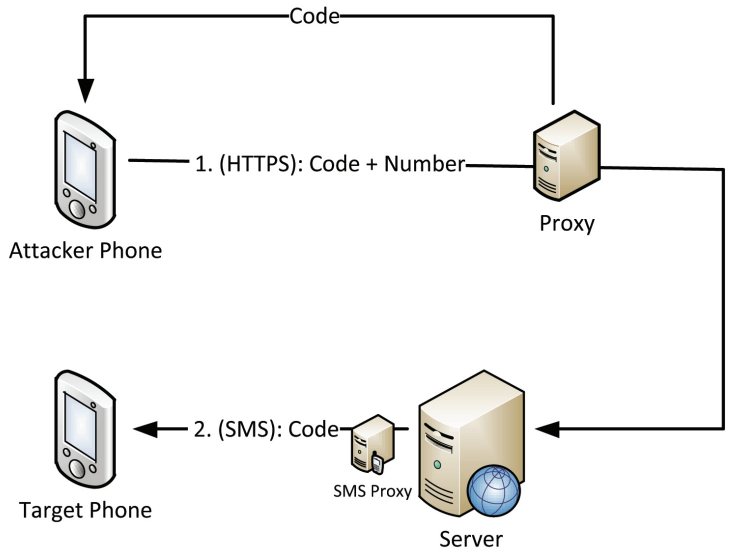


Figure 4: Account Hijacking in WhatsApp

Conclusion

- 6 out of 9 tested applications have broken authentication mechanisms
- Many other vulnerabilities
- All identified flaws stem from well-known software design and implementation errors
  - Trusting the client
  - No input validation
  - Weak or no authentication mechanisms

S. Schrittwieser, P. Frühwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, E. Weippl: "Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications," in Network and Distributed System Security Symposium (NDSS 2012), 2012.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Improving OS Security through Domain Separation

Manuel Leithner

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

State of OS security

Professional exploit developers and operating system vendors are caught up in an arms race, driving the price of exploits up and resulting in no effective security gain for end users despite massive investments. Exploit mitigations such as ASLR, DEP/NX, AntiROP, AppArmor and Application Sandboxes are routinely broken weeks after release. On the other hand, strict OS hardening would decrease usability - for instance, W^X on anonymous memory tends to break multimedia applications and strongly obfuscated programs such as Skype along with exploits relying on this technique.

Principles

- Accept exploitation
- Contain effects
- Remove persistents

Approach

- Split the system into domains
  - Drivers
  - Storage
  - Multimedia
  - Mail/Chat
  - Code signing
  - Web browsing (red domain)
- Restrict domains
  - Harden kernels, add capabilities on need-to-have basis
  - Dedicated domain as choke point for networking
  - Data exchange between domains only on user request
- Make it usable
  - Common display for GUIs of different domains
  - Streamline data exchange without compromising security
  - Disposable domains for small tasks (such as opening PDFs)

Red domain

- Untrusted domain for high-risk applications
- Least privilege
- Common use: Web browsers

Implementation

- Xen-based
- Network driver domain: Controls physical networking devices, common routing/filtering/capture point
- Storage domain: Contains shared package manager database, synchronized storage and handles removable media
- Internet access only for domains ‘Red Domain’, ‘Mail/Chat’ and ‘Storage’
- Transient VMs: Held in RAM only, no persistence whatsoever
- Dom0-driven integrity verification of domain base image before boot

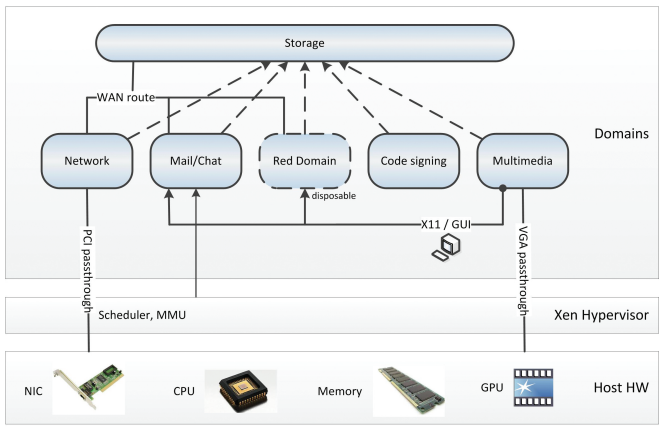


Figure 1: System Overview

Based on Qubes OS

- Storage domain: Contains common read-only file system base and per-domain modifications
- Domains share X11 screen, visually separated
- Disposable VMs: Single-use domains for document viewing

Hardware requirements

- VT-x/AMD-V hardware virtualization
- VT-d/AMD-Vi IOMMU, prevents DMA attacks
- Xen VGA passthrough

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

IMSI-Catch me if you can: IMSI Catcher Catchers

Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, Manuel Leithner, Edgar Weippl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

Problem and Motivation

- **IMSI Catchers** identify and eavesdrop on mobile phones
- Recently, number of vendors rose and prices plunged
- Self-made devices have been presented for US$ 15,000
- IMSI Catcher audience is not limited to law enforcement agencies anymore
- No numbers on unofficial or non-governmental use of IMSI Catchers exist

Background

- IMSI Catchers perform an active radio attack
- IMSI Catchers leave artifacts in network structure
- This project puts forward multiple ways to detect such devices.

Methodology

10 artifacts caused by IMSI Catchers have been identified

- Frequency usage
- Cell ID and location
- Base station capabilities
- Network Parameter
- Cell register forcing attacks
- UMTS downgrading
- Encryption
- Cell imprisonment
- Traffic forwarding
- Usage pattern

Detection platform

- Artifacts (10) and corresponding detection methods (12) have been examined for implementability on different platforms
- Mobile devices
  - Android offers standard API support for 7 of 12 detection methods
  - iOS offers only private API for baseband information and had to be excluded
- Stationary
  - We designed a network of stationary measurement units for long time data collection.
  - Several GSM/UMTS modems (USB/Serial) were surveyed
  - Telit modules offer best support for 9/12 detection methods

Mobile IMSI Catcher Catcher

- Android application
- Uses standard API
  - Runnable on abroad number of devices
  - Does not require root privileges
- Collects neighbor cell data in proximity of the user
- Simple warning system for end users

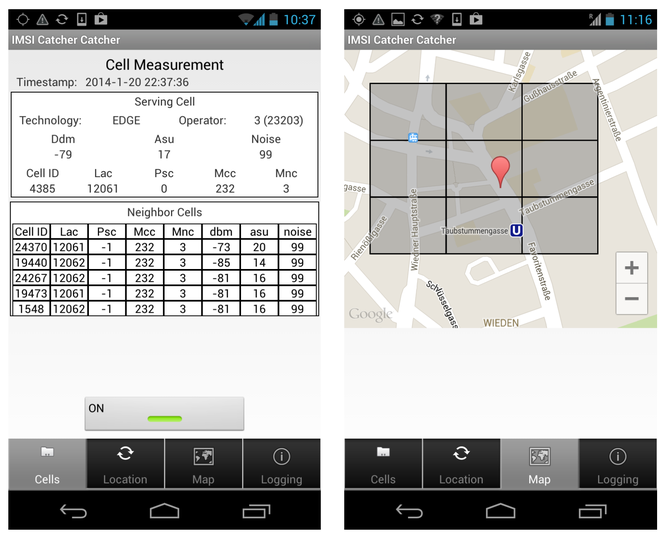


Figure: Screenshots

Stationary IMSI Catcher Catcher

- Fixed mounted measurement unit (e.g. on rooftops)
- Based on RaspberryPI and Telit GPRS Modules
- Internet uplink via WiFi or cable
- Scans all GSM 900 and GSM 1800 frequencies every 5-7 minutes

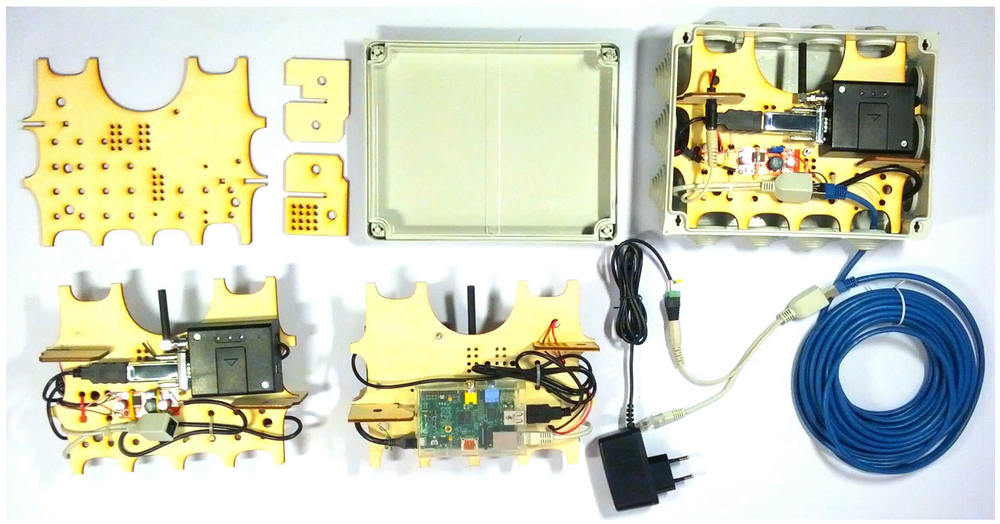
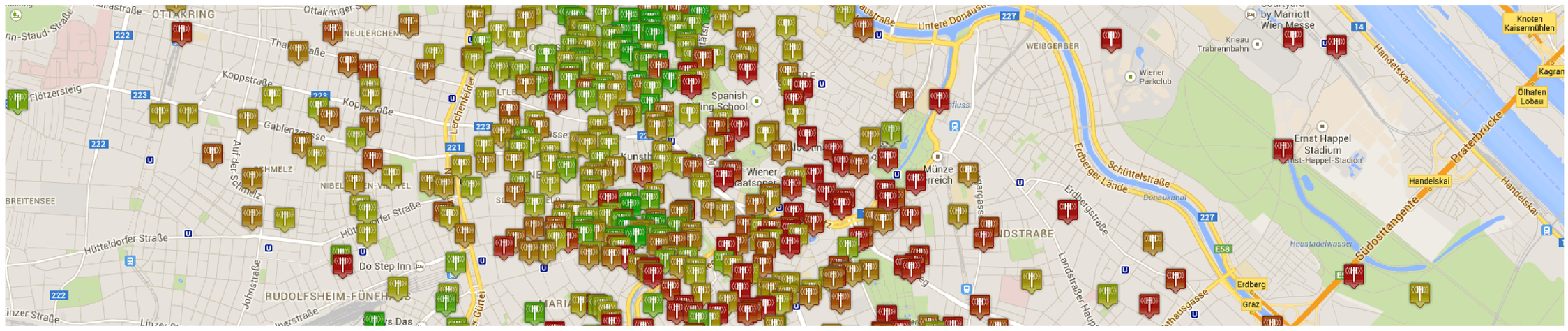


Figure: Station construction using laser cut parts



IMSI-Catch Me If You Can: IMSI-Catcher-Catcher; 2014; Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, Manuel Leithner, Edgar Weippl; under review

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFW und das Land Wien gefördert. Das Programm COMET wird von der FFG abgewickelt.

Malware in Silicon II

Adrian Dabrowski, Heidelinde Hobel, Katharina Krombholz, Peter Fejes, Lorenz Zechner, Edgar Weippl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

Introduction

Hardware Trojans are used to introduce malfunctions or change the behavior in a concrete way (hostile takeover)

For example:

- Leakage of secret information or encryption keys from servers, mobile devices or military applications (e.g., via so-called side-channels).
- Manipulation of smart meters or other metering systems.
- Disturbance of monitoring tasks for critical and dangerous processes, e.g., in airplanes, cars, elevators, household, and kitchen appliances.

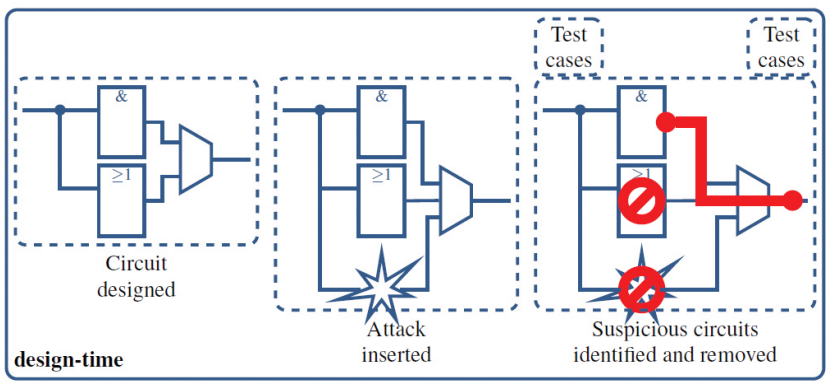


Figure 1: Technique for detecting and removing Trojans according to [1]

Motivation

- As a decreasing number of electronics manufacturers can afford their own chip production, it is outsourced to third parties in other countries, thus increasing the risk of having the design compromised.
- A chip designer needs a way to verify the integrity of its design before and after production.
- Typically, Trojans are only activated by a special trigger, which makes their detection an even greater challenge.
- Chip Graffiti (Fig. 2) – a non-functional modification by the chip or mask designer for artistic purposes – suggests that functional modifications might also go unnoticed.

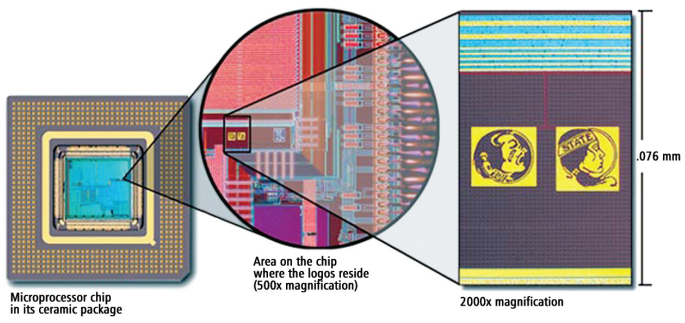


Figure 2: Some IC designers see it as a sport to perpetuate themselves on commercial ICs by inserting artistic non-functional modifications into the design [2]. Hence, the question arises whether this knowledge can be used to insert functional modifications, such as Trojans.

Malware Testing Framework

- As real-world examples are rarely published due to image considerations, we designed our own testing framework and Trojan construction set.
- Interchangeable modules allow us to test different aspects of Trojans independently, e.g., a specific trigger against several detection methods.

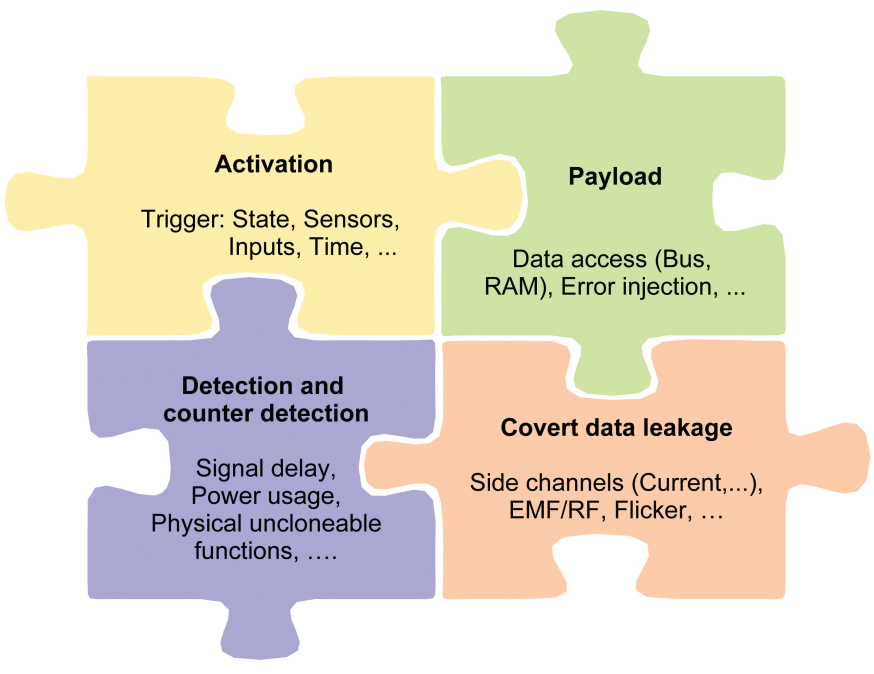


Figure 3: Our Trojan testing framework comprises four mostly interchangeable building blocks and is implemented and tested on FPGAs

Secure Development Life Cycle

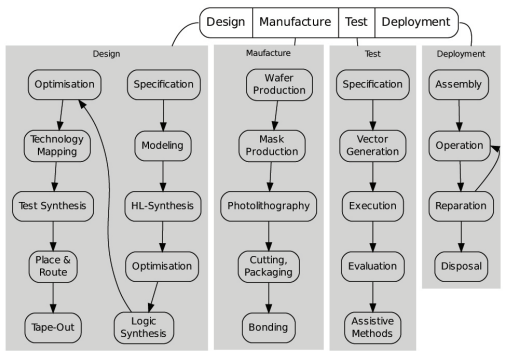


Figure 4: Development phases prone to unauthorized modifications

This project aims to develop a secure development life cycle to ensure the security, confidentiality, and integrity of designs.

Conclusion

- Hardware Trojans are an emerging threat due to the decentralization of the production chain.
- Research into hardware security is still at an early stage compared to the awareness for software security, which is already widely established.
- Guidelines are required for ensuring a trusted production chain (secure development life cycle)

[1] M. Hicks, M. Finnicum, S. King, M. Martin, J. Smith; Overcoming an Untrusted Computing Base: Detecting and Removing Malicious Hardware Automatically. In Security and Privacy (SP), 2010 IEEE Symposium on. 159-172.
[2] H. Goldstein; The Secret Art of Chip Graffiti, IEEE Spectrum article on chip artwork, Volume: 39, Issue: 3, Mar 2002, pp. 50-55.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

QR Code Security – Why Apps are Unable to Protect the User against Malicious QR Codes

Katharina Krombholz, Peter Frühwirt, Ioannis Kapsalis,
Johanna Ullrich, Markus Huber, Edgar Weippl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

Problem & Motivation

- QR Codes are used to make information instantly accessible (e.g. billboard advertising, monetary transactions)
- Problem: The human eye is not able to decode QR codes. Therefore, the users ultimately depend on software to verify the encoded content.
- QR codes are used as attack vector for phishing attacks.
- Are QR code reader applications able to protect the users from phishing attacks?

Figure 1: Example QR code sticker used in the experiment

Evaluation of QR Code Readers

We evaluated the 12 most popular QR code reader apps for Android, iOS and Windows Phone.
We identified **additional functional features** such as synchronization amongst devices or price comparison that may require the transmission of user-related sensitive data. Then we investigated **security protection mechanisms** provided by the reader apps to protect the user against attacks. Additionally, we monitored information exchanged between the app and corresponding external services via an HTTP(S) interception proxy to identify **privacy violations**. Our findings show that **most QR code reader apps are unable to protect the users against phishing** and **significantly violate their privacy**. Many apps leak information to external parties even though it is not required by the additional functional features.

Intercultural Comparative User Study

To determine **cultural differences in security awareness**, we simulated phishing attacks with QR codes as attack vector. The QR codes were deployed in highly frequented urban spaces and had a link to an online survey encoded. The study was conducted in 4 European cities: **Athens, Helsinki, Paris** and **Vienna**. Among others, we found that

- French users **scan QR codes significantly more often** than Finns (t-test, probability of error $p = 0,043$) and Austrians (t-test, probability of error $p = 0,03$).
- In Paris, more than 70% of the participants **perceived our QR codes as fishy or reported to always be skeptic when scanning QR codes**. In comparison to that, less than 30% of the participants from Athens had doubts on the trustworthiness of our QR code stickers. (t-test, probability of error $p = 0,05$).

App	Modification Detection	Website Analysis	URI Display
Scan	No	No	No
Barcode Scanner	No	No	Yes
RedLaser	No	No	Yes
Bakodo	No	No	Yes
QR Droid	No	No	Yes
Quick Scan	No	No	Yes
ShopSavvy	No	No	No
QR Code Reader	No	No	No
Qrafter	No	Yes	Yes
ScanLife	No	No	No
i-nigma	No	No	Yes
AT&T Code Scanner	No	No	No

Table 1: Security features provided by QR code readers

App	External Communication	User Tracking	Location Data
Scan	Yes	Yes	No
Barcode Scanner	No	No	No
RedLaser	Yes	Yes	Yes
Bakodo	Yes	Yes	Yes
QR Droid	Yes	Yes	No
Quick Scan	Yes	No	No
ShopSavvy	Yes	Yes	Yes
QR Code Reader	No	No	No
Qrafter	Yes	No	No
ScanLife	Yes	Yes	Yes
i-nigma	Yes	Yes	No
AT&T Code Scanner	Yes	Yes	Yes

Table 2: Privacy violations of QR Code readers

Conclusion

- We conducted an **extensive vulnerability analysis** on the QR code processing chain.
- We showed that on the one hand, **users are not aware of the associated risks** and reader apps are **not able to protect the user** against QR code based attacks.
- We are currently developing a framework to make QR code processing on mobile devices both **secure and usable**.

Sang Kil Cha, Thanassis Avgerinos, Alexandre Rebert, and David Brumley. Unleashing mayhem on binary code. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, SP '12, pages 380--394, Washington, DC, USA, 2012. IEEE Computer Society.
Kevin Coogan, Gen Lu, and Saumya Debray. Deobfuscation of virtualization-obfuscated software: a semantics-based approach. In *Proceedings of the 18th ACM conference on Computer and communications security*, CCS '11, pages 275--284, New York, NY, USA, 2011. ACM.
Cullen Linn and Saumya Debray. Obfuscation of executable code to improve resistance to static disassembly. In *Proceedings of the 10th ACM conference on Computer and communications security*, CCS '03, pages 290--299, New York, NY, USA, 2003. ACM.
Andreas Moser, Christopher Kruegel, and Engin Kirda. Limits of static analysis for malware detection. In *23rd Annual Computer Security Applications Conference (ACSAC 2007), December 10-14, 2007, Miami Beach, Florida, USA*, pages 421--430. IEEE Computer Society, 2007.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFW und das Land Wien gefördert. Das Programm COMET wird von der FFG abgewickelt.

Reflections on Privacy Considerations in Social Media

Katharina Krombholz, Dieter Merkl, Edgar Weippl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

Motivation

- Social networks such as Facebook, Twitter, Google+ have become a mass phenomenon in recent years (Facebook: 901 million monthly active users in March 2012)
- User-generated content: Web 2.0 paradigm shift – users not only as consumers but also as producers of content
- Self-presentation and disclosure vs. privacy and data security
- Complex information sharing model leads to leakage of sensitive information
- Risks associated with lack of privacy: stalking, mobbing, identity theft, price discrimination and many more

The Facebook Social Engineering Experiment

- Goal: To infiltrate existing friendship networks with 8 fake profiles
- Simulation of a socialbot network
- Socialbot network = botnet that controls fake profiles
- Data collection: Qualitative data and quantitative data that describe interactions with other users and Facebook user data of the participants' profiles
- As a result, we determined human factors for a successful attack
- The figure to the right shows the friendship network of one of our fake profiles

The Focus Groups

- Goal: A deeper understanding of the observations from the Facebook social engineering experiment to strengthen the results and to learn about the participants' privacy considerations
- Discussion with friends of our fake profiles (students that went to the same high school as listed by 3 of the fake profiles)
- Summary of results: The young people were mostly aware of the risks associated with weak privacy configurations. Most of them knew how to lock out particular audiences. However, almost all of them were friends with at least one fake profile and explained how they perceived those profiles.

The Survey

- Sample size n = 212
- Goal: To measure and compare disclosure and privacy considerations

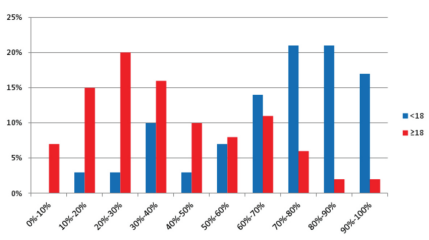


Figure 2: the reported percentage of friends that the participants meet more than 5 times a year.

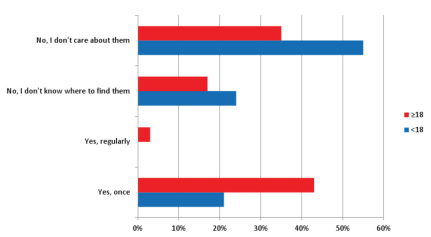


Figure 3: the reported answers to the question whether they had read Facebook's legal terms and data security guidelines.

Contribution

We studied different aspects of privacy in social media, as well as the impact of excessive disclosure on privacy leaks. Furthermore, we studied the effectiveness of social engineering in social media by conducting an experiment with fake profiles on Facebook.

- How do Facebook users treat their personal data on the platform?
- How much do they trust the platform and their interaction partners?
- Why is social engineering in social media so effective?
- What strategies do they follow to protect their privacy?

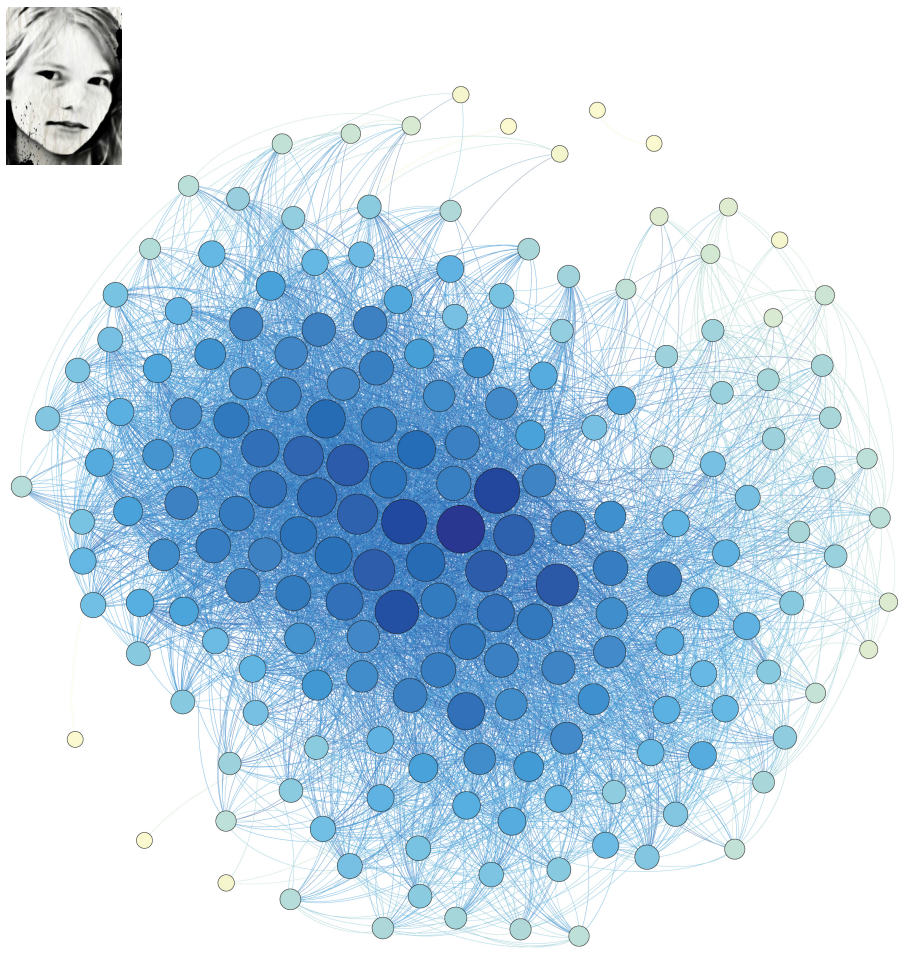


Figure 1: The friendship network and profile picture of Melissa, where size and color of any chosen node indicate the node's degree. A high density means many mutual friends in the network.

Conclusion

- Facebook users are aware of privacy-related issues. However, their behavior mostly does not map the level of awareness, as people tend to behave differently than they perceive they do.
- Social engineering is effective; the effectiveness is strongly determined by human factors and the social attractiveness of a profile.
- Social attractiveness is highly correlated with the number of interactions with other users.
- Mutual friends, same location and same educational information are more likely to influence the establishment of a friendship relation than, e.g., the same interests.

K. Krombholz, D. Merkl, E. Weippl: „Fake Identities in Social Media – A Case Study on the Sustainability of the Facebook Business Model" in Journal of Service Science Research (JoSS), Springer, Vol 4 2012, pp. 175-212.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Security Analysis of Metropolitan Locking Systems Using the Example of the City of Vienna

Adrian Dabrowski, Gilbert Wondracek, Wolfgang Kastner

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

Introduction

In Vienna, 92% of residential buildings are equipped with a system that allows access for postal delivery, emergency services and maintenance personnel via a device in the front door intercom. The mechanical key is currently available under the counter from many locksmiths for €10-20. Since 2006, house owners can replace the old mechanical BG key by an RFID-based system named "BEGEH".
BG is used in Vienna and several other cities in eastern Austria.

Analysis

1) Normal user cards can easily be read out, but require a card simulator for exploitation because they are UID-dependent.
   We built one ourselves for €20.
2) A specific card type (Baucard) can be manufactured from any compatible transponder, such as an old ski ticket.
3) Cards have low UID entropy.
4) The blacklist feature is not updated frequently enough to be effective.

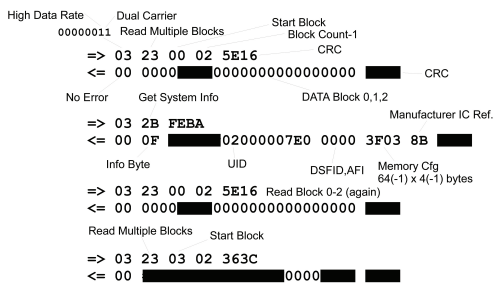


Figure 3: Transmission dump

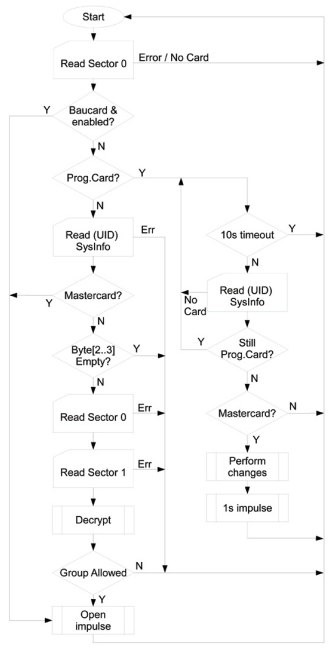


Figure 4: Reconstructed model of inner workings – basis for further tests

Experiment

In an experiment, we put a midrange RFID reader into a post package and sent it to a building equipped with the BEGEH system. We successfully recorded the key. Later, we used the gained data with a card simulator.

Figure 5 : Card skimmer

Motivation

The large circulation of "Z" or "BG" keys makes many people uncomfortable

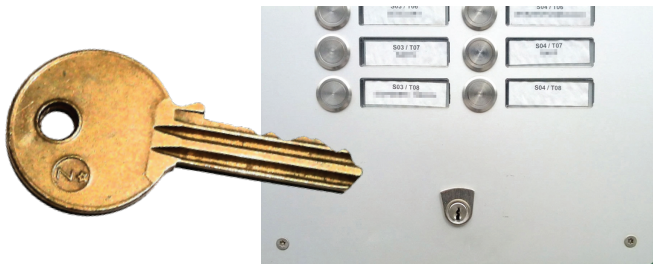


Figure 1: Mechanical BG key and lock in a door intercom

The new system promises more control: Only accredited companies are handed RFID keys. The house owner can allow certain user groups (e.g., postal service) but deny others (e.g., advertising).

Figure 2: RFID-based BEGEH card and reader device

Contribution

Build a sniffing and simulation device for this card system.

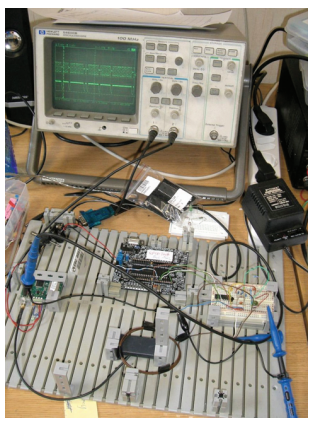


Figure 6: Measuring station and simulator prototype

We also found several weaknesses in UID key distribution and encryption of other locking systems and electronic purse products.

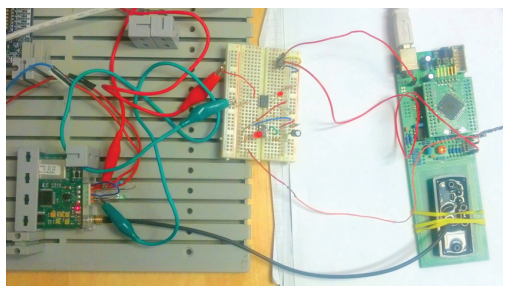


Figure 7: Fuzzing and brute forcing of RFID reader device

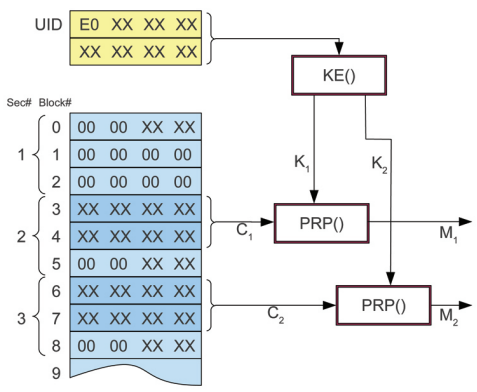


Figure 8: Model of key data structure and encryption

Field Test

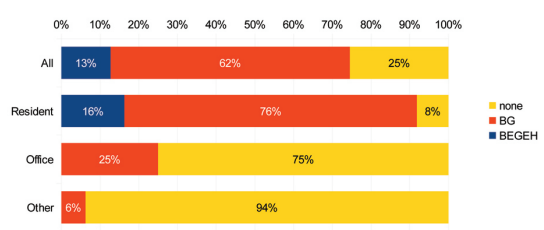


Figure 9: Results: 16% of residential buildings in Vienna had switched to the electronic RFID system by the end of 2012. (n=110)

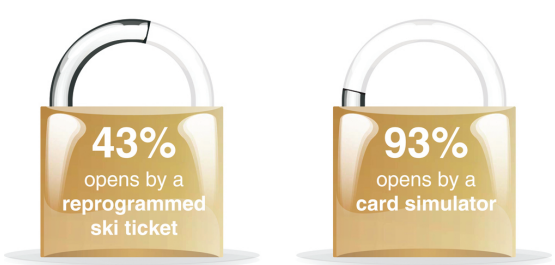


Figure 10: Of these RFID installations, 43% can be opened using a manipulated ski ticket and 93% by simulating a post access card or fire brigade card.

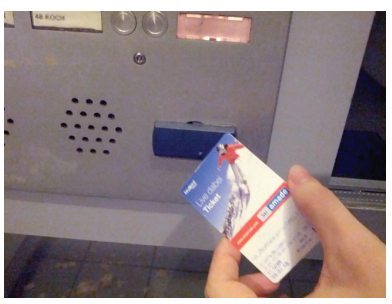


Figure 11: Opening a building entrance using an old reprogrammed ski ticket.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Security of Patched DNS

Amir Herzberg, Haya Shulman

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

Defenses Against Cache Poisoning

The defenses against cache poisoning by off-path attackers, RFC 5452, are based on challenge-response mechanisms:

- DNS resolver incorporates challenges in the query that it sends to the name server, and the name server is expected to echo those challenges back in the DNS response
- Upon receipt of a DNS response, the resolver validates that the challenges are identical to those sent in the request

Source Port Randomization

The most popular challenge-response mechanism is source port randomization

- increases the search space to 2^{32}
- additional (popular) defenses are query and IP randomization
- Most popular port assignment, standardized in RFC6056, is a per-destination port selection. Supported by popular OS, e.g., Linux kernel

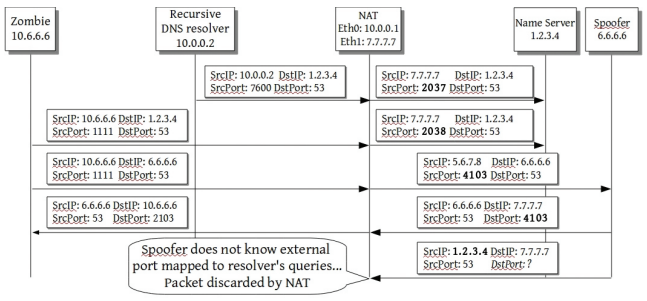


Figure 1: Per-destination port allocation method

Attack Steps

Experimental Evaluation

- Per-destination random (iptables Netfilter 2.6)
- Preserving (Cisco IOS)
- Random (Cisco ASA)
- Windows XP ICS
- Free BSD

Attack Steps:

- Hole punching in the NAT: send a UDP packet to the name server.
- The off-path attacker sends a packet to each destination port with source IP of the name server. The payload contains the destination port.
- One packet gets through: forward this packet to the attacker.

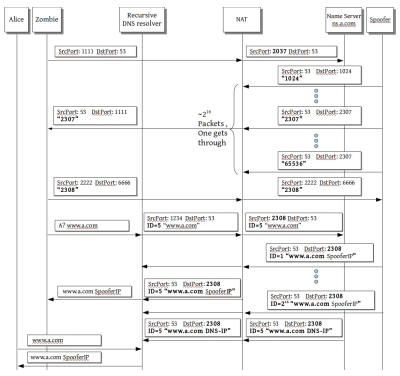


Figure 3: Source port derandomization for resolver behind-NAT scenario

IP Address Randomization

Top level domains have 6 name servers on average (Figure 4)
Add entropy to DNS requests by selecting the IP of name server at random
Validate that response arrives from correct IP.

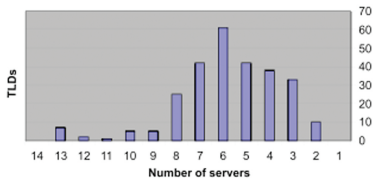


Figure 4: Distribution of IPs among TLDs

Source Port Derandomization

We found techniques to circumvent the port randomization by off-path attackers. Our techniques rely on the use of network address translation (NAT) devices; see Figure 2

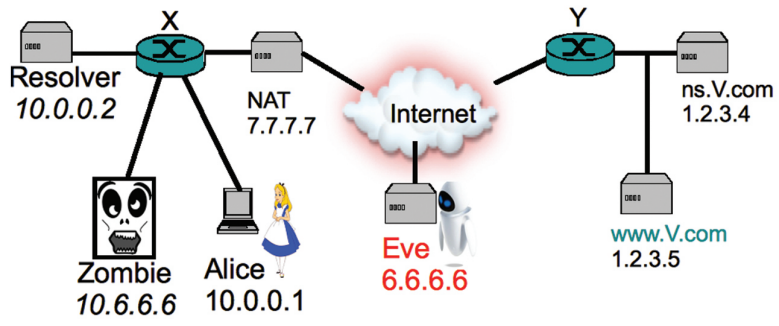


Figure 2: Scenario and attack model

Our techniques allow the reduction of the entropy in a DNS request to 2^{16} bits, and nullify the protection offered by the anti-poisoning defenses.

IP Address Derandomization

IP address derandomization holds against resolvers compliant with RFC 4697

- avoid querying non-responsive name servers.

Attack idea: use fragmentation to ruin DNS responses.
Cause timeout and retransmission of DNS requests at resolver.
As a result, the resolver marks the name server as non-responsive and avoids sending DNS requests to it.

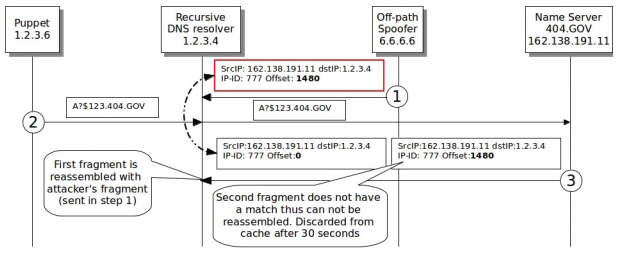


Figure 5: IP address derandomization via seconf fragment spoofing.

Conclusions

Our results show that relying on non-cryptographic defenses for security of DNS is risky.
We present techniques that allow to circumvent the defenses, and expose the DNS resolvers to attacks.
Our main message to raise awareness to the importance of adoption of DNSSEC.

A. Herzberg, H. Shulman: "Security of patched dns," in Computer Security–ESORICS 2012, pp. 271–288, 2012.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Social Snapshots: Digital Forensics for Online Social Networks

Markus Huber

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

Research problem

- **Data extraction from online social networks (OSNs)**
- **Current approaches and their shortcomings:**
  - State-of-the-art: custom Web crawler
  - No metadata (e.g., timestamps)
  - Incomplete (e.g., private messages)
  - High maintenance due to website layout changes
  - Social snapshots: novel method for reliable data extraction

How it works

- **Automated Web browser injects custom OSN third-party app**
  - Web automation: Java + Selenium Framework + Firefox
  - Custom app: PHP + modified Facebook Graph API SDK
- **Prototype, based on free software, for Facebook**
- **Provide credentials or hijack user session**

Evaluation

- **Feasibility: Implementation**
- **Implementation challenges**
  - PHP app: SDK threading support (performance)
  - Email: OCR challenge, evade crawler detection
  - Automation: Selenium cookie authentication
- **Testbed**
  - Client: Xubuntu, Firefox 3.6
  - Server: Ubuntu Server, Apache2
- **Collected data**
  - 25 Facebook accounts
  - Test subjects provided credentials

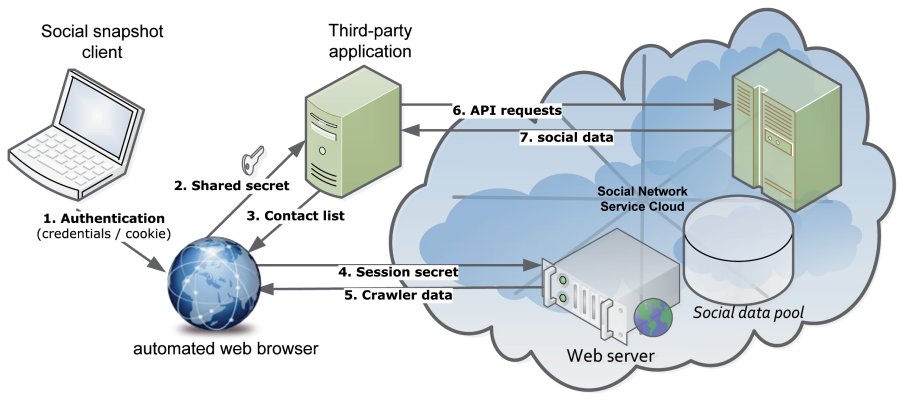


Figure 1: Social snapshot application framework

First results

- **Social snapshots provide**
  - More information than Facebook's download feature
  - Complete Facebook account data
- **Extraction takes less than 15 minutes per account**
- **Facebook does not detect or block our tool**

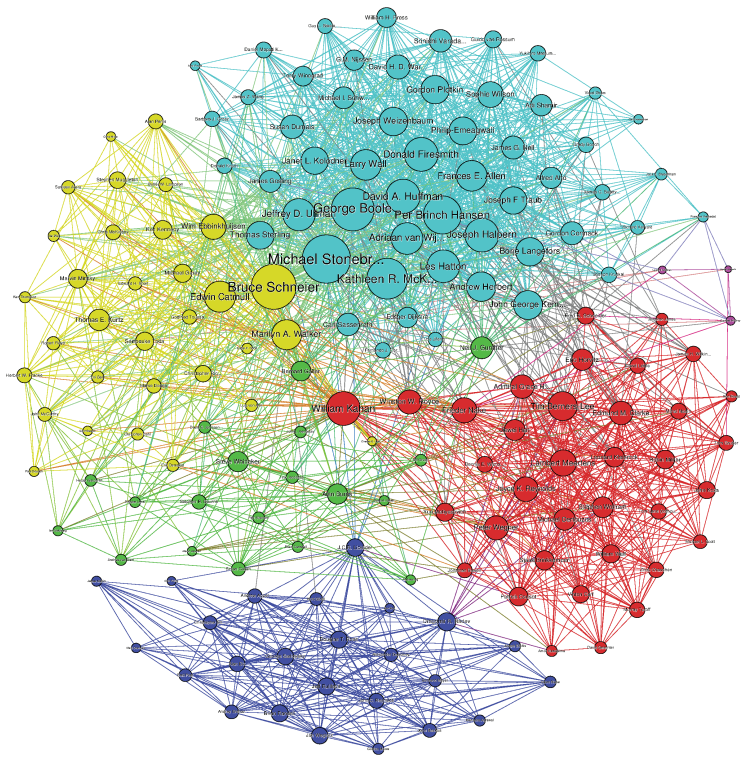


Figure 2: Anonymized social interconnection graph

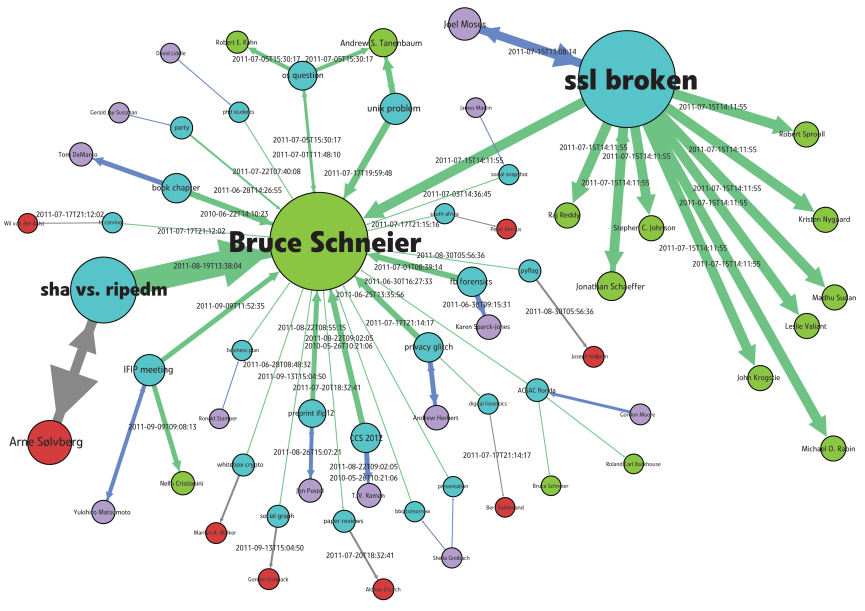


Figure 3: Anonymized example of user inbox

Conclusion and future research

- **Open source, available for download**
- **Full paper and more information:** http://socialsnapshots.nysos.net
- **Give our tool a try:** http://is.gd/snapshotsurvey
- **Current research**
  - Automatic analysis of social snapshots
  - Visual representation of data
  - Reliable storage and analysis of social snapshots

M. Huber, M. Mulazzani, M. Leithner, S. Schrittwieser, G. Wondracek, E. Weippl: "Social Snapshots: Digital Forensics for Online Social Networks," in Annual Computer Security Applications Conference (ACSAC), 2011.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Stealth DoS Attacks on Secure Channels

Amir Herzberg, Haya Shulman

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

Ensuring Performance with Anti-Replay Window

IPsec uses an anti-replay mechanism to provide performance guarantees to applications above it.
The anti-replay window size of IPsec was never analyzed, and its default size was arbitrarily set to 64K.
In this work we study the impact of an incorrectly adjusted anti-replay window on TCP connections.
We assume that a man-in-the-middle attacker is located between two gateways and can inspect the traffic that traverses the gates, see Figure 1

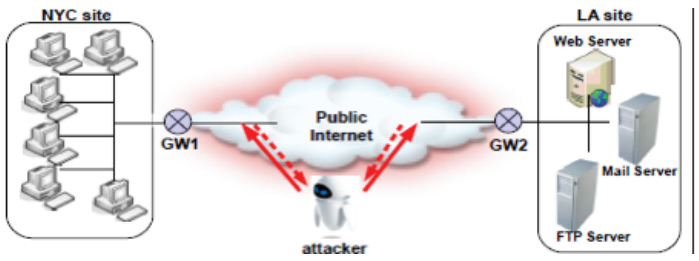


Figure 1: Scenario and attacker model.

Motivating Anti-Replay Window

We show that when the anti-replay window is not correctly adjusted, the attacker can degrade performance of TCP connections by applying packet reordering or by duplicating packets.

- Why use an anti-replay window? If no window is used, attacker can duplicate and replay legitimate packets. This compromises correctness and also results in degradation of service for TCP connections.

Calculating Anti-Replay Window Size

How to adjust the anti-reply window of IPsec to prevent the attacks?
Let d_{MIN} be the minimal delay on the network, e.g., d_{MIN}=0, assume this is the attacker's rate. Let d_{MAX} be maximum delay. Attacker can set delays to all packets in the interval $[d_{MIN},d_{MAX}]$. Let R bytes/sec be the transmission rates, let L_{MIN} bytes be the minimal packet size, and let W be the IPsec anti-replay window size, i.e., maximum number of packets.
Then IPsec will not discard packets if the following holds: $W \geq \frac{R(d_{MAX}-d_{MIN})}{L_{MIN}}$

Attack on Small Anti-Replay Window

- Why not use a very large anti-replay window? Not efficient!
- Use arbitrary size anti-replay window? Degradation of service attack :
  1. Attacker reorders 3 packets
  2. TCP reduces sending rate

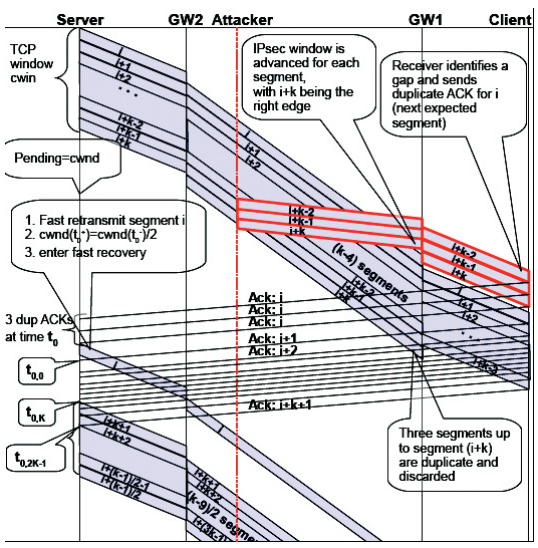


Figure 2: Duplicate packets reduce throughput of TCP connections.

Attack on Correctly Adjusted Anti-Replay Window

We show that even a correctly adjusted IPsec window does not prevent all attacks, and the attacker can still reorder packets (Figure 3).

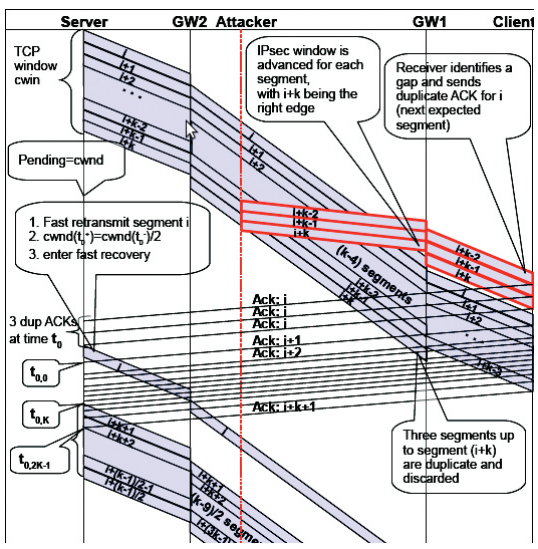


Figure 3: Attack on correctly adjusted IPsec anti-replay window.

Countermeasures

The gateway should reorder the packets and pass them in order to the receiving end host
This design prevents benign reordering as well as malicious attacks
However requires processing and maintaining state at the gateway

Conclusions

Networks experience benign and malicious reordering.
The impact on throughput of TCP connections may be devastating.
We showed: IPsec Anti-Replay window does not ensure performance.
Thus alternative mechanisms should be investigated: we presented firewall based design to ensure performance to TCP flows.

[1] A. Herzberg and H. Shulman. Stealth DoS Attacks on Secure Channels. In Proceedings of the 17th Annual Network and Distributed System Security Symposium (NDSS'10).

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

User-friendly Secure Mobile Environments

Georg Merzdovnik, Markus Huber, Christoph Hochreiner,
Peter Aufner, Alexej Strelzow, Edgar Weippl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

secure sba-research.org

u'smile

Mobile Application Security

Research Challenges:

- Apps use sensitive personal information (e.g. location information)
- Pervasive applications pose challenges to security (Internet of Things)
- No easy interfaces for end users to assess security

Collaboration

- Josef Ressel Center for User-Friendly Secure Mobile Environments
- Joint research with FH Hagenberg
- Industrial partners: A1 Telekom Austria AG and LG Nexera Business Solutions AG

Location Privacy

Motivation

- Applications access sensitive location information
  - e.g. a weather app does not need to know your exact position, the current city would probably be enough
- Application developers have little incentive to protect user privacy

Mobile Location Obfuscation

- Obfuscate location before it is sent to the server
- Categorisation of applications to determine location granularity and usable obfuscation algorithm
- Implementation of proxy- and system interception based approaches

  Proxy based: can be deployed on network level, no need to modify the device, can not intercept all traffic

  System based: can intercept location-method calls, needs root privileges on device, harder to set up for multiple devices

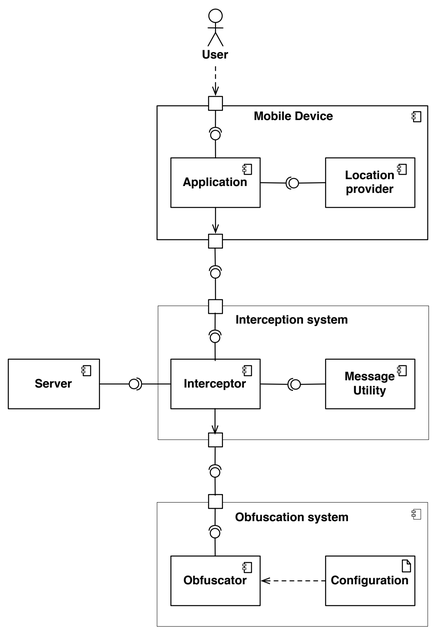


Figure 1: Proxy architecture

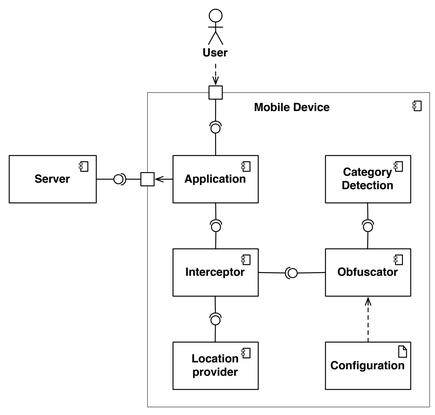


Figure 2: System interception architecture

Results

- Evaluation based on top-free Android applications
- Obfuscation techniques are feasible for mobile location obfuscation

Secure Middleware

Motivation

- Mobile devices are becoming the central point of ambient computing
- Middleware provides easy means to develop applications
  - But: also introduces new security concerns (Plug-in, App-Permissions)

Plug-in & Application Analysis

- Extending Ambient Dynamix with plug-in/application analysis
  - Assert application permission use
  - Analyse plug-ins regarding used/allowed methods

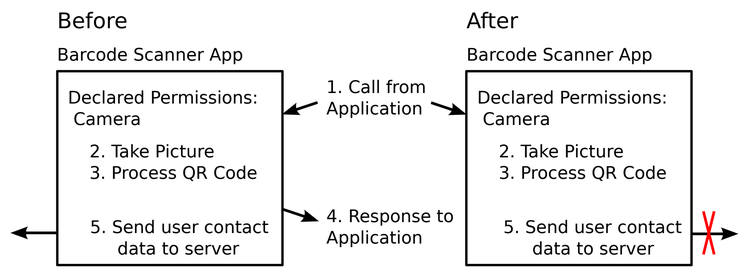


Figure 3: Asserting permissions of plug-ins

Mobile Malware Self-Check Interface

- Integration with dynamic analysis sandbox "Andrubis"
- Allows users to assess the threat level of downloaded applications

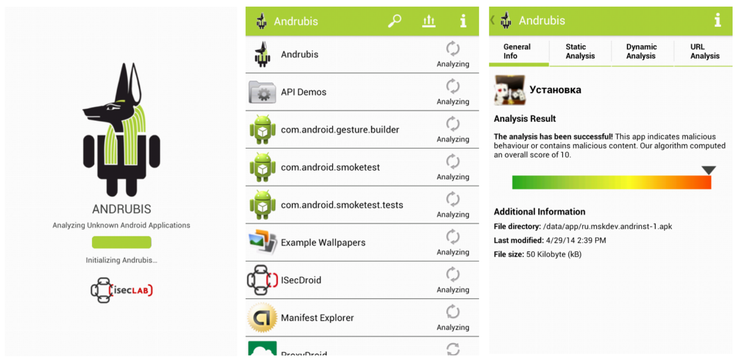


Figure 4: Andrubis self-check submission application

Ongoing & Future Research

- Extension of library swapping capabilities on rooted devices
  - Increase users privacy through secure/privacy preserving libraries
- On-device dynamic security analysis of applications
- Extending privacy in Internet-of-Things (IoT) applications
- Analysing and improving App-to-App communication methods

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwfw Bundesministerium für Wissenschaft, Forschung und Wirtschaft
FFG
wirtschaftsagentur wien zit Die Technologieagentur der Stadt Wien
Christian Doppler Forschungsgesellschaft
FWF Der Wissenschaftsfonds.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFW und das Land Wien gefördert. Das Programm COMET wird von der FFG abgewickelt.

Using Generalization Patterns for Fingerprinting of Partly Anonymized Microdata

Sebastian Schrittwieser and Peter Kieseberg

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
secure sba-research.org

k-anonymity and fingerprinting

k-anonymity

- Sensitive data needs to be anonymized for further processing.
- Properties that can be linked to identify a person uniquely are called quasi-identifiers (QI).
- The k-anonymity criterion is satisfied if each record is indistinguishable from at least k-1 other records with respect to the quasi-identifiers.

Fingerprinting

- For fingerprinting, intrinsic attributes of data are utilized to discover unauthorized disclosure.
- No additional ''marks'' are added that could be removed.
- It is important to use attributes that lie deep inside the data, i.e., can only be removed by drastically reducing the value of the data.

Generalization of quasi-identifiers

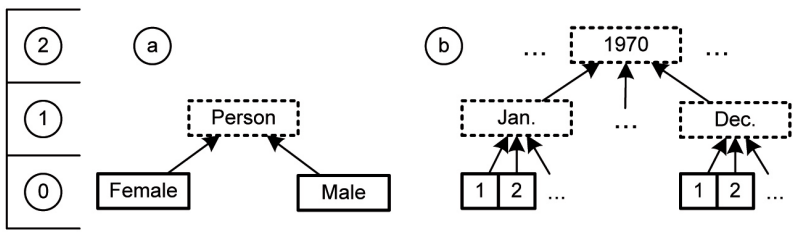


Figure 1: Generalization of quasi-identifiers

- The quasi-identifiers can be generalized to several granularity levels.
- Possible generalization levels depend largely on the nature of the data and requirements specified by the user.
- Combinations of different granularity levels result in a multitude of generalization strategies for a given data set.

Utilizing k-anonymity for fingerprinting

Solution outline

- A minimum anonymity level k is chosen.
- All possible data generalizations featuring an anonymity level of at least k are calculated.
- The solutions are clustered with respect to the data precision, i.e., we use *data quality* as primary clustering criterion to ensure fairness in data distribution.

Data precision metrics

- In general, anonymization reduces the data quality.
- Data precision metrics measure the information loss for a given generalization.
- The choice of the metric can have a great effect on the rating of a generalization, so qualitative analysis on the impacts of different data precision metrics and eventual optimal solutions are still needed.

Example

Detecting data breaches

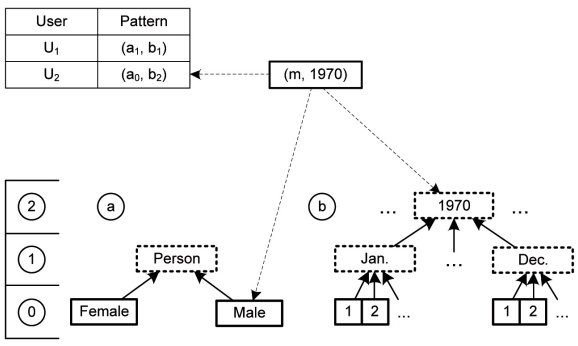


Figure 2: Detecting data breaches

Data setup

- For original data containing the quasi-identifiers ''birthdate'' and ''sex'', two generalization strategies G_0 and G_1 are constructed and assigned to the users U_0 and U_1, respectively.
- In case the record (m, 1970) is encountered, the owner of the data can detect the security leak at user U_1 using only the structure of the data.

Further Work

Work on new data precision metrics

- Evaluate existing data precision metrics and their shortcomings
- Define new metrics that cater to special needs
- Improve the grouping algorithms for defining equivalency classes

Practical application and forensics

- Implementation of a prototype of the algorithms as a proof-of-concept
- Development of an open-source real-world solution
- Advanced forensic recovery of data

S. Schrittwieser, P. Kieseberg, I. Echizen, S. Wohlgemuth, N. Sonehara, E. Weippl: "An Algorithm for k-anonymity-based Fingerprinting," in International Workshop on Digital-forensics and Watermarking (IWDW 2011), 2011.
S. Schrittwieser, P. Kieseberg, I. Echizen, S. Wohlgemuth, N. Sonehara: "Using Generalization Patterns for Fingerprinting Sets of Partially Anonymized Microdata in the Course of Disasters," in Workshop on Resilience and IT-Risk in Social Infrastructures (RISI 2011), 2011.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

Visualization of simulated cyber attacks exposed by the Thales Hypervisor Framework

Peter Kieseberg, Alexej Strelzow

COMET
Competence Centers for Excellent Technologies
www.ffg.at/comet

secure
sba-research.org

Project Overview

Short Summary

Cybercrime is a known rising threat for national and international businesses. Once an attack has been spotted, time becomes the crucial factor for initiating countermeasures. This simulation addressed this very threat and visualized the impact of cyber attacks on routers of the Austrian backbone net, its subnets and the business within. The attack scenario was developed together with the security expert Wolfgang Czerni and was simulated with a modified version of the Thales Hypervisor Framework.
It was presented at the security congress "KSÖ Sicherheitskongress 2012" in Vienna, Austria.

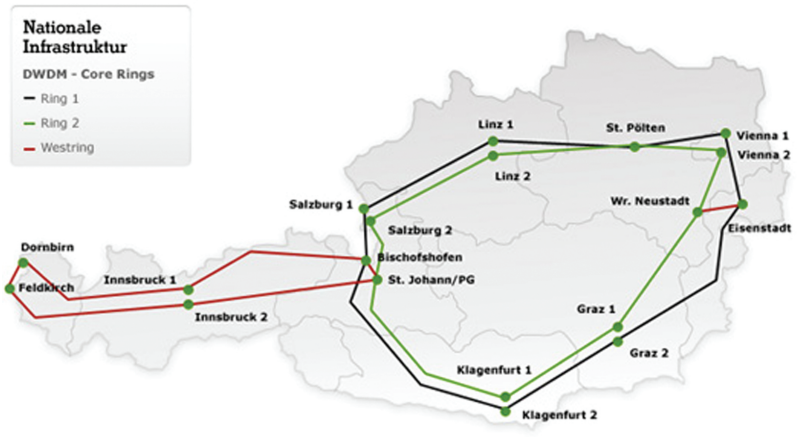


Figure 1: Fiber channel backbone net of Austria.

Challenges

Organizational

- Defining and designing a worst-case cyber attack scenario for Austria
- Gathering information of displayed entities (national businesses, etc.)

Technical

- Customization of the Thales Hypervisor Framework
- Automating standard configuration procedures
- Integration of a remote simulation interface to simulate proper scenarios

The Scenario

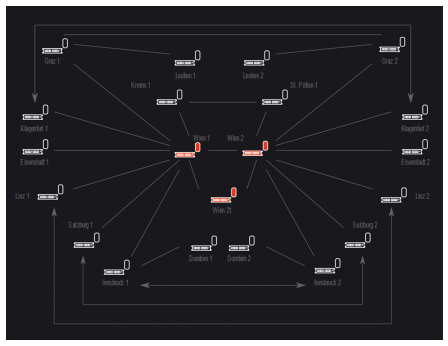


Figure 2: Topology of the Austrian backbone net. Three routers are down.

Visualized Entities

- Critical facilities (top 800 companies)
- Routers of the Austrian backbone net
- Routers of the radio relay system
- Mobile communications network
- Energy provider (SCADA net)

Short scenario summary

- Router outage from Vienna to western parts of Austria.
- Mobile communications and companies experience outage.
- Routers are coming up and going down randomly.
- A concentrated attack forces all routers to go down.
- Eventually all routers and the communications network come up.

The Hypervisor Framework

Hypervisor Architecture

- Based on a secure Service-Oriented Architecture (SOA) framework.
- Web-based Human-Machine Interface (HMI) that provides a total view of equipment status, incidents/alarms and resource allocation.
- Fully scalable due to SOA solution.

Human-Machine Interface (HMI)

- Extensive use of modern Rich Internet Application (RIA) HMI frameworks.
- Short reaction time using data push to web clients based on COMET architecture.
- Graphics management optimized using vector-based schematics (SVG format).
- High availability architecture.

Developments by SBA

- SBA is the lead partner concerning the development of simulations with Thales Hypervisor Framework.

New enhancements developed by SBA

- Development of a remote simulation interface with sockets.
- The 3 screen principle: Geo Information, Alert Matrix and Topology View.
- Zoom functionality in the Geo Information topology.
- Tool for configuration transformation (XLS to XML).
- Tool for GEO data gathering.

Next project [KIRAS] - Protection drill for computer-based cross-business disaster logic (SCUDO)

Goal

- Creation of a training process for national security emergencies in Austria.
- Validation of international standards and their application to Austria.

Project Partners

- Thales Austria GmbH (project leader)
- SBA Research GmbH
- nic.at Internet Verwaltungs- und Betriebsgesellschaft m.b.H.
- Zentraler Informatikdienst der Universität Wien (ZID)
- Universität Wien Arbeitsgruppe Rechtsinformatik

Project Partners

- Infraprotect GmbH
- REPUCO Unternehmensberatung GmbH
- Bundeskanzleramt
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.