secure
sba-research.org

COMET

Competence Centers for
Excellent Technologies

IMPACT 2014

22.05.2014

16.00	**A Min Tjoa** Obmann SBA Research	*Eröffnung der Vorträge*
16.10	**SBA Lightning Talks**	
	Dimitris Simos	*Combinatorial Testing for Web Application Security*
	Christoph Falta	*Spearphishing in Real Life*
	Peter Kieseberg	*Planspiele für unternehmensübergreifende ICT-Desaster*
	Johanna Ullrich	*Sichere Netzwerkprotokolle*
	Thomas Konrad	*Heartbleed in Österreich: Machen Admins ihren Job?"*
16.40	**Michael Hollauf** MindMeister	*MindMeister – Securing a Global Cloud App*
17.05		*Pause* *... Kaffee & Erfrischungen* *... Bauernsushi, - Guglhupf*
17.25	**Franz Wotawa** Technische Universität Graz	*Model-based Testing – Theory and Application*
17.50	**Sebastian Schrittwieser & Peter Frühwirt** Fachhochschule St. Pölten SBA Research	*Security through Obscurity, powered by HTTPS*
18.15		*Jahresfest SBA Research* *... reichhaltig Speis & Trank* *... Naturbier-Verkostung der Brauerei Leutschach*

Die Abstracts finden Sie auf der Rückseite

MindMeister – Securing a Global Cloud App

Michael Hollauf, MindMeister

MindMeister ist die führende Mind Mapping Plattform im Web mit über 2,5 Millionen Benutzern. Michael Hollauf, einer der Gründer des Unternehmens mit Sitz in Wien, wird nach einer kurzen Produktvorstellung einige ausgewählte Security- und Privacy-Aspekte des Tools beleuchten, etwa wie die NSA-Affäre die Geschäfte des Unternehmens beeinflusst hat, oder wie jüngst mit dem Heartbleed-Bug umgegangen wurde.

Model-based Testing – Theory and Application

Franz Wotawa, Technische Universität Graz

Modellbasiertes Testen ist ein sehr wichtiges Verfahren zur Verifikation und Validierung von Software und Systemen. In meinem Vortrag werde ich neben den Ideen und Grundlagen hinter dem modellbasierten Testen auch auf die Anwendung in der Praxis eingehen. Neben dem Hauptanwendungsgebiet des modellbasierten Testens dem funktionalen Test steigt die Bedeutung auch im Bereich des Testens von Sicherheitsmerkmalen. Für beide Applikationsdomänen werden Beispiele aus der Praxis diskutiert.

Security through Obscurity, powered by HTTPS

Sebastian Schrittwieser, Fachhoschule St. Pölten & Peter Frühwirt, SBA Research

Smartphone-Applikationen sind gegen Analyse und Modifikation mit Hilfe einer Reihe von Sicherheitsmaßnahmen wie Verschlüsselung, Codesignierung und Sandboxing geschützt. Für Applikationen mit Netzwerkkommunikation können jedoch effektive Angriffsvektoren in deren Übertragungsprotokollen gefunden werden. Viele Entwickler von Smartphone-Applikationen verstecken die Implementierungsdetails ihrer Protokolle in SSL/TLS-Verbindungen. Während SSL/TLS gegen Mitlesen auf dem Transportweg schützt, ist es eine ungeeignete Schutzmaßnahme gegen Protokollanalyse. Das Konzept der SSL-Interception ermöglicht die Analyse und Modifikation von Übertragungsprotokollen mit nahezu unbegrenzten Möglichkeiten: Schummeln in Online-Spielen, kostenloses Freischalten von Zusatzfunktionalität in Applikationen, Sicherheitsanalyse von Protokollen, usw. In diesem Vortrag demonstrieren wir wie Applikationsentwickler unsichere Protokolle in SSL/TLS zu verstecken versuchen und zeigen, dass bekannte Gegenmaßnahmen in der Praxis kaum genutzt werden.