
SBA
Research

Secure Coding with AI

Federal Ministry
Innovation, Mobility
and Infrastructure
Republic of Austria

Federal Ministry
Economy, Energy
and Tourism
Republic of Austria

FFG
Promoting Innovation.

vienna
business
agency

For the
City of Vienna

European
Commission

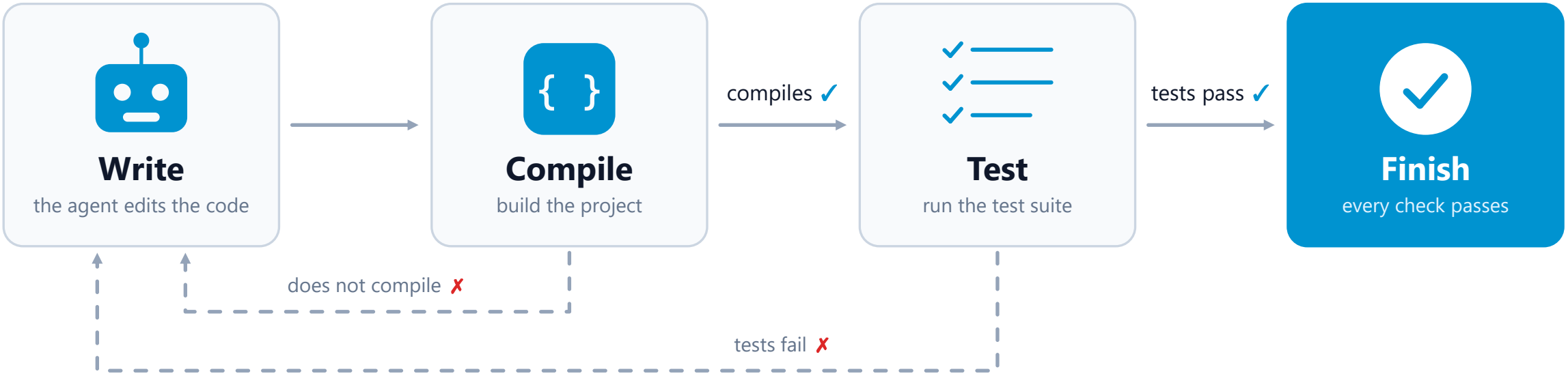
FWF Austrian
Science Fund

netidee
FÖRDERUNGEN

Coding is largely solved.

Boris Cherny, Head of Claude Code – Lenny's Podcast

The Agent Loop



Write, check, repeat, until every check passes.

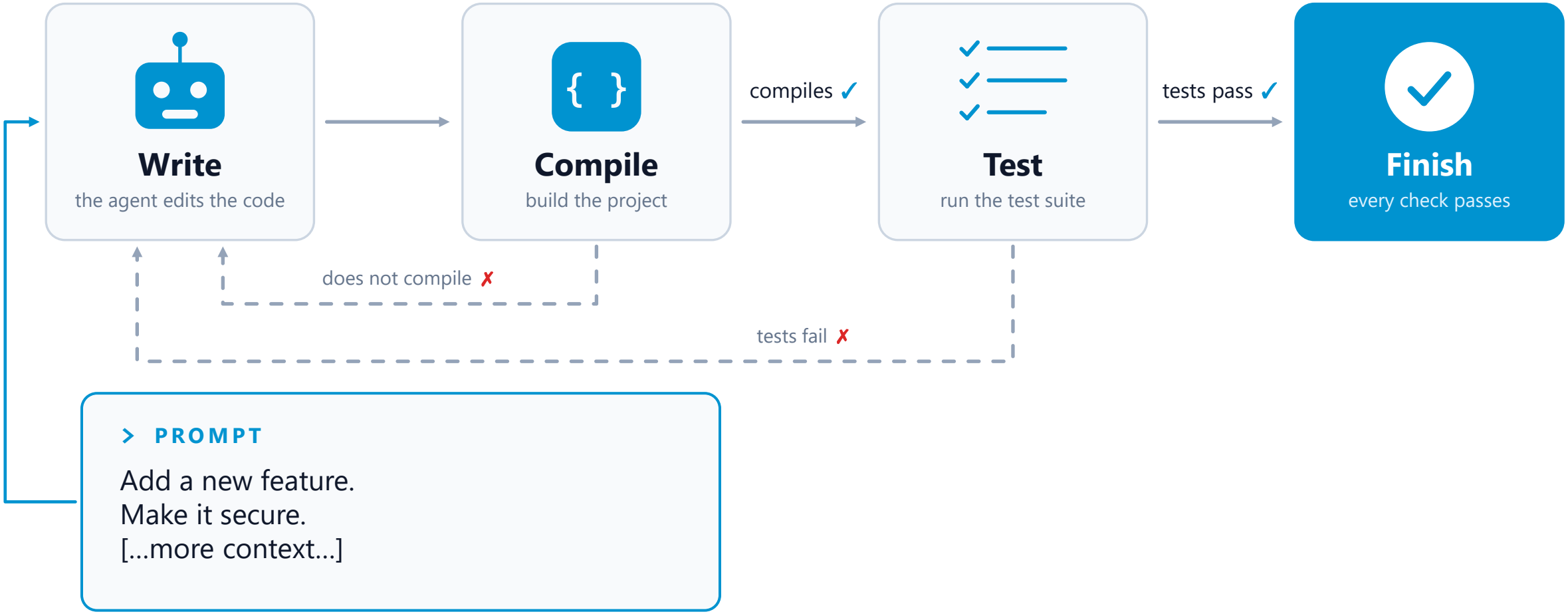
Have AI agents killed Secure Coding?

About me...

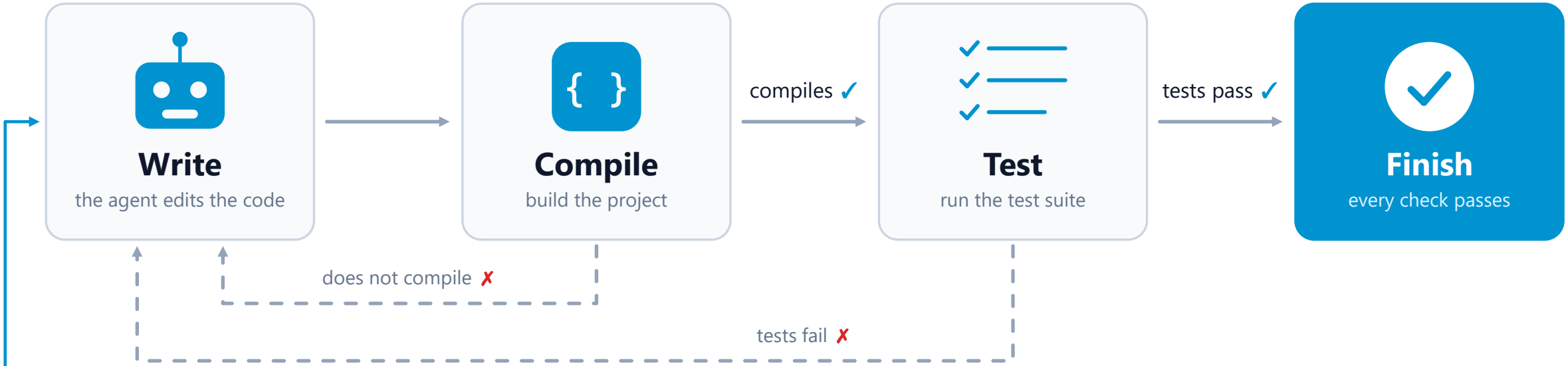
- Fabian Funder, Security Consultant
  - Penetration tests
  - Source code audits
  - Security trainings
  - SDLC consulting
- SBA Research



The Agent Loop



The Agent Loop



> PROMPT

Add a new feature.
Watch out for SQL injection, Cross-Site Scripting, Cross-Site Request Forgery, …
[…more context…]

Does this generate secure software?
Why not?

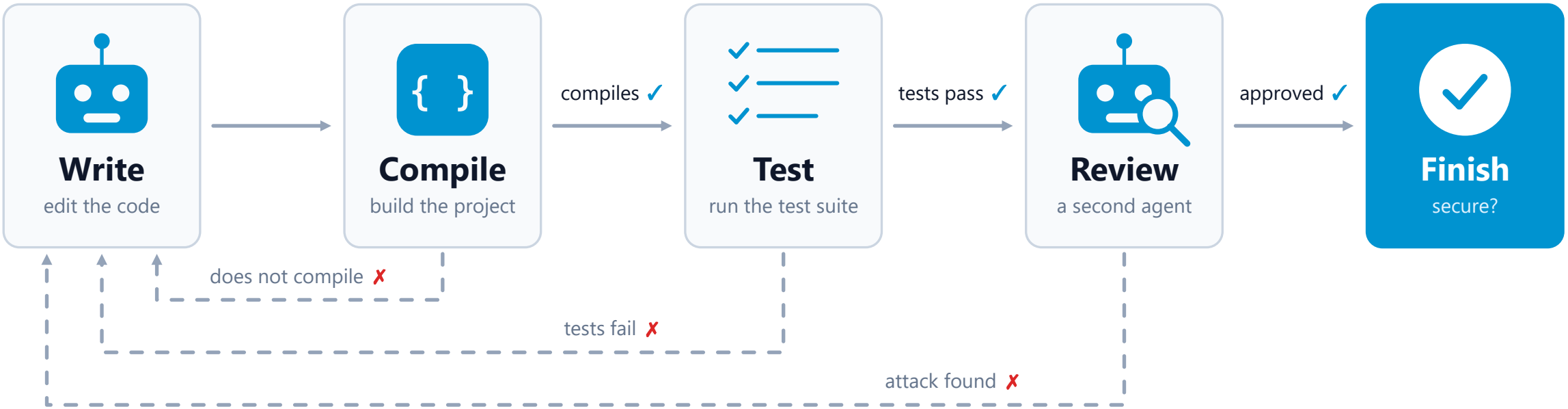
No observable outcome proves a thing secure

Cormac Herley, Unfalsifiability of Security Claims (2016)

Program testing can be used to show the presence of bugs, but never their absence!

Edsger W. Dijkstra

Adversarial Review



We don’t know if the code with the change is more secure than the code without it.

A change can add new vulnerabilities, or fail to mitigate an vulnerability we intended to fix.

The Take-away From Herley's Paper

- Formulate falsifiable security goals
- Falsifiable:

  Using parameterized queries for all database access is sufficient to prevent SQL injection in this application.

- Unfalsifiable:

  If you don't sanitize all user inputs, then you are insecure.

So, what helps?

Tools and Libraries

- Abstraction over common problems
- Offer an Interface that:
  - Provides secure defaults
  - Makes secure path easy and insecure path explicit
- Shift responsibility to the tool
  - Tool's responsibility: implementation
  - Your responsibility: *correct* usage, updates, …

Angular's Approach to XSS

Angular

```
private sanitizer = inject(DomSanitizer);
// […]
constructor() {
  trusted =   // explicit opt-out
    this.sanitizer.bypassSecurityTrustHtml(untrusted);
}
```

- Values are untrusted by default
- Untrusted values are escaped or sanitized
- Need to opt-out explicitly
- Searchable name

Shell

```
grep -rn 'bypassSecurityTrust' src/
```

- Assuming Angular works as expected, we are not affected by Cross-Site Scripting (XSS).
- Check by grepping.

Security Principles & Design Patterns

- Security Principles
  - High-level properties software, or
  - The way software is created
- Design Patterns
  - Make it hard to do something wrong
- Goal:

Make security of a system measurable

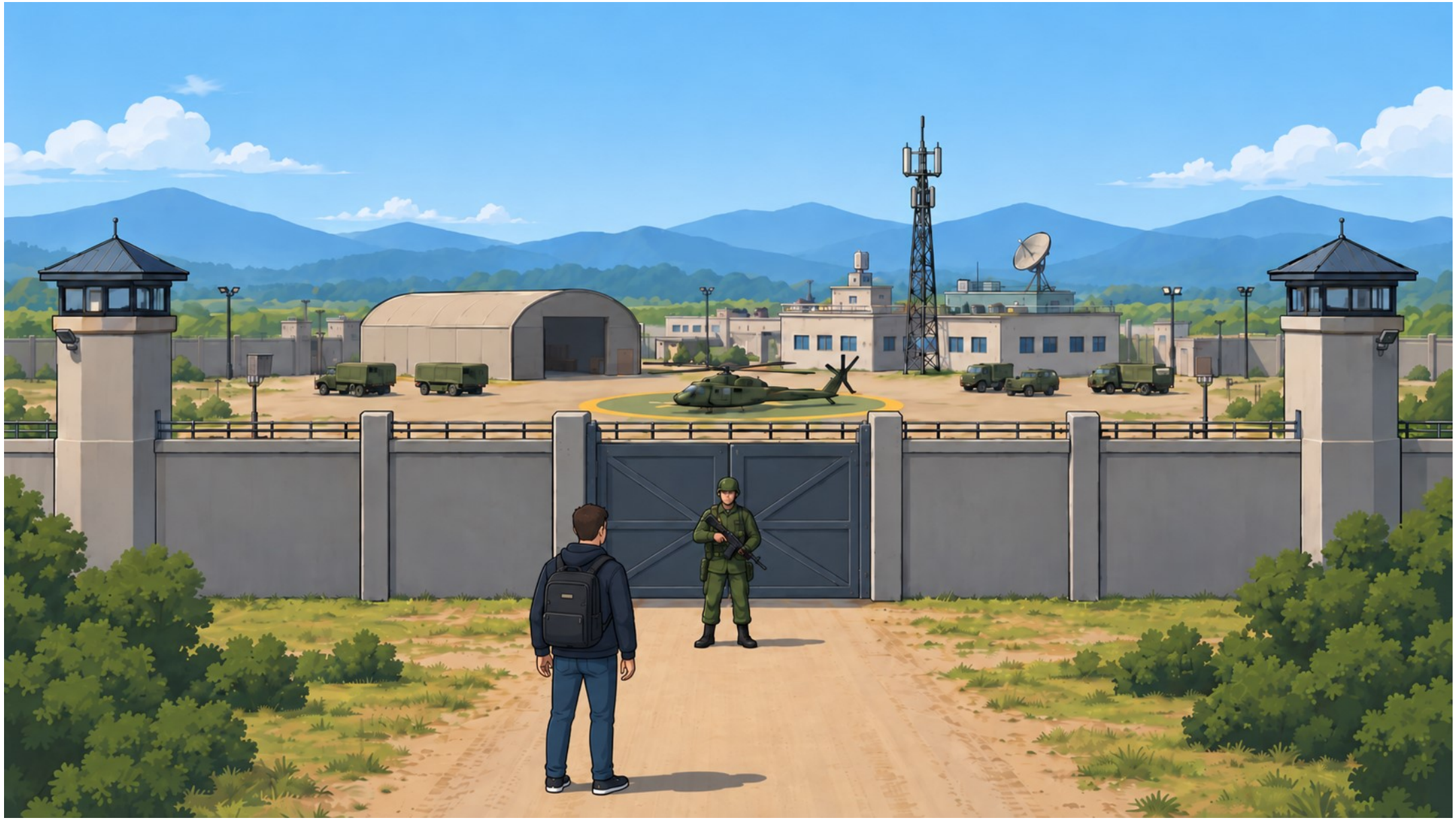
One Door, One Guard

Complete mediation: every access to every object must be checked for authority.

Saltzer & Schroeder, The Protection of Information in Computer Systems (1975)

- Single Access Point Pattern (One Door)
- Check Point Pattern (One Guard)

Yoder & Barcalow, Architectural Patterns for Enabling Application Security (1997)





Demo

One Door, One Guard

https://github.com/FabianTUW/Frontcontroller-demo

Generation Time vs Verification Time

- Generation Time:
  - When code is generated:
  - Patterns take effect at generation time
  - Only one way to add `app.route(…)`
    - Agent will (probably) choose that way
- Verification Time:
  - When code is verified by the agent
    - Detect use of risky function
    - Divergence from patterns

Good artists copy
Great artists steal

attributed to Pablo Picasso, popularized by Steve Jobs

Have AI Agents Killed Secure Coding?

- No
- Secure Coding matters more than ever
  - Make secure path easy
  - Make insecure path explicit
  - Enables long term efficient coding!
- More code more problems!

What do you think?

- Secret Prompt I don’t know about?
- Are there other reasons why AI agents generate insecure code? Are they more impactful?

Contact Information

Fabian Funder

SBA Research

Floragasse 7, 1040 Vienna

ffunder@sba-research.org



Federal Ministry Innovation, Mobility and Infrastructure Republic of Austria

Federal Ministry Economy, Energy and Tourism Republic of Austria

FFG Promoting Innovation.

vienna business agency | For the City of Vienna

European Commission

FWF Austrian Science Fund

netidee FÖRDERUNGEN