

Carnegie Mellon University
Security and Privacy Institute



Concluding update

Future Enterprise Security Initiative

Rethinking security across enterprise ecosystems through innovations in artificial intelligence, computer science, engineering, and human-factors research

Faculty Co-Directors:

Lujo Bauer

Professor, Electrical and Computer Engineering + Software and Societal Systems Dept.

Vyas Sekar

Professor, Electrical and Computer Engineering

Thank you, sponsors of the Future Enterprise Security Initiative



Enterprises Are Evolving Across the Board



Small/medium
factories and
manufacturing



Healthcare



Finance +
ID platforms



Energy/grid



IoT

1

Complex ecosystem with
third party dependencies



e.g. sensors
• from third party
• software supply chain
• internal dependencies

2

Remote, distributed, work modalities



Remote admin

Outsourced management

Other unexpected trends may arise!

Breaches Are Norm, Not Exception

A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack



Cyberattack Forces a Shutdown of a Top U.S. Pipeline

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.

JBS cyberattack: From gas to meat, hackers are hitting the nation, and consumers, where it hurts



A Reason for Hope?



Large corporation

- Global visibility
- Bespoke solutions
- Large tech teams

The Grand Challenge Question

Can we ensure that the operational security of **all enterprises** is as good as the select few “hyperscale operations” that have large security teams and global-scale visibility into threats?



Large corporation

- Global visibility
- Bespoke solutions
- Large tech teams

Equivalent operational security



“Future proof”?



Small to medium enterprise

- Local visibility
- Third party, commodity
- Small tech teams

Future Enterprise Security Initiative

Foundations for understanding cyber risk and dependencies in complex ecosystems and supply chains

AI-driven workflows to automate security management and data-driven decision-making to minimize the need for large human teams

Least-privilege-by-design infrastructure, including trustworthy outsourcing, remote work/management, and deployable software-defined architectures



Collaborative capabilities to effectively get real-time and global visibility of threats

Vision: *To create the knowledge and capabilities to build and implement secure enterprise systems*

through CMU cybersecurity, privacy, AI, computer science and engineering, human-factors research

+ industry expertise and engagement

Future Enterprise Security Initiative

Y1 13 projects

- **Synthetic data generation** (for testing, threat analysis, ...)
- Tools to guide **deception-as-a-defense** strategy
- **Automatic testing of microservices**
- Engineer-focused **tools to build provably secure and performant Rust code**
- **Mapping software dependencies** at scale
- ...

Y2 12 projects

- Using **LLMs to simplify enterprise security management**, improve software analysis (fuzzing, bug finding)
- **Network infrastructure hardening**
- Engineer-focused **tools to build provably secure and performant Rust code**
- **Mapping software dependencies** at scale
- ...

Y3 (Oct '24 -) 10 projects

- **LLM-assisted JS vulnerability detection**
- **Resiliency through graceful degradation**
- **Data provenance tracing for generative AI**
- **Prioritized software patching**
- Engineer-focused **tools to build provably secure and performant Rust code**
- ...

Y1 → Y3: shift to **leverage *and* remediate generative AI**

Future Enterprise Security Initiative

Y1

13 projects

Y2

12 projects

Y3

10 projects

Outcomes

- Academic papers, awards
- **20+ code repositories:** code verification, bug finding, testing new defenses, detecting attacks, building more secure systems
- **Follow-up funding** from NSF, DARPA, SEI, Siemens, Amazon, Cisco, ...
- Student **internships with sponsors** (4 Microsoft, 5 Amazon)
- Student **full-time jobs with sponsors** (2 Microsoft, 7 Amazon)
- Example **tech transfer:**
 - Tools in use at Microsoft at Amazon (on in-production systems)
 - Updates to industry-standard NIST facial recognition benchmark
 - Faculty sabbatical (Amazon)

Future Enterprise Security Initiative



Participating faculty: Yuvraj Agarwal, Lujo Bauer, Fraser Brown, Fei Fang, Giulia Fanti, David Garlan, Virgil Gligor, James Hoe, Limin Jia, Carlee Joe-Wong, Gauri Joshi, Eunsuk Kang, Swarun Kumar, Claire Le Goues, Ruben Martins, Heather Miller, Rohan Padhye, Bryan Parno, Corina Pasareanu, Anthony Rowe, Vyas Sekar, Nihar Shah, Justine Sherry, Ben Titzer, Steven Wu, Osman Yagan, ...