



Cyber Autonomy @ Cylab Initiative

Lujo Bauer and Vyas Sekar, co-directors

AI is rapidly changing the landscape of threats and capabilities

Traditional approaches to computer security no longer suffice, and simply keeping pace with attacks is increasingly difficult.

- **Increasing asymmetry between attackers and defenders**
 - As connected devices rapidly proliferate, **the attack surface has increased dramatically**
 - 0.5 billion connected devices in 2003. 20+ billion by 2025
 - Traditional security operations rely on manually predefined rules and human time-scale responses
- **Transformational advances in machine learning and AI**
 - AI for code generation and workflow automation means **our ability to build and deploy new features far exceeds our ability to secure systems**
 - AI is unlocking new offensive and defensive capabilities at a rapid pace

We need **foundational research** to understand autonomous attack and defense capabilities and to build human-system interactions to match

We need foundational research

We are creating the *scientific foundations for building and evaluating future autonomous security products*

Foundations for Autonomous Attack and Defense

Create foundations for science of cyber autonomy to empower defenders with the tools and methods to autonomously catch problems before real attacks happen.

E.g., abstractions for expressing capabilities, leaderboard capabilities, datasets for cyberevals

Human-AI Collaboration for Cyber Autonomy

Understand real-world constraints of operators to design adequate defense systems with autonomous tools;

E.g., debugging attack and defense systems and human-AI collaborative tooling.

Systems Support for Autonomous Operations

Design and implement systems advances required for next-generation autonomous security operations.

E.g. emulation systems and datasets for training models; sandbox, staging, and verification systems; scalable telemetry and log analytics; and software-defined data/control plane capabilities.

Initiative Co-Directors



Vyas Sekar

Tan Family Professor, Electrical and
Computer Engineering



Lujo Bauer

Professor, Electrical and Computer
Engineering, Software and Societal
Systems Department