Computer & Network Security Lab 
CUNY Hunter College

The Computer & Network Security Lab at CUNY Hunter College examines the security concerns that impact computing today. Computers and systems play a huge part in our everyday lives, opening up opportunities for criminals and hackers to try to access information and interfere with our lives. Our research is funded by CUNY and others. Our students and graduates work or have worked at LinkedIn, American Express, Accenture, Deloitte, ViacomCBS, and Raytheon.

We partner with multiple universities worldwide, including Korea University, University of Bonn, and more.

Get in touch: spock@ieee.org
www.cs.hunter.cuny.edu/~spock/

Faculty

Sven Dietrich

PhD Students

Current

Shoufu Luo
Jeremy D. Seideman
Isa Jafarov

Past

Patrick Duessel
(Graduated 2018, now Senior Director at Raytheon)

Why computer and network security?

From data breaches to software vulnerabilities, network intrusions and malware, there are many ways that bad actors can try to disrupt people's lives.

Since smartphones, home automation, and cloud services play a large part of our lives, we have more of our lives in the digital world. This means that there are that many more opportunities for systems and data to be captured, changed, and leveraged for nefarious purposes.

Security is an arms race - both sides are constantly innovating and mitigating, in order to bypass the other. By understanding the threats that exist, we look for new ways to protect against them, and look for ways to protect against future threats.

Last modified: September 2022
Source code and binary similarity

Software projects move towards community-based development (using tools such as SourceForge and GitHub) and create more opportunities for developers to reuse and share code. While this helps advance the field and allows for new and varied software, it also opens up the possibility of software vulnerabilities—defects in software that can lead to data integrity issues or attack possibilities. Being able to detect similar chunks of code in both source and binary files helps detect these vulnerabilities, see how widespread they are, and determine the optimal strategy to fix them, protecting the entire software landscape.


Software Vulnerability Origin Discovery

Vulnerabilities are a prevalent problem—bots, trojans, and ransomware exploit them computers, steal data, and interrupt systems, the Internet, and access. Being able to determine the origin of that vulnerability—where it came from and how it evolved—helps researchers determine how to protect the software supply chain and where it originated. In this way, both software and security engineers can help track down the source responsible for the software flaw. Cf. NTIA’s Software Bill of Materials (SBOM) in industry.


Insider Threat

Insiders present a special problem in computer security. They are “inside the system” and can cause severe damage. We aim to find behavioral patterns to identify abnormal behavior in enterprise networks and host log files using machine learning techniques.


Cybersecurity Experimentation Frameworks

We are building a highly configurable cybersecurity experimentation testbed. This DETER-style testbed allows for proper testing of attack and defense mechanisms in a safe environment away from the production networks. It also allows for federation with existing experimentation testbed networks. Our multi-node testbed allows for experiments to be run on a variety of hardware platforms and at network speeds up to 10 Gbps. The next generation of testbeds is already in the making.

DDoS, botnets, and next-generation networks

We are investigating new attack and defense techniques for the current and next-generation Internet architectures, including Software Defined Networks.
