Computer & Network Security Lab
CUNY Hunter College

HUNTER
The City University of New York

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, Cisco, and Raytheon.

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

Faculty

Sven Dietrich

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

PhD Students

Current

Isa Jafarov

Saskia Laura Schröer

Shoufu Luo (2023)

Past

Jeremy D. Seideman (2023)

Patrick Duessel (2018)

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 current threats in the open and dark web, we look for new ways to protect against them in a systems-oriented approach, including the use of AI and machine learning, and look for ways to protect against future threats.

Last modified: October 2024

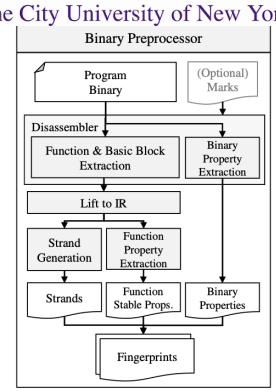
THE GRADUATE CENTER
CITY UNIVERSITY OF NEW YORK

Selected current projects at the CNS Lab

HUNTER
The City University of New York

Source code and binary similarity

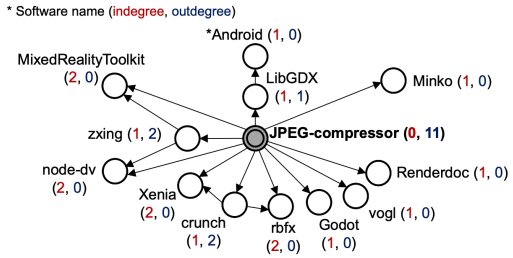
Software projects move towards community-based development (using tools such as SourceForge and GitHub) and create more opportunities for developers to reuse and share code. While this helps advance the field and allows for new and varied software, it also opens up the possibility of software vulnerabilities - 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 across system architectures.



- Hajin Jang, Kyeongseok Yang, Geonwoo Lee, Yoonjong Na, **Jeremy D. Seideman**, **Shoufu Luo**, Heejo Lee, and **Sven Dietrich**, QuickBCC: Quick and Scalable Binary Vulnerable Code Clone Detection. *In Proceedings of ICT Systems Security and Privacy Protection (SEC 2021), IFIP Advances in Information and Communication Technology*, Vol 625. Springer, Cham. https://doi.org/10.1007/978-3-030-78120-05, 2021.

Software and Protocol Vulnerability 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 – including 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.



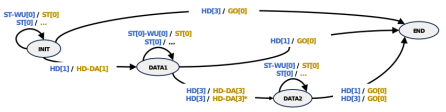
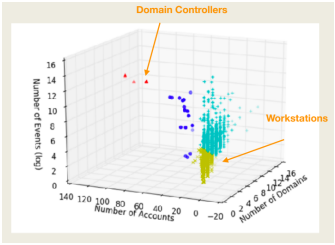


Fig. 5: State machine of Nginx and H2O (Chromium and Opera traces)

- Seunghoon Woo, Dongwook Lee, Sunghan Park, Heejo Lee, and **Sven Dietrich**, "V0Finder: Discovering the Correct Origin of Publicly Reported Software Vulnerabilities," *In Proceedings of the 30th USENIX Security Symposium*, pp. 3041–3058, 2021.
- Choogin Lee, **Isa Jafarov**, **Sven Dietrich**, Heejo Lee. "PRETT2: Discovering HTTP/2 DoS Vulnerabilities via Protocol Reverse Engineering," *In Proceedings of the 2024 European Symposium on Research in Computer Security (ESORICS),* pp. 3-23, 2024.

Anomaly Detection and Insider Threat

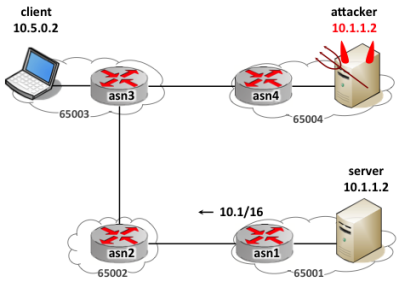
Insiders present a special problem in computer security. They are "inside the system" and can cause severe damage. We aim to find behavioral patterns to identify abnormal behavior in enterprise networks and host log files using machine learning techniques.



- **Patrick Duessel**, **Shoufu Luo**, Ulrich Flegel, **Sven Dietrich**, and Michael Meier, "Tracing Privilege Misuse Through Behavioral Anomaly Detection in Geometric Spaces," *In Proceedings of the 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)*, 2020, pp. 22-31, https://doi.org/10.1109/SADFE51007.2020.00012, 2020.

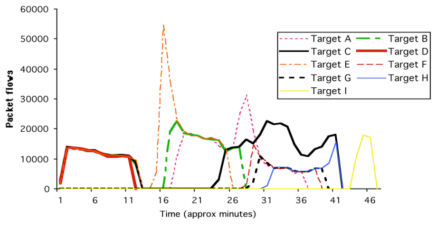
Cybersecurity Experimentation Frameworks

We are building a highly configurable cybersecurity experimentation testbed. This SPHERE-style (formerly DETER) 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, next-generation networks, and the metaverse

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



- Jelena Mirković, **Sven Dietrich**, David Dittrich, and Peter Reiher. *Internet Denial of Service: Attack and Defense Mechanisms*, 400 pp., Prentice Hall PTR, December 2004.
- Marc C. Dacier, Hartmut König, Radoslaw Cwalinski, Frank Kargl and **Sven Dietrich**, "Security Challenges and Opportunities of Software-Defined Networking," in *IEEE Security & Privacy*, vol. 15, no. 2, pp. 96-100, March-April 2017, https://doi.org/10.1109/MSP.2017.46, 2017.
- Ilies Benhabbour, Yérom-David Bromberg, Marc Dacier, Sven Dietrich, Rodrigo Miragaia Rodrigues, Paulo Esteves-Verissimo. "Attacks on tomorrow's virtual world." In *Proceedings of the IEEE 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks DSN Disrupt*, June 2023.

THE GRADUATE CENTER
CITY UNIVERSITY OF NEW YORK