Understanding Cybersecurity Series (UCS)
Behaviour-Centric Cybersecurity Center (BCCC),
York University, Toronto, ON, Canada
Volume 2 (October 2025)

BCCC

YORK UNIVERSITÉ UNIVERSITY

CONTENT

From the Founder's Desk

To address the growing challenges of cybersecurity resiliency, it is essential to advance both the use of AI in cybersecurity and the development of Secure AI itself. On one hand, AI-driven tools are needed to support daily security projects, detecting anomalies, analyzing threats, and automating response at scale. On the other, AI models must be designed with robustness, privacy, and trustworthiness to withstand adversarial attacks, poisoning, and misuse. Researchers and developers urgently require open-source tools, datasets, and analyzers that make these capabilities accessible, reproducible, and adaptable to real-world threats. With this mission, the **Understanding Cybersecurity Series (UCS)** delivers inclusive, AI-powered and secure-by-design resources that bridge research, industry, and education. Through open datasets, analyzers, training programs, and simplified outreach, **UCS** empowers students, academics, developers, and professionals to both apply AI effectively in cybersecurity and to safeguard AI systems themselves, fostering innovation and resilience across the ecosystem.

As a Canada Research Chair in Cybersecurity, I recognized the need for a comprehensive knowledge mobilization program that could cater to the unique needs of audiences ranging from K-12 students to seniors, spanning technical and nontechnical backgrounds. The **UCS** program was created to address this gap, offering two distinct sets of materials: academic and technical resources for researchers, educators, and professionals, and non-technical resources tailored for youth, seniors, and the general public. Through this initiative, we aim to advance cybersecurity education and research while equipping the community with the tools and awarness needed to navigate and secure an increasingly digital world. The **UCS** represents a commitment to inclusivity, accessibility, and innovation in the pursuit of a more resilient cybersecurity ecosystem.

Arash Habibi Lashkari, PhD
Canada Research Chair in Cybersecurity
Professor at York University, Toronto, ON, Canada

BCCC
Behaviour-Centric
Cybersecurity Center

Understanding Cybersecurity Series (UCS)

Analyzer and Analytic Series

Explore Our Open-Source Cybersecurity Tools: Powerful Analyzers and Analytic for Research and Development

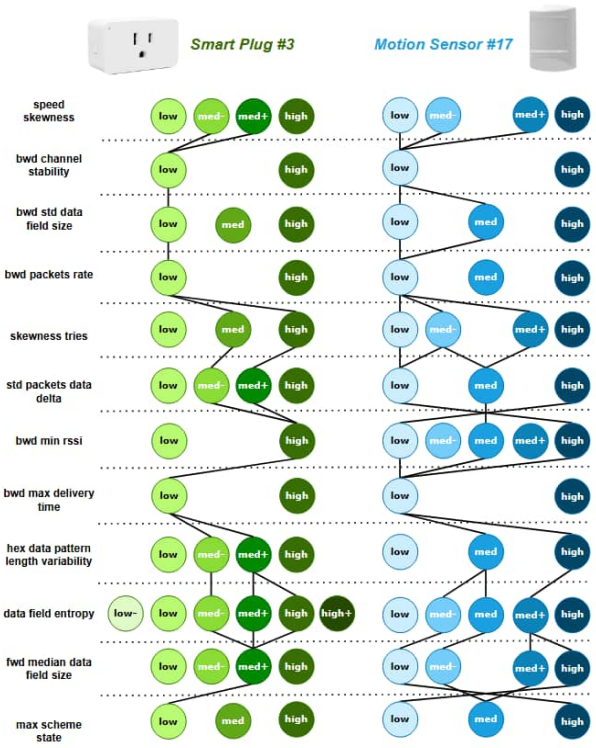
https://www.yorku.ca/research/bccc/Analyzers/

IoT-ZwaveNetLyzer V1.0

IoT ZWave Network Analyzer

- As part of the Understanding Cybersecurity Series (UCS) , IoT-ZwaveNetLyzer is an open-source Python project developed for analyzing Z-Wave network traffic in IoT environments. It generates bidirectional traffic flows and extracts over 400 statistical and protocol-level features , such as signal strength (RSSI), packet speed, acknowledgment ratios, and channel usage patterns. By profiling both forward and backward communication streams, it enables a fine-grained understanding of device behavior and communication efficiency across smart home and industrial IoT networks.

- Designed for scalability and transparency, IoT-ZwaveNetLyzer supports both Linux and Windows environments and can be customized through simple configuration files, enabling flexible use in research and experimentation. The analyzer is a crucial tool for building and validating IoT intrusion detection systems, providing a structured framework to characterize device behavior, network stability, and traffic anomalies in both real and simulated environments.



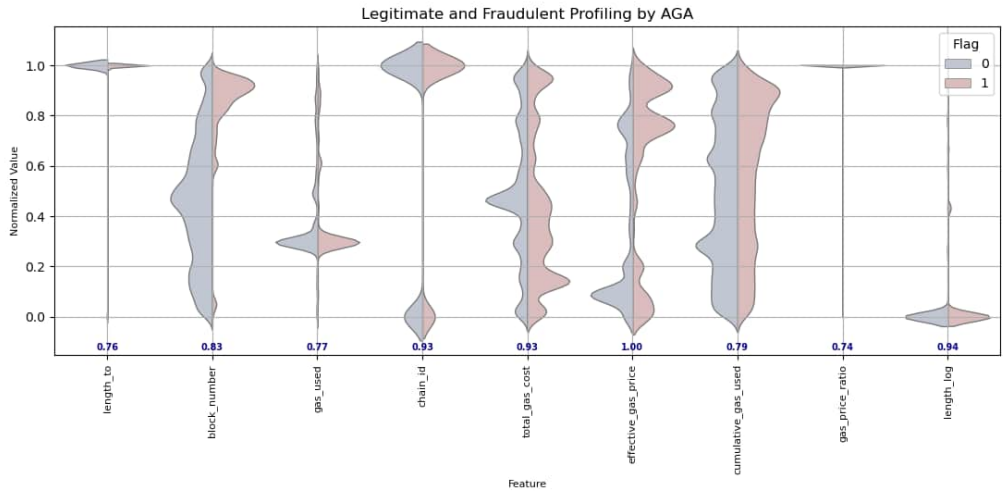
https://www.yorku.ca/research/bccc/Analyzers

DeFiTranLyzer V1.0

Decentralized Finance Transaction Analyzer

- DeFiTransLyzer, part of the Understanding Cybersecurity Series (UCS), is an open-source Python framework designed to extract and analyze features from Ethereum wallets and transactions. Its Wallet Analyzer processes JSON-based wallet records to compute statistical measures such as averages, variance, skewness, gas usage, and transaction values, while also capturing dynamics like durations, error rates, and interacting addresses. The results are returned as a structured feature dictionary, providing a clear view of wallet-level behavior.

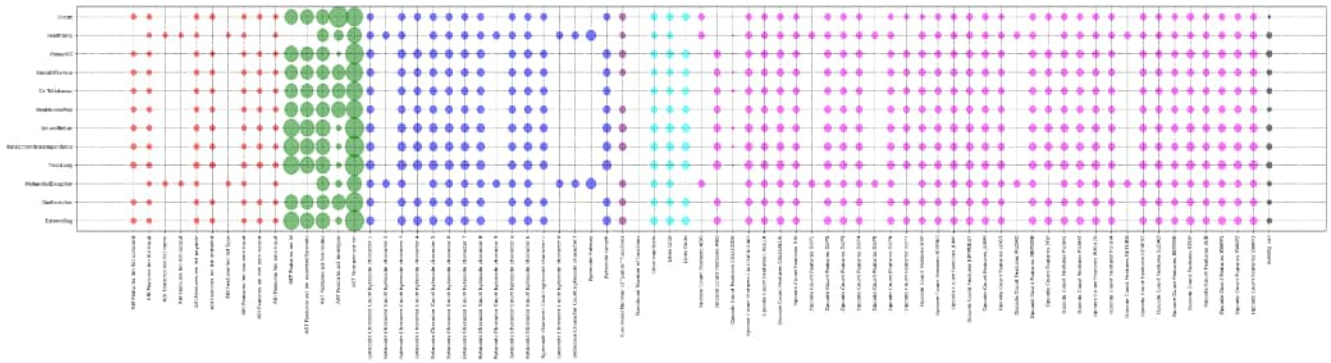
- The Transaction Analyzer complements this by parsing individual transaction data. It extracts gas usage, values, and efficiency ratios, while also analyzing event logs, token transfers, contract creation, and self-interactions. By returning structured transaction-level features, it provides detailed insights into blockchain activity. Together, the two modules form a unified toolchain for profiling Ethereum behavior, supporting vulnerability research, behavioral modeling, and broader DeFi security studies.



https://www.yorku.ca/research/bccc/Analyzers

SCsVulLyzer (V2.0, V1.0)
Smart Contracts Vulnerability Analyzer

- SCsVulLyzer V2.0, part of the Understanding Cybersecurity Series (UCS), is an open-source Python tool that extracts over 240 features to profile Ethereum Smart Contracts for vulnerability detection. It extends V1.0 by classifying features into compiler-based (e.g., AST, ABI) and non-compiler-based categories, the latter using NLP to detect critical security-related keywords.
- This version also introduces new feature groups, Contract Information, Source Code Information, and Solidity Information, capturing metrics such as function counts, loops, and lines of code. A key addition is bytecode entropy, which measures randomness and complexity in smart contracts, enabling deeper insights for vulnerability analysis, anomaly detection, and cryptographic risk assessment.



https://www.yorku.ca/research/bccc/Analyzers

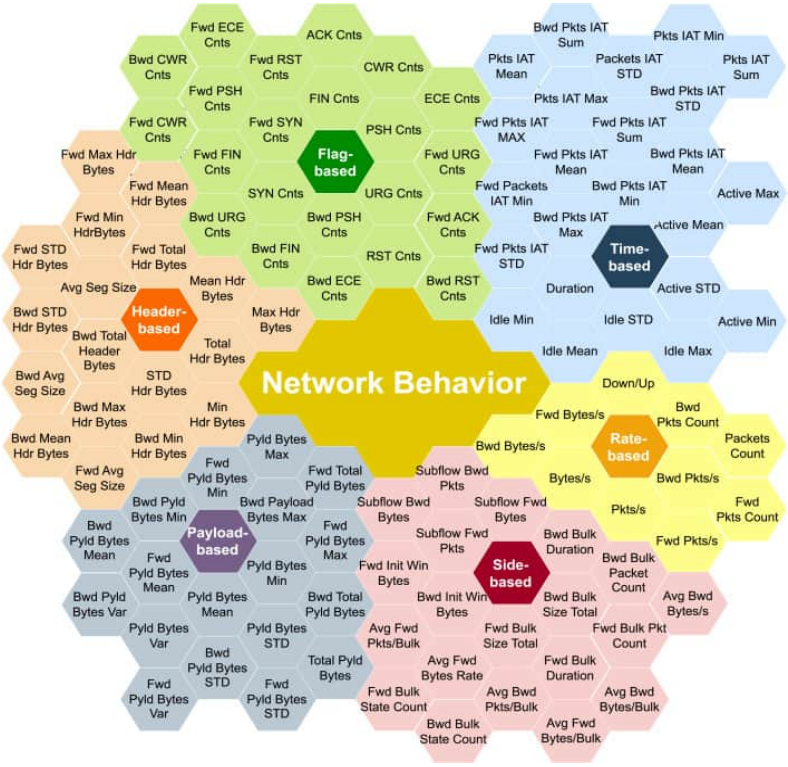
BCCC Behaviour-Centric Cybersecurity Center

NTLFlowLyzer V1.0, V2.0, V3.0

Network and Transportation Layers

Flow Analyzer

- NTLFlowLyzer, part of the Understanding Cybersecurity Series (UCS) and the second component of NetFlowLyzer, is an open-source Python tool for extracting network layer features from TCP-based traffic to support anomaly profiling. It builds bidirectional flows at the network and transport layers, with the first packet defining forward and backward directions for separate statistical and time-based analysis.
- The tool allows users to select or add features and adjust flow timeout settings. TCP flows are terminated automatically when a connection ends (FIN or RST), when maximum duration is reached, or after inactivity, ensuring accurate and flexible flow profiling for security research.

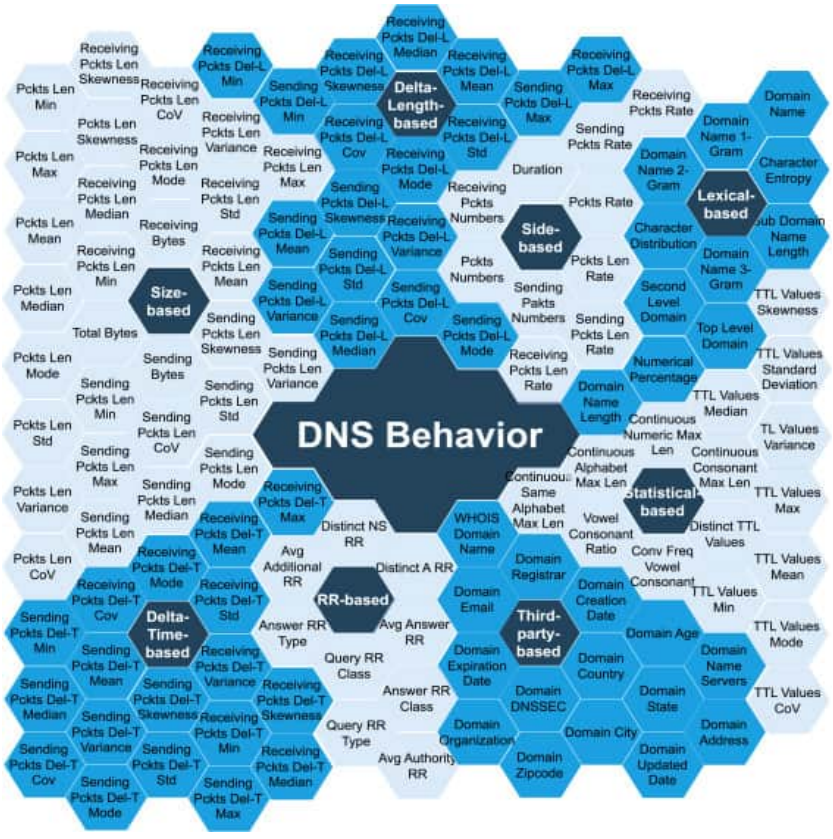


https://www.yorku.ca/research/bccc/Analyzers

ALFlowLyzer V1.0

Application Layer Flow Analyzer

- ALFlowLyzer, part of the Understanding Cybersecurity Series (UCS) and the third component of NetFlowLyzer, is an open-source Python tool for extracting application-layer features from network traffic to support anomaly profiling. It focuses on flows where threats often emerge, extending analysis beyond transport and network layers.
- The tool builds bidirectional flows with separate forward and backward statistics, allows feature selection or addition, and supports flow timeout customization. The first release targets the DNS protocol, with future versions planned to cover additional application-layer protocols.

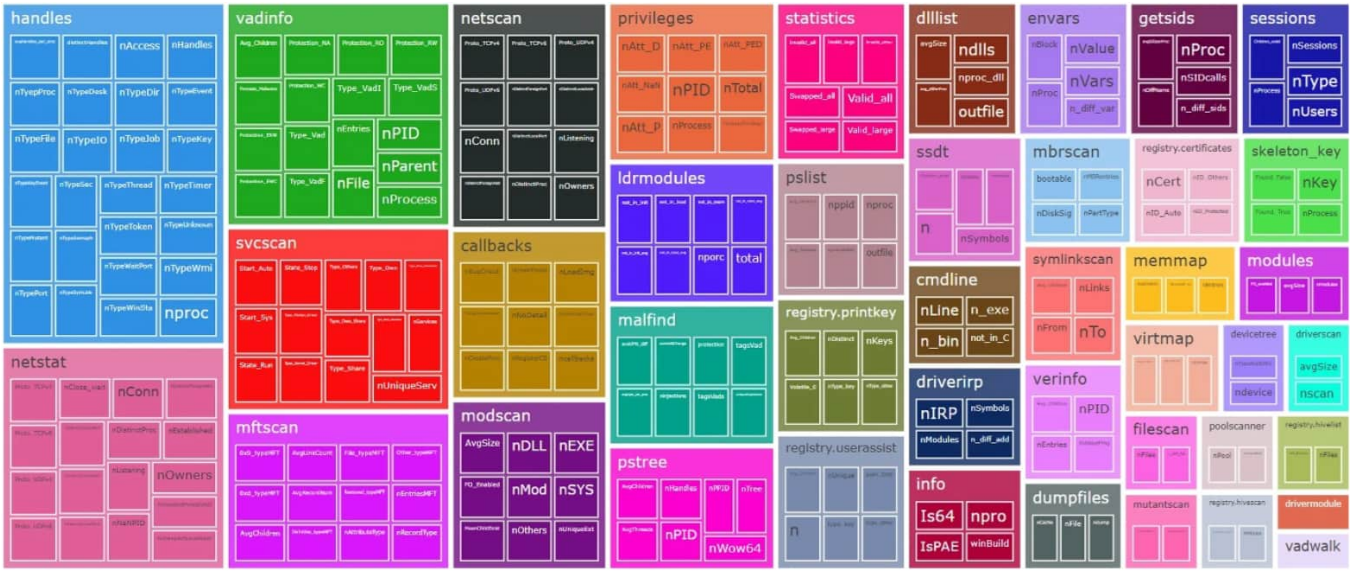


https://www.yorku.ca/research/bccc/Analyzers

VolMemLyzer V1.0, V2.0
Volatile Memory Analyzer

- Memory forensics is essential in cybersecurity and digital forensics, especially for fighting advanced threats and malware. In this dynamic environment, memory analysis tools and methods must be efficient. By prioritising the prominent features in a memory, investigators can speed up their analysis. The VolMemLyzer (Volatile Memory Analyzer) can extract over 250 features from memory snapshots, speeding up analysis and enabling deeper explorations. It serves as a catalyst for memory forensics research and innovation.

- The new VolMemLyzer-V2 is a tool based on functional programming paradigm with dependencies on up-dated Volatility3 Framework based on python 3.



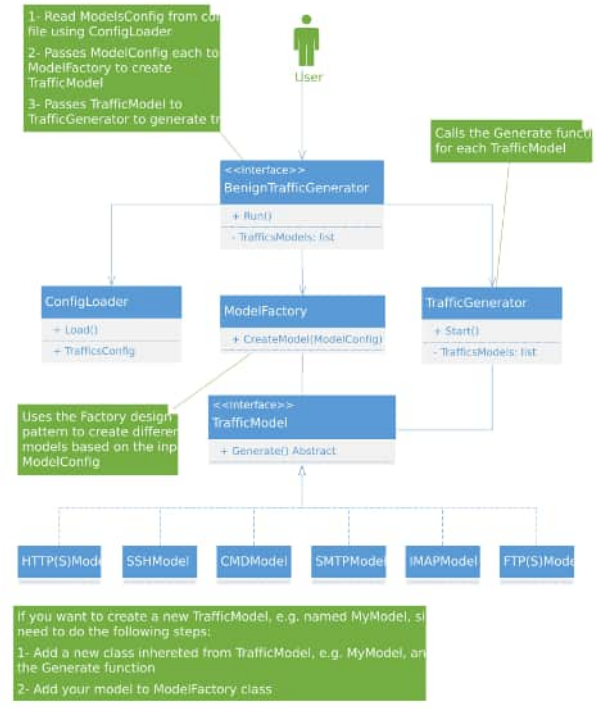
https://www.yorku.ca/research/bccc/Analyzers

BCCC Behaviour-Centric Cybersecurity Center

BUP V1.0
Benign User Profiler

- Benign User Profiler (BUP), part of the Understanding Cybersecurity Series (UCS), is an open-source Python project designed to capture and model normal user behavior across systems and networks. Instead of focusing only on malicious activity, BUP emphasizes benign actions, creating accurate baselines that improve the reliability of anomaly detection.

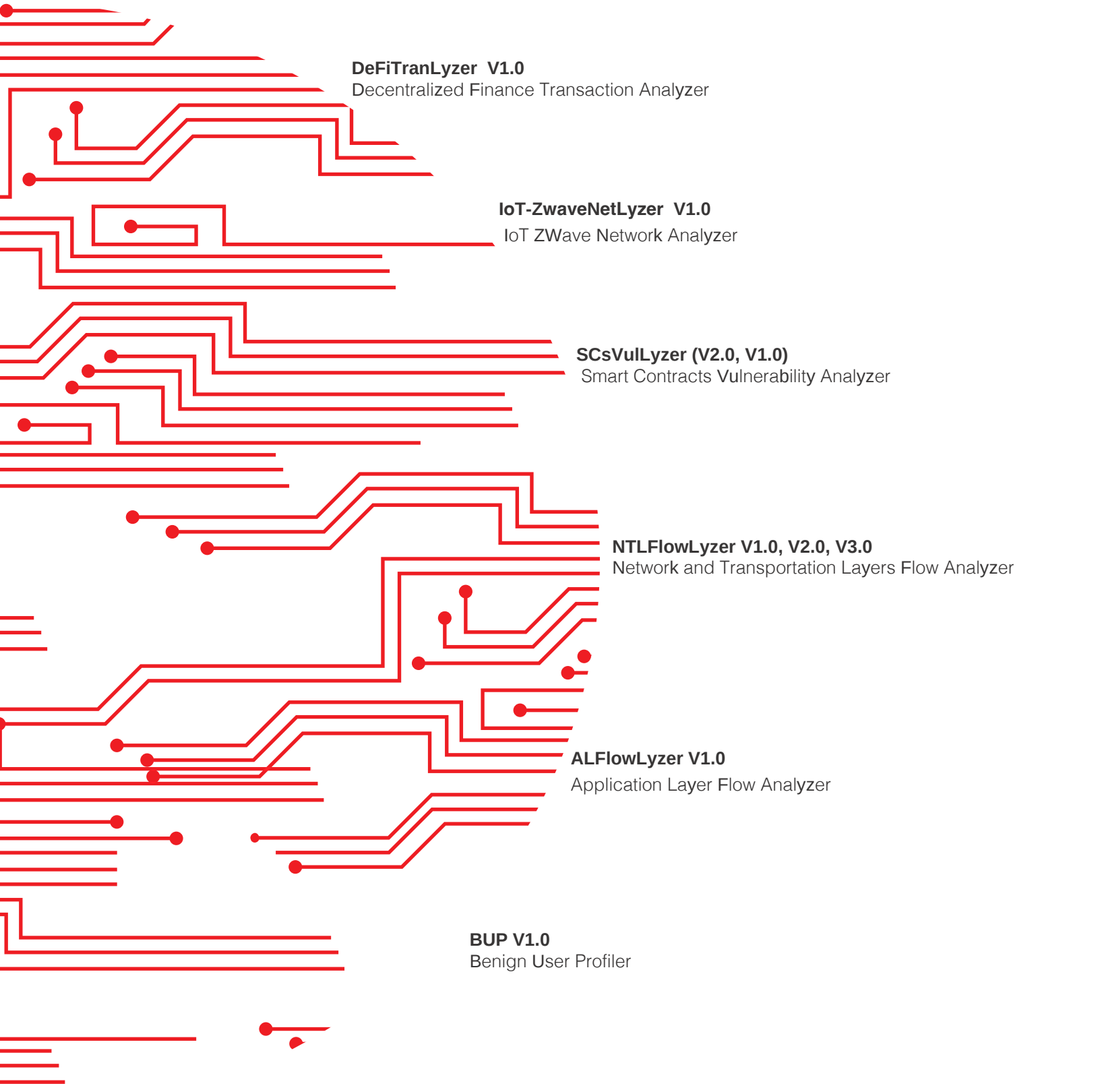
- The framework extracts and analyzes behavioral features to build structured profiles of typical user activities. These profiles can be used to support machine learning models, enhance behavioral analytics, and reduce false positives, ultimately strengthening cybersecurity solutions with a clearer distinction between normal and ab-normal behaviors.



https://www.yorku.ca/research/bccc/Analyzers

Understanding Cybersecurity Series (UCS)

Analyzer Series



DeFiTranLyzer V1.0
Decentralized Finance Transaction Analyzer

IoT-ZwaveNetLyzer V1.0
IoT ZWave Network Analyzer

SCsVulLyzer (V2.0, V1.0)
Smart Contracts Vulnerability Analyzer

NTLFlowLyzer V1.0, V2.0, V3.0
Network and Transportation Layers Flow Analyzer

ALFlowLyzer V1.0
Application Layer Flow Analyzer

BUP V1.0
Benign User Profiler

BCCC
Behaviour-Centric Cybersecurity Center

BCCC
Behaviour-Centric
Cybersecurity Center

Understanding Cybersecurity Series (UCS)

Dataset Series

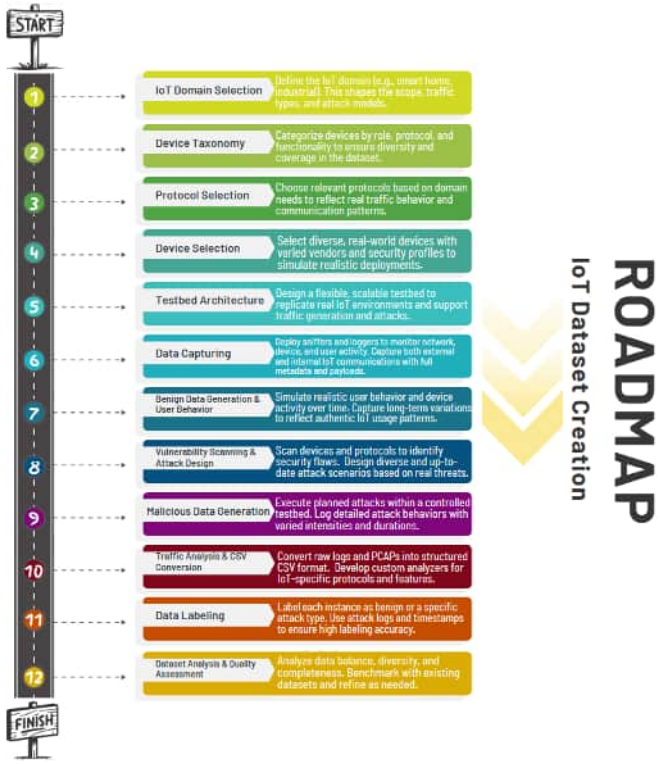
Access Our Cybersecurity Datasets: Trusted Resources for Research, Training, Testing, Evaluation and Innovation

https://www.yorku.ca/research/bccc/Datasets

BCCC-IoT-IDS-ZWzve-2025

IoT ZWave Intrusion Detection Network Traffic

- The BCCC-IoT-IDS-Zwave-2025 dataset is a large-scale, multi-source IoT intrusion detection dataset developed at York University's Behaviour-Centric Cybersecurity Centre (BCCC). It was created over five months using a realistic smart home testbed with more than 50 IoT devices and 88 distinct attack scenarios, capturing both IP-based and Z-Wave protocol communications — a first of its kind to integrate these layers in a unified dataset. The dataset encompasses multi-modal data sources including Z-Wave traffic, IP network traffic, MQTT logs, and device activity records, providing a comprehensive view of smart home behavior under benign and malicious conditions.
- To enable deep protocol-aware analysis, the research team designed IoT-ZwaveNetLyzer, the first dedicated Z-Wave traffic analyzer capable of extracting over 400 features from network flows. The dataset is publicly available through BCCC's GitHub repository and serves as a benchmark for researchers focusing on device profiling, anomaly detection, and multi-protocol IoT threat analysis. By combining realistic smart home traffic with extensive attack scenarios and diverse communication protocols, the BCCC-IoT-IDS-Zwave-2025 dataset represents a major advancement in cybersecurity dataset creation and supports the development of next generation IoT intrusion detection systems.

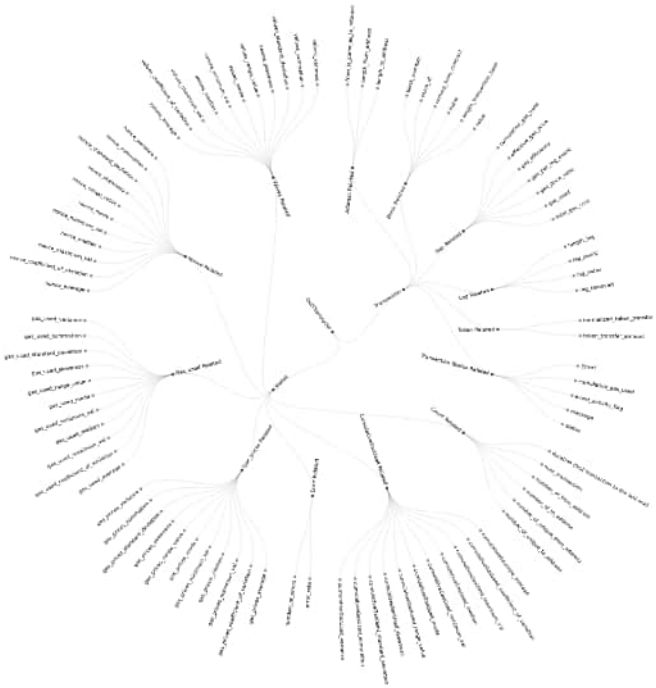


https://www.yorku.ca/research/bccc/Datasets

BCCC-DeFiFraudTrans-2025
DeFi Fraud Transactions

- BCCC-DeFiFraudTrans-2025 is a large-scale, Ethereum-based benchmark designed explicitly for profiling fraudulent and legitimate DeFi transactions. It contains 1,026,867 annotated transaction samples spanning from 2017 to 2024, drawn from 9,374 unique wallet addresses. The dataset integrates both wallet-level and transaction-level attributes, with 79 features extracted via the DeFiTransLyzer-V1.0 analyzer. These features are organized into categories, including gas usage, cumulative gas consumption, token transfers, nonce behavior, block identifiers, transaction status, and error rates, providing a fine-grained view of transaction dynamics.

- Unlike many prior datasets, BCCC-FraudDefi-2025 was curated to be balanced, feature-rich, and validated: fraudulent labels were assigned based on Etherscan tags and then cross-checked with anomaly detection, consistency verification, and duplicate removal. The dataset enables evaluation of advanced fraud detection methods, including zero-day attacks, by eliminating reliance on prior wallet history and focusing purely on transaction-level behavior.



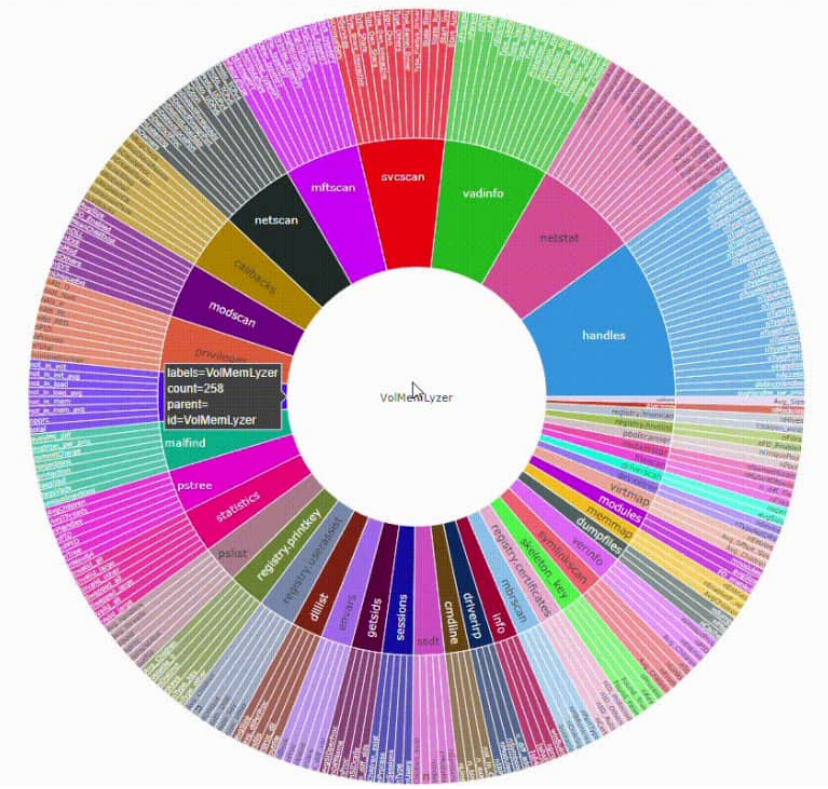
https://www.yorku.ca/research/bccc/Datasets

BCCC-Mal-NetMem-2025

Large-Scale Multisources Malware Analysis Dataset using Network Traffic and Memory

- The BCCC-Mal-NetMem-2025 dataset comprises over 7.7 million labeled records from controlled experiments involving 15 malware categories and 32 individual malware samples. These categories include ransomware, Trojan downloaders, coin miners, remote access tools (RATs), spyware, backdoors, and worms. The data was collected by executing each malware in isolated Windows environments equipped with real-time network and memory monitoring tools to ensure comprehensive behavioral capture.

- The dataset integrates memory and network traffic features, offering a multidimensional view of malware behavior for accurate profiling. This hybrid structure allows advanced AI-driven threat detection and malware characterization, consistent labeling, and session-based organization that supports detailed analysis. The BCCC-Mal-NetMem-2025 is a unique benchmark for behavioral malware analysis, bridging gaps between static profiling and real-world execution patterns.

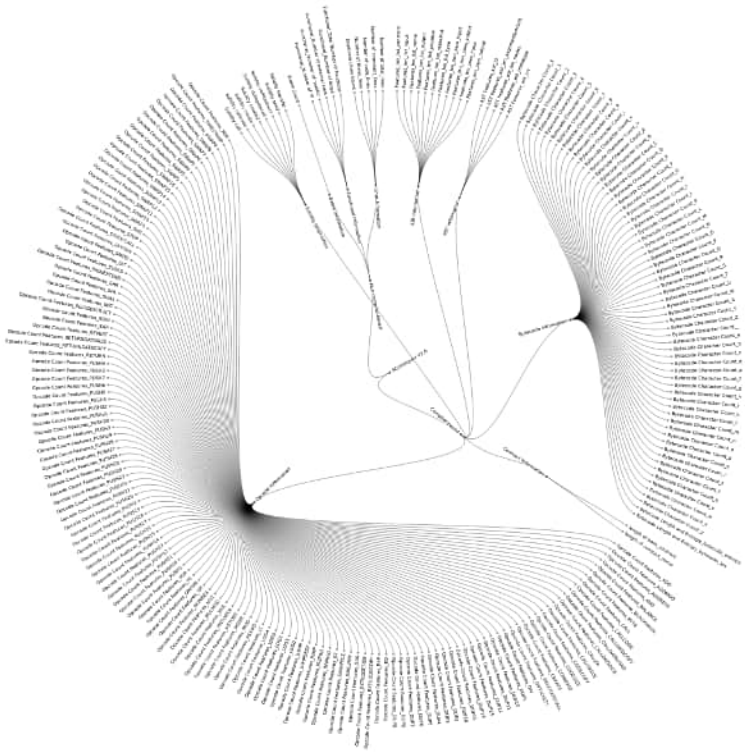


https://www.yorku.ca/research/bccc/Datasets

BCCC-SCsVuls-2024

Smart Contracts Vulnerabilities

- BCCC-SCsVuls-2024 is a large-scale dataset designed for analyzing and detecting vulnerabilities in Solidity-based smart contracts. It contains 111,897 labeled samples covering 11 major vulnerability types, including Re-entrancy (17,698), IntegerUO (16,740), Denial of Service (12,394), and 26,914 Secure contracts. Curated from trusted sources such as Smart Bugs, Ethereum SCs, and SmartScan-Dataset, it offers a diverse and representative collection to support blockchain security research.

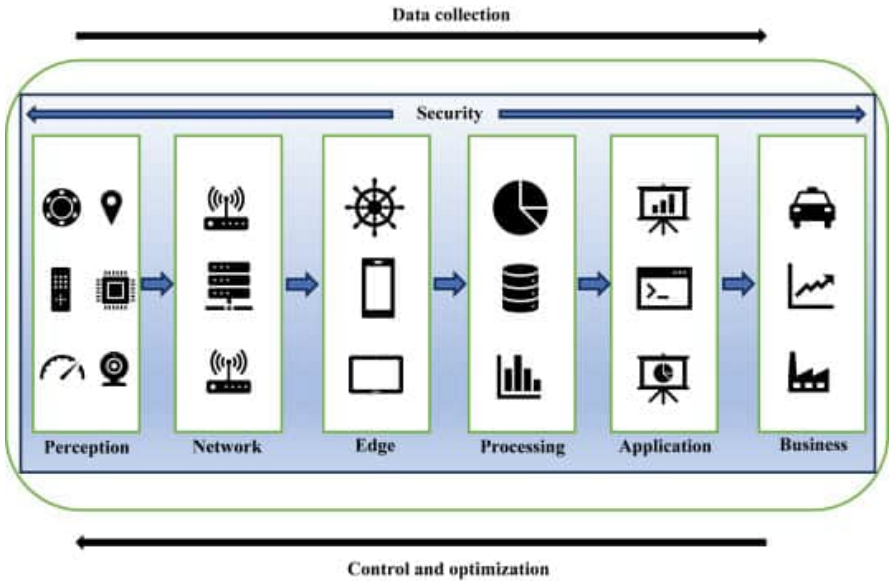


https://www.yorku.ca/research/bccc/Datasets

CIC-BCCC-NRC TabularIoTAttack-2024

Tabular IoT Attack Dataset

- The CIC-BCCC-NRC TabularIoTAttack-2024 dataset is a comprehensive collection of IoT network traffic data generated as part of an advanced effort to create a reliable source for training and testing AI-powered IoT cybersecurity models. This dataset is designed to address modern challenges in detecting and identifying IoT-specific cyberattacks, offering a rich and diverse set of labeled data that reflects realistic IoT network behaviours. The dataset extracted a wide array of network characteristics using CICFlowMeter, with each record containing relevant features such as network flows, timestamps, source/destination IPs, and attack labels.



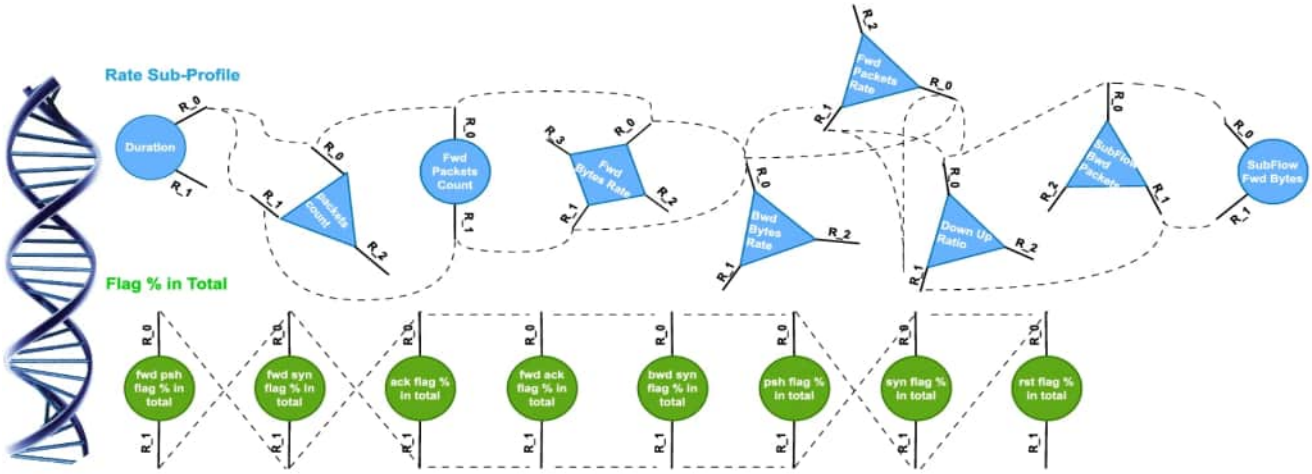
https://www.yorku.ca/research/bccc/Datasets

BCCC-CSE-CIC-IDS2018

Large-Scale Intrusion Detection Dataset

- The BCCC-CSE-CIC-IDS2018 dataset is an enhanced version of CSE-CIC-IDS2018 with 46 million labelled records and 300 features, addressing key issues to improve data quality and reliability for behavioral profiling in IDS research. Labeling inconsistencies, particularly for DoS attacks, were corrected by aligning attack labels with attacker IPs instead of timestamps. NTLFlowLyzer, a new network traffic analyzer, was developed to resolve anomalies in extracted features and refine feature implementation.

- Additionally, protocol issues were fixed by removing UDP-based attacks previously misclassified due to TCP-specific analysis. Attacks with insufficient flow counts were retained but excluded from analysis and profiling. The dataset now includes an expanded feature set to detect evolving cyber threats better, making it a robust benchmark for AI-driven IDS/IPS research.

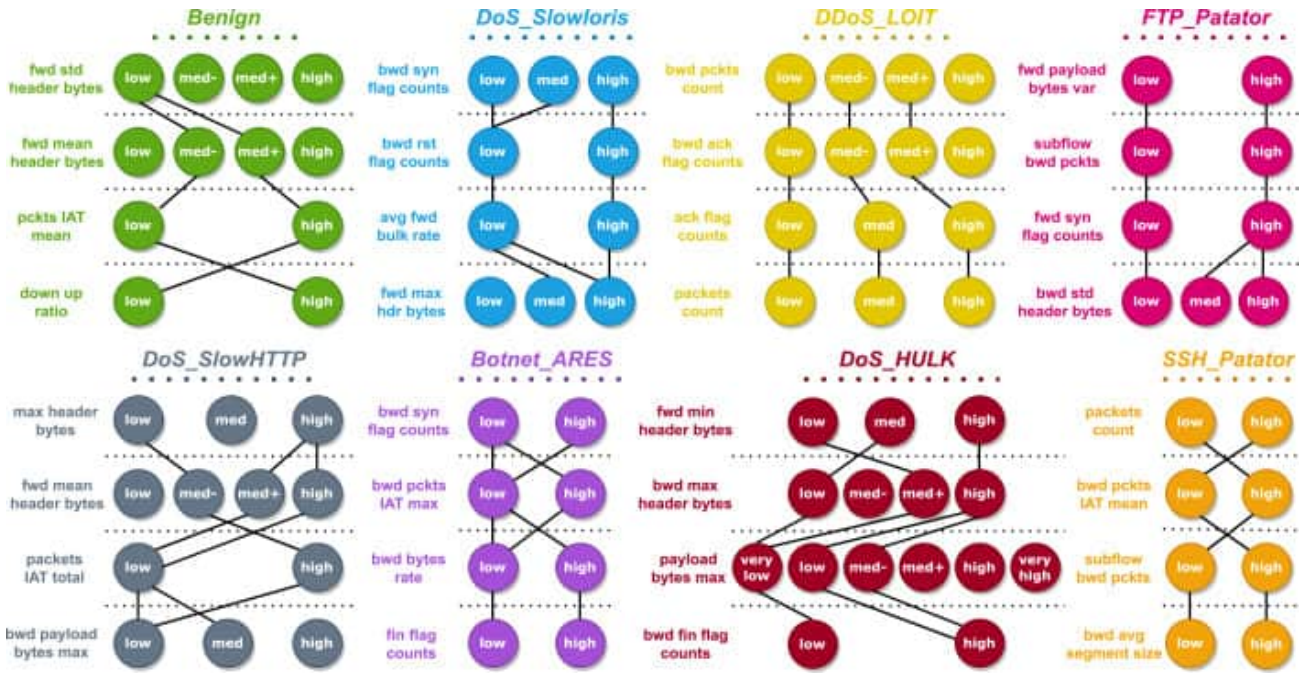


https://www.yorku.ca/research/bccc/Datasets

BCCC-CIC-IDS2017

Intrusion Detection Dataset

- Using NLFlowLyzer, we successfully generated the “BCCC-CIC-IDS2017” dataset by extracting key flows from raw network traffic data of CIC-IDS2017, resulting in CSV files integrating essential network and transport layer features. This new dataset offers a structured approach for analyzing intrusion detection, combining diverse traffic types into multiple sub-categories. The “BCCC-CIC-IDS2017” dataset enriches the depth and variety needed to rigorously evaluate our proposed profiling model, advancing research in network security and enhancing the development of intrusion detection systems.



https://www.yorku.ca/research/bccc/Datasets

BCCC-DarkNet-2025

Encrypted Traffic Dataset

- BCCC-DarkNet-2025 is an augmented, research-driven dataset that supports encrypted traffic analysis and threat detection across anonymized communication networks. It integrates and extends two benchmark datasets, CIC-Darknet2020 and Darknet-Dataset-2020, selected for their robust coverage of encryption protocols and darknet-specific traffic behaviors. The dataset includes diverse encrypted traffic types like VPN, Tor, I2P, Freenet, and ZeroNet, with multi-class labeling and protocol-specific annotations. These sources were chosen based on well-defined criteria, including support for time-dependent patterns, entropy measures, and behavioral features critical to identifying obfuscated malicious activities.

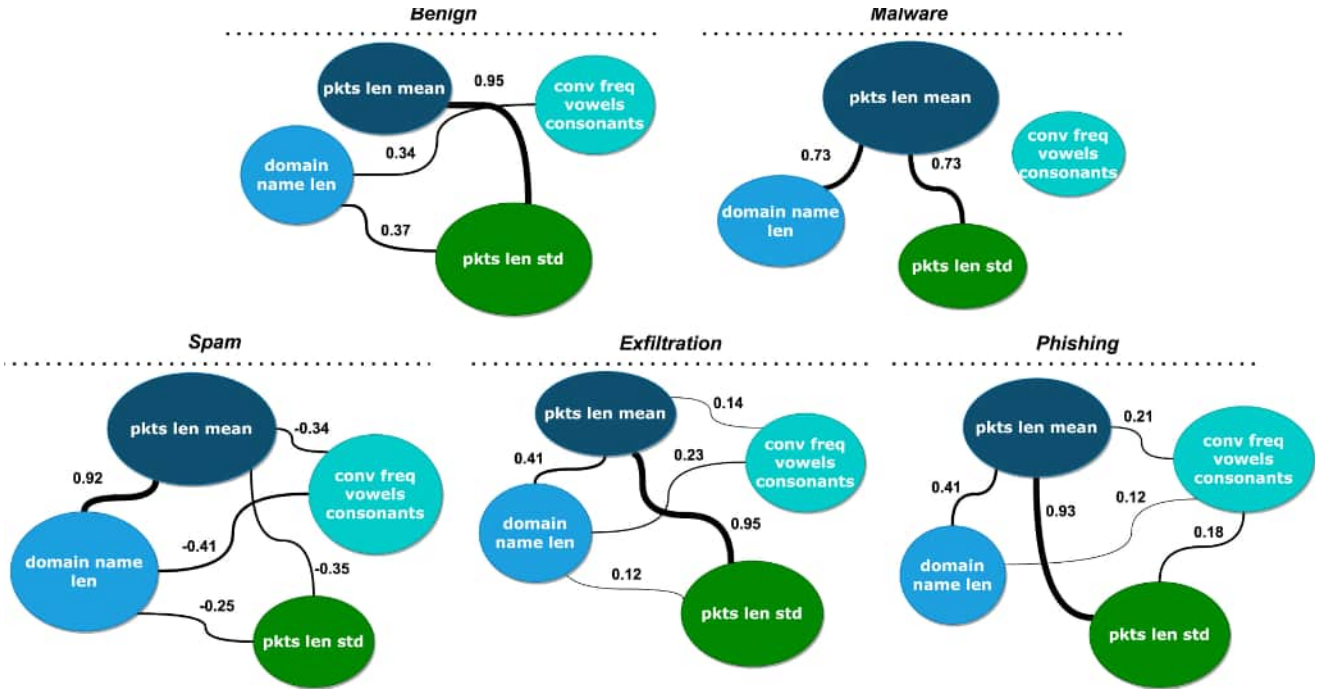
- The dataset has been standardized to ensure consistency and scalability using NTLFlowLyzer-V3, a custom flow-based feature extractor. This preprocessing step harmonizes temporal, statistical, and protocol-level features across both datasets, enabling seamless integration into machine learning pipelines. The result is BCCC-DarkNet-2025, a unified and enriched dataset that significantly improves classifier performance in encrypted traffic scenarios by capturing structural and behavioral anomalies. It is a valuable resource for developing AI-powered cybersecurity solutions in dynamic and evasive threat environments.

https://www.yorku.ca/research/bccc/Datasets

BCCC-CIC-Bell-DNS-2024

Malicious DNS and Attacks

- Using ALFlowLyzer, we successfully generated an augmented dataset, "BCCC-CIC-Bell-DNS-2024," from two existing datasets: "CIC-Bell-DNS-2021" and "CIC-Bell-DNS-EXF-2021." ALFlowLyzer enabled the extraction of essential flows from raw network traffic data, resulting in CSV files that integrate DNS metadata and application layer features. This new dataset combines light and heavy data exfiltration traffic into six unique sub-categories, providing a comprehensive structure for analyzing DNS data exfiltration attacks. The "BCCC-CIC-Bell-DNS-2024" dataset enhances the richness and diversity needed to effectively evaluate our proposed profiling model.

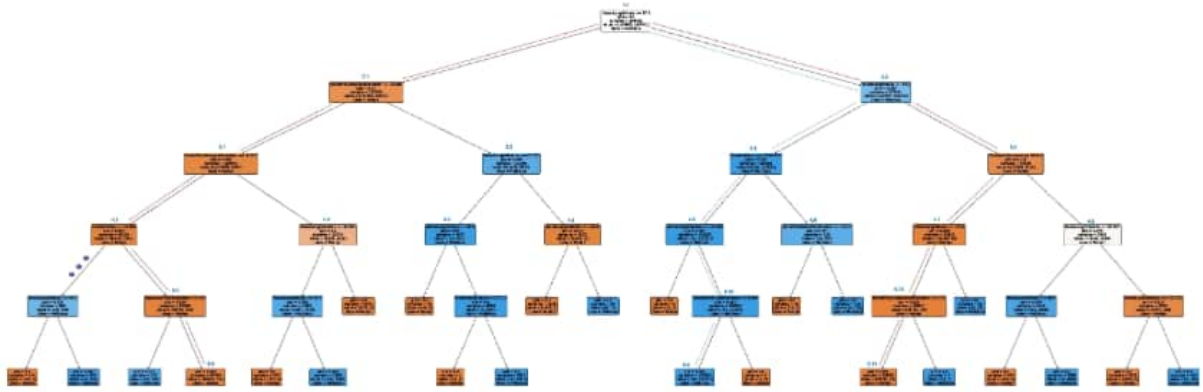


https://www.yorku.ca/research/bccc/Datasets

BCCC-CIRA-CIC-DoHBrw-2020

DNS over HTTPS

- The 'BCCC-CIRA-CIC-DoHBrw-2020' dataset was created to address the imbalance in the 'CIRA-CIC-DoBre-2020' dataset. Unlike the 'CIRA-CIC-DoHBrw-2020' dataset, which is skewed with about 90% malicious and only 10% benign Domain over HTTPS (DoH) network traffic, the 'BCCC-CIRA-CIC-DoHBrw-2020' dataset offers a more balanced composition. It includes equal numbers of malicious and benign DoH network traffic instances, with 249,836 instances in each category. This balance was achieved using the Synthetic Minority Over-sampling Technique (SMOTE). The 'BCCC-CIRA-CIC-DoHBrw-2020' dataset comprises three CSV files: one for malicious DoH traffic, one for benign DoH traffic, and a third that combines both types.



https://www.yorku.ca/research/bccc/Datasets

Understanding Cybersecurity Series (UCS)

Dataset Series

BCCC-Mal-NetMem-2025
Large-Scale Multisources Malware Analysis Dataset using Network Traffic and Memory

BCCC-IoT-IDS-ZWzve-2025
IoT ZWave Intrusion Detection Network Traffic

BCCC-SCsVuls-2024
Smart Contracts Vulnerabilities

CIC-BCCC-NRC TabularIoTAttack-2024
Tabular IoT Attack Dataset

BCCC-CIC-IDS2017
Intrusion Detection Dataset

BCCC-DeFiFraudTrans-2025
DeFi Fraud Transactions

BCCC-CSE-CIC-IDS2018
Large-Scale Intrusion Detection Dataset

BCCC-DarkNet-2025
Encrypted Traffic Dataset

BCCC-CIC-Bell-DNS-2024
Malicious DNS and Attacks

BCCC-CIRA-CIC-DoHBrw-2020
DNS over HTTPS

BCCC
Behaviour-Centric Cybersecurity Center

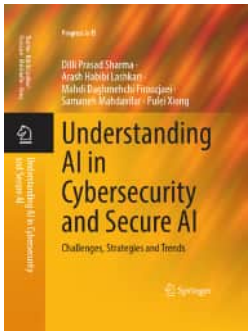
BCCC
Behaviour-Centric
Cybersecurity Center

Understanding Cybersecurity Series (UCS)

BOOK SERIES

Discover Our Published Cybersecurity Books: Essential Reads for Every Enthusiast

https://www.yorku.ca/research/bccc/publications/



BOOK 7

Understanding AI in Cybersecurity and Secure AI: Challenges, Strategies, and Trends

- This book presents an overview of the emerging topics in Artificial Intelligence (AI) and cybersecurity and addresses the latest AI models that could be potentially applied to a range of cybersecurity areas. Furthermore, it provides different techniques of how to make the AI algorithms secure from adversarial attacks. The book presents the cyber threat landscape and explains the various spectrums of AI and the applications and limitations of AI in cybersecurity. Moreover, it explores the applications and limitations of secure AI.
- The authors discuss the three categories of machine learning (ML) models and reviews cutting-edge recent Deep Learning (DL) models. Furthermore, the book provides a general AI framework in security as well as different modules of the framework; similarly, chapter four proposes a general framework for secure AI. It explains different aspects of network security including malware and attacks.
- The book also includes a comprehensive study of various scopes of application security; categorised into three groups of smartphone, web application, and desktop application and delves into the concepts of cloud security. The authors discuss state-of-the-art Internet of Things (IoT) security and describe various challenges of AI for cybersecurity, such as data diversity, model customising, explainability, and time complexity and includes some future work. They provide a comprehensive understanding of adversarial machine learning including the up-to-date adversarial attacks and defences. The book finishes off with a discussion of the challenges and future work in secure AI.

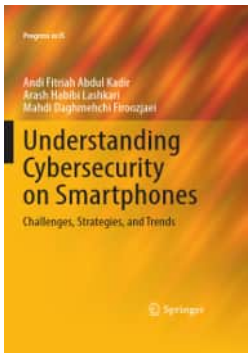
https://www.yorku.ca/research/bccc/publications/

BOOK 6

Understanding Cybersecurity Management in Healthcare: Challenges, Strategies, and Trends

- Digital technology is increasingly used in the healthcare sector, and healthcare organizations handle sensitive and confidential information that needs to be kept secure and protected. Therefore, the importance of cybersecurity in healthcare cannot be overstated. Cyber threats can compromise patient data, disrupt healthcare services, and put personal safety at risk.
- This book provides an understanding of cybersecurity in healthcare, which is crucial for protecting personal information, ensuring compliance with regulations, maintaining patient trust, and preventing cyber-attacks. Before defining cybersecurity in healthcare, the authors introduce the healthcare environment and cybersecurity basics to readers. They then emphasize the importance of data protection and privacy, software, and personal cybersecurity. Also, they highlight the importance of educating staff about cybersecurity. The discussion continues with data and information security in healthcare, including data threats and vulnerabilities, the difference between data protection and privacy, and how to protect data. Afterward, they focus on the software system frameworks and types of infra-security and app security in healthcare.
- By understanding the risks and challenges of cybersecurity in healthcare, healthcare providers and organizations can better protect sensitive and confidential data and ensure the safety and privacy of those they serve.

https://www.yorku.ca/research/bccc/publications/

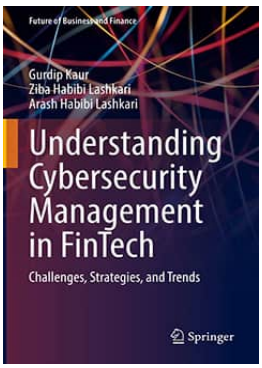


BOOK 5

Understanding Cybersecurity on Smartphones: Challenges, Strategies, and Trends

- This book offers a comprehensive overview of smartphone security, focusing on various operating systems and their associated challenges. It covers the smartphone industry's evolution, emphasizing security and privacy concerns. It explores Android, iOS, and Windows OS security vulnerabilities and mitigation measures. Additionally, it discusses alternative OSs like Symbian, Tizen, Sailfish, Ubuntu Touch, KaiOS, Sirin, and HarmonyOS.
- The book also addresses mobile application security, best practices for users and developers, Mobile Device Management (MDM) in enterprise settings, mobile network security, and the significance of mobile cloud security and emerging technologies such as IoT, AI, ML, and blockchain. It discusses the importance of balancing innovation with solid security practices in the ever-evolving mobile technology landscape.

https://www.yorku.ca/research/bccc/publications/



BOOK 4

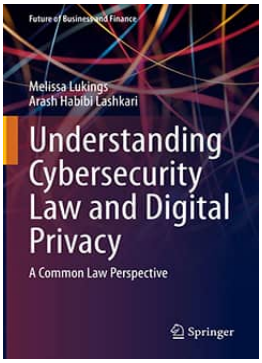
Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends

- This book uncovers the idea of understanding cybersecurity management in FinTech. It commences with introducing fundamentals of FinTech and cybersecurity to readers. It emphasizes on the importance of cybersecurity for financial institutions by illustrating recent cyber breaches, attacks, and financial losses. The book delves into understanding cyber threats and adversaries who can exploit those threats. It advances with cybersecurity threat, vulnerability, and risk management in FinTech.

- The book helps readers understand cyber threat landscape comprising different threat categories that can exploit different types of vulnerabilties identified in FinTech. It puts forward prominent threat modelling strategies by focusing on attackers, assets, and software and addresses the challenges in managing cyber risks in FinTech.

- The authors discuss detailed cybersecurity policies and strategies that can be used to secure financial institutions and provide recommendations to secure financial institutions from cyber-attacks.

https://www.yorku.ca/research/bccc/publications/



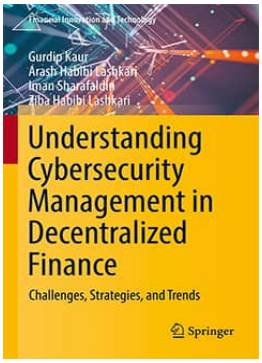
BOOK 3

Understanding Cybersecurity Law and Digital Privacy: A Common Law Perspective

- Cybersecurity, data privacy law, and the related legal implications overlap into a relevant and developing area in the legal field. However, many legal practitioners lack the foundational understanding of computer processes which are fundamental for applying existing and developing legal structures to the issue of cyber-security and data privacy. At the same time, those who work and research in cybersecurity are often unpre-pared and unaware of the nuances of legal application.

- This book translates the fundamental building blocks of data privacy and (cyber)security law into basic knowledge that is equally accessible and educational for those working and researching in either field, those who are involved with businesses and organizations, and the general public.

https://www.yorku.ca/research/bccc/publications/



BOOK 2

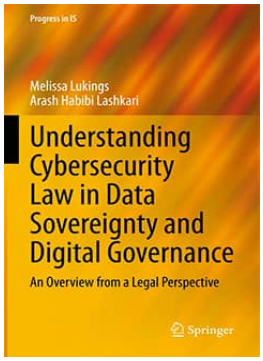
Understanding Cybersecurity Management in Decentralized Finance: Challenges, Strategies, and Trends

- This book discusses understand cybersecurity management in decentralized finance (DeFi). It commences with introducing fundamentals of DeFi and cybersecurity to readers. It emphasizes on the importance of cybersecurity for decentralized finance by illustrating recent cyber breaches, attacks, and financial losses. The book delves into understanding cyber threats and adversaries who can exploit those threats. It advances with cybersecurity threat, vulnerability, and risk management in DeFi. The book helps readers understand cyber threat landscape comprising different threat categories for that can exploit different types of vulnerabilities identified in DeFi. It puts forward prominent threat modelling strategies by focusing on attackers, assets, and software.

- The book includes the popular blockchains that support DeFi include Ethereum, Binance Smart Chain, Solana, Cardano, Avalanche, Polygon, among others. With so much monetary value associated with all these technologies, theperpetrators are always lured to breach security by exploiting the vulnerabilities that exist in these technologies. For simplicity and clarity, all vulnerabilities are classified into different categories: arithmetic bugs, re-Entrancy attack, race conditions, exception handling, using a weak random generator, timestamp dependency, transaction-ordering dependence and front running, vulnerable libraries, wrong initial assumptions, denial of service, flash loan attacks, and vampire..

- Since decentralized finance infrastructures are the worst affected by cyber-attacks, it is imperative to understand various security issues in different components of DeFi infrastructures and proposes measures to secure all components of DeFi infrastructures. It brings the detailed cybersecurity policies and strategies that can be used to secure financial institutions. Finally, the book provides recommendations to secure DeFi infrastructures from cyber-attacks.

https://www.yorku.ca/research/bccc/publications/



BOOK 1

Understanding Cybersecurity Law in Data Sovereignty and Digital Governance: An Overview from a Legal Perspective

- This book provides an overview of the topics of data, sovereignty, and governance with respect to data and online activities through a legal lens and from a cybersecurity perspective. This first chapter explores the concepts of data, ownerships, and privacy with respect to digital media and content, before defining the intersection of sovereignty in law with application to data and digital media content. The authors delve into the issue of digital governance, as well as theories and systems of governance on a state level, national level, and corporate/organizational level. Chapter three jumps into the complex area of jurisdictional conflict of laws and the related issues regarding digital activities in international law, both public and private.
- Additionally, the book discusses the many technical complexities which underlay the evolution and creation of new law and governance strategies and structures. This includes socio-political, legal, and industrial technical complexities which can apply in these areas. The fifth chapter is a comparative examination of the legal strategies currently being explored by a variety of nations. The book concludes with a discussion about emerging topics which either influence, or are influenced by, data sovereignty and digital governance, such as indigenous data sovereignty, digital human rights and self-determination, artificial intelligence, and global digital social responsibility.
- Cumulatively, this book provides the full spectrum of information, from foundational principles underlining the described topics, through to the larger, more complex, evolving issues which we can foresee ahead of us.

https://www.yorku.ca/research/bccc/publications/

Understanding Cybersecurity Series (UCS)

BOOK Series

Understanding AI in Cybersecurity and Secure AI
Challenges, Strategies, and Trends

Understanding Cybersecurity Management in Healthcare
Challenges, Strategies, and Trends

Understanding Cybersecurity Management in FinTech
Challenges, Strategies, and Trends

Understanding Cybersecurity On Smartphones
Challenges, Strategies, and Trends

Understanding Cybersecurity Law and Digital Privacy
A Common Law Perspective

Understanding Cybersecurity Management in Decentralized Finance
Challenges, Strategles, and Trends

Understanding Cybersecurity Law in Data Sovereignty and Digital Governance:
An Overview from a Legal Perspective

BCCC
Behaviour-Centric Cybersecurity Center

BCCC
Behaviour-Centric
Cybersecurity Center

Understanding Cybersecurity Series (UCS)
Blog Series

Read Our Cybersecurity Blogs: Insights, Trends, and Expert Prespectives

https://www.yorku.ca/research/bccc/blog/

Blog 8

Understanding AI in Cybersecurity and Secure AI (UCSecAI)

- Understanding AI in Cybersecurity and AI Security: AI Safety and Fairness Nowadays: Explained (UCSAISec-05)
- Understanding AI in Cybersecurity and AI Security: Defense Methods for Adversarial Attacks and Privacy Issues in Secure AI (UCSAISec-04)
- Understanding AI in Cybersecurity and AI Security: AI Security and Privacy (UCSAISec-03)
- Understanding AI in Cybersecurity and AI Security: AI in IoT and OT Security (UCSAISec-02)
- Understanding AI in Cybersecurity and AI Security: AI in Cybersecurity (UCSAISec-01)

https://www.yorku.ca/research/bccc/blogs/

Blog 7

Understanding Cybersecurity on Healthcare (UCSHC)

- Understanding Cybersecurity Management in Healthcare (UCSMH) - Cybersecurity Challenges, Best Practices, and Future Work in Healthcare (Article 4)
- Understanding Cybersecurity Management in Healthcare: Cybersecurity Governance and Ethics in Healthcare (Article 3)
- Understanding Cybersecurity Management in Healthcare: Detection and Prevention of Cyber-attacks in Healthcare (Article 2)
- Understanding Cybersecurity Management in Healthcare (UCSMH) - Defining Cybersecurity in Healthcare (Article 1)

https://www.yorku.ca/research/bccc/blog/

Blog 6

Understanding Cybersecurity on SmartPhones (UCSPh)

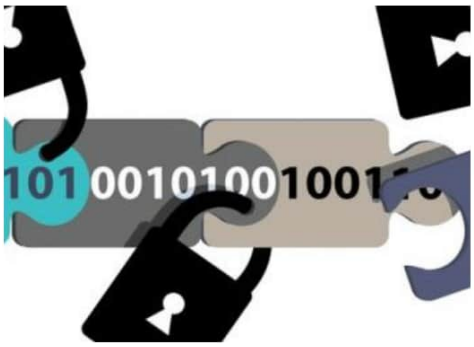
- Understanding Cybersecurity management in Healthcare: Cybersecurity Cybersecurity Challenges, Best Practices, and Future Work in Healthcare (Article 4)
- Understanding Cybersecurity management in Healthcare: Detection and Prevention of Cyberattacks in Healthcare (Article 2)
- Understanding Cybersecurity management in Healthcare: Cybersecurity Governance and Ethics in Healthcare (Article 3)
- Understanding Cybersecurity management in Healthcare: Defining Cybersecurity in Healthcare (Article 1)

https://www.yorku.ca/research/bccc/blog/

Blog 5

Understanding Cybersecurity Management in DeFi (UCM-DeFi)

- Understanding Cybersecurity Management in DeFi (UCM-DeFi) – Smart Contracts and DeFi Security and Threats (Article 5)
- Understanding Cybersecurity Management in DeFi (UCM-DeFi) – Blockchain Security (Article 4)
- Understanding Cybersecurity Management in DeFi (UCM-DeFi) – DeFi Platforms (Article 3)
- Understanding Cybersecurity Management in DeFi (UCM-DeFi) – Introduction to Smart Contracts and DeFi (Article 2)
- Understanding Cybersecurity Management in DeFi (UCM-DeFi) – The Origin of Modern Decentralized Finance (Article 1)



https://www.yorku.ca/research/bccc/blog/

Blog 4

Understanding Current Cybersecurity Challenges in Law (UCCCL)

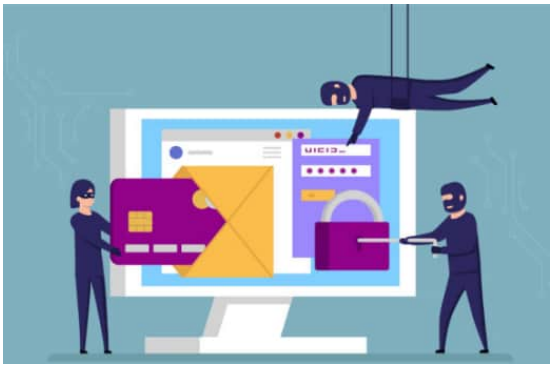
- Understanding current cybersecurity challenges in law (UCCCL) - Legal Considerations for Artificial Intelligence and Technological Development (Article 6)
- Understanding current cybersecurity challenges in law: Data Breaches and Increased Data Awareness (Article 5)
- Understanding current cybersecurity challenges in law: balancing responsibilities in digital content censorship (Article 4)
- Understanding current cybersecurity challenges in law: determining online jurisdictional authority (Article 3)
- Understanding current cybersecurity challenges in law: digital governance and social responsibility meet user-generated content (Article 2)
- Understanding current cybersecurity challenges in law: data sovereignty & cross-border data transfers (Article 1)

https://www.yorku.ca/research/bccc/blog/

Blog 3

Understanding Cybersecurity management for FinTech (UCM-FinTech)

- Understanding cybersecurity management for FinTech: cybersecurity policy and strategy management (Article 6)
- Understanding cybersecurity management for FinTech: security issues on financial market infrastructures (Article 5)
- Understanding cybersecurity management for FinTech: cybersecurity vulnerabilities and risk in FinTech (Article 4)
- Understanding cybersecurity management for FinTech: cybersecurity threats in FinTech (Article 3)
- Understanding cybersecurity management for FinTech : information security governance in FinTech (Article 2)
- Understanding cybersecurity management for FinTech (UCMF) - introduction to FinTech and the importance of security objects (Article 1)



https://www.yorku.ca/research/bccc/blog/

Blog 2

Understanding Android Malware Families (UAMF)

- Understanding Android Malware Families (UAMF) – Adware and Backdoor (Article 5)
- Understanding Android Malware Families (UAMF) – Riskware – is it worth it? (Article 4)
- Understanding Canadian Cybersecurity Laws: refactored — our series in summary (Article 10)
- Understanding Android Malware Families (UAMF) – Ransomware and scareware (Article 3)
- Understanding Android Malware Families (UAMF) – The Trojan: An impersonator in the background (Article 2)
- Understanding Android Malware Families (UAMF) – The Foundations (Article 1)

https://www.yorku.ca/research/bccc/blog/

Blog 1

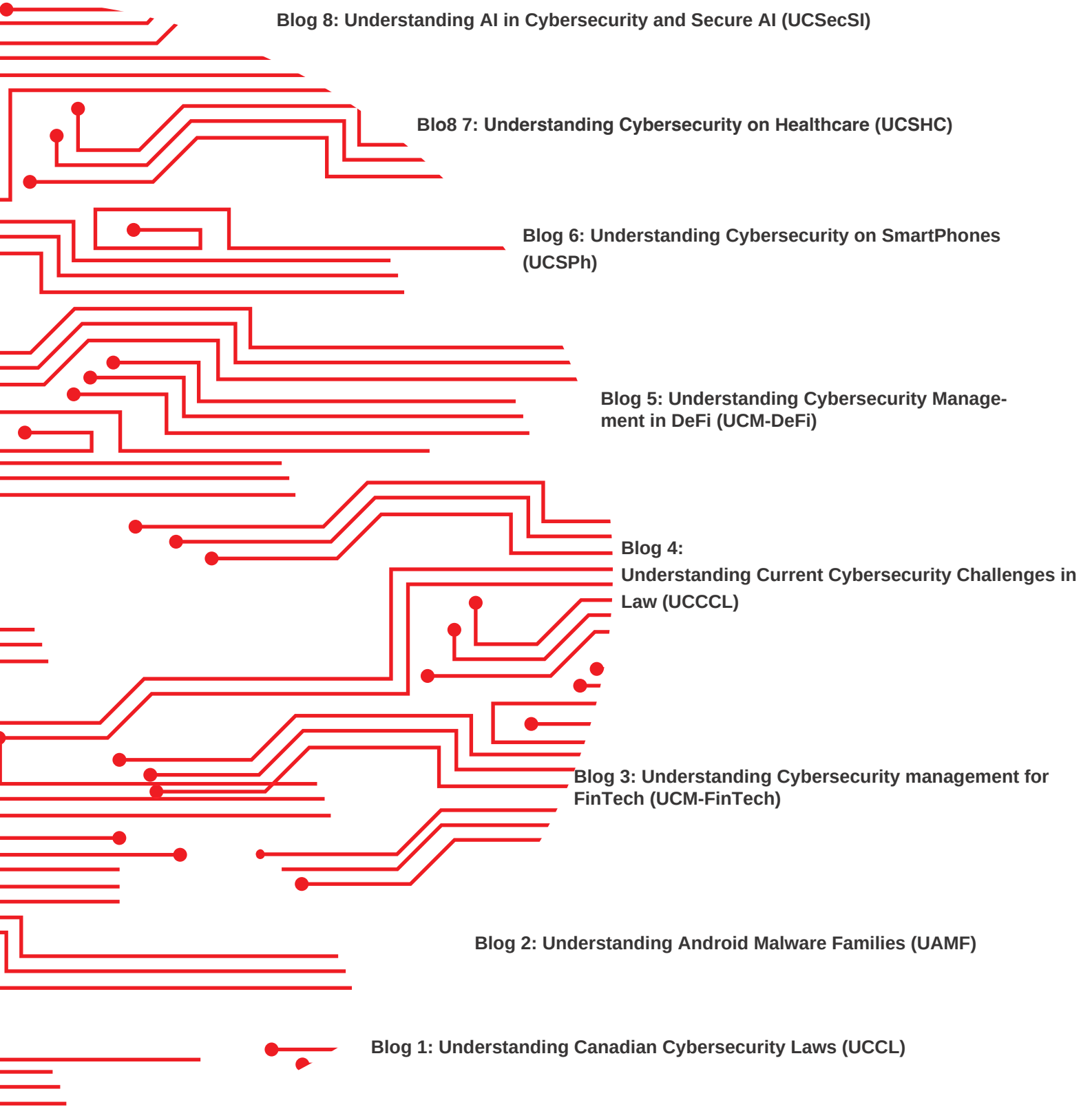
Understanding Canadian Cybersecurity Laws (UCCL)

- Understanding Canadian Cybersecurity Laws: refactored — our series in summary (Article 10)
- Understanding Canadian Cybersecurity Laws: Legislative Modernization — Responding and Adapting to Technological Change in a Global Domain (Article 9)
- Understanding Canadian Cybersecurity Laws: Measuring Up — Outlining Existing National Cybersecurity Legislation in Canada, the UK, Australia, and the US (Article 8)
- Understanding Canadian cybersecurity laws: Deep, dark, and undetectable – Canadian jurisdictional considerations in global encrypted networks (Article 7)
- Understanding Canadian cybersecurity laws: Peer-to-peer privacy protection - “Intrusion upon seclusion” and the protection of intimate images (Article 6)
- Understanding Canadian Cybersecurity Laws: Insert Something Clever Here - Canada’s Anti-Spam Legislation (Article 5)
- Understanding Canadian Cybersecurity Laws: Interpersonal Privacy and Cybercrime - Criminal Code of Canada (Article 4)
- Understanding Canadian cybersecurity laws: Privacy Protection in the Modern Marketplace-PIPEDA (Article 3)
- Understanding Canadian cybersecurity laws: Privacy and access to information, the Acts (Article 2)
- Understanding Canadian cybersecurity laws: the foundations (Article 1)

https://www.yorku.ca/research/bccc/blog/

Understanding Cybersecurity Series (UCS)

Blog Series



Blog 8: Understanding AI in Cybersecurity and Secure AI (UCSecSI)

Blo8 7: Understanding Cybersecurity on Healthcare (UCSHC)

Blog 6: Understanding Cybersecurity on SmartPhones (UCSPh)

Blog 5: Understanding Cybersecurity Management in DeFi (UCM-DeFi)

Blog 4: Understanding Current Cybersecurity Challenges in Law (UCCCL)

Blog 3: Understanding Cybersecurity management for FinTech (UCM-FinTech)

Blog 2: Understanding Android Malware Families (UAMF)

Blog 1: Understanding Canadian Cybersecurity Laws (UCCL)

BCCC
Behaviour-Centric Cybersecurity Center

BCCC
Behaviour-Centric
Cybersecurity Center

Understanding Cybersecurity Series (UCS)
Workshop Series

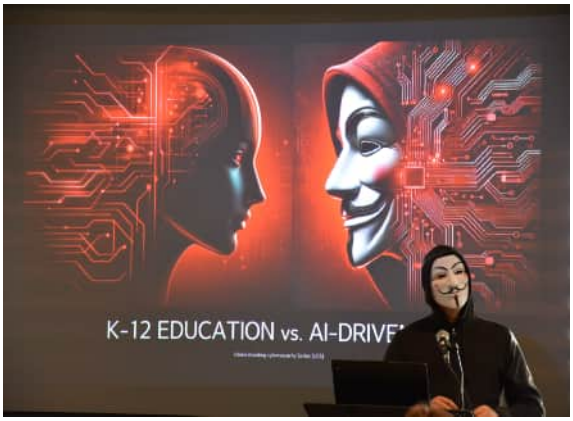
Empowering Cybersecurity Learning Through Workshops and Talks

https://www.yorku.ca/research/bccc/Workshops

Workshops

Understanding Cybersecurity Series Workshops (UCSW)

- Elevating Cybersecurity Vigilance: Fusing Knowledge Dissemination via the Understanding Cybersecurity Series (UCS) knowledge mobilization Program, eIT Europe (July 18, 2025)
- The Future of Cybersecurity: Leveraging Tools and Data for Enhanced Threat Detection, McMaster University, Canada (Oct 31, 2024)
- Elevating Cybersecurity Vigilance: UCS for Fintech and Digital Finance, University of Windsor, Canada (Sep 27)
- AI's Impact On Cyber Security (What You Need To Know), Markham Board of Trade, ON, Canada (Sep 26, 2024)
- Elevating Cybersecurity Vigilance: Understanding Cybersecurity Series (UCS), eIT, Europe (July 5th, 2024)



https://www.yorku.ca/research/bccc/Workshops

Workshops

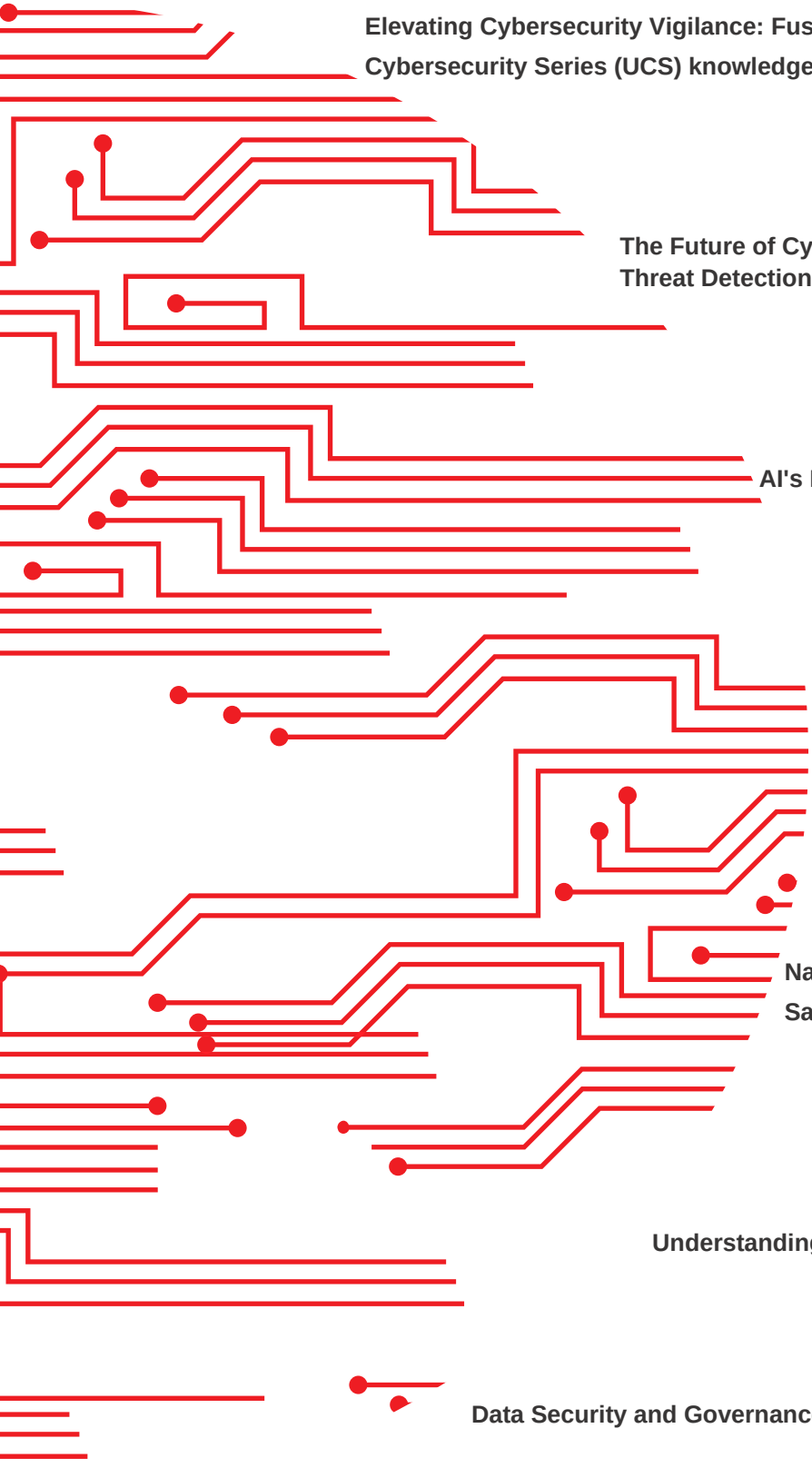
Understanding Cybersecurity Series Workshops (UCSW)

- Elevating Cybersecurity Vigilance: Understanding Cybersecurity Series (UCS), AVIVA, Muskoka, ON, Canada (May 1st, 2024)
- Elevating Cybersecurity Vigilance: Understanding Cybersecurity Series (UCS), MacEwan University, Alberta (February 9th)
- Elevating Cybersecurity Vigilance: Understanding Cybersecurity Series (UCS), NICT, Tokyo, Japan (December 1st, 2023)
- Navigating Cybersecurity: Empowering Public Safety and Awareness through UCS, York Circle, ON (October 14th, 2023)
- Understanding Cybersecurity Series (UCS), A&T University, NC, USA, (April 20th, 2023)
- Data Security and Governance, University of Toronto, ON (Jan 17th, 2023)

https://www.yorku.ca/research/bccc/Workshops

Understanding Cybersecurity Series (UCS)

Workshop Series



Elevating Cybersecurity Vigilance: Fusing Knowledge Dissemination via the Understanding Cybersecurity Series (UCS) knowledge mobilization Program

The Future of Cybersecurity: Leveraging Tools and Data for Enhanced Threat Detection

AI's Impact On Cyber Security (What You Need To Know)

Elevating Cybersecurity Vigilance: Understanding Cybersecurity Series (UCS)

Navigating Cybersecurity: Empowering Public Safety and Awareness through UCS

Understanding Cybersecurity Series (UCS)

Data Security and Governance

BCCC Behaviour-Centric Cybersecurity Center

BCCC
Behaviour-Centric
Cybersecurity Center

Understanding Cybersecurity Series (UCS)
Contest Series

Celebrate Creativity in Cybersecurity: The Cybersecurity Cartoon Award (CSCA) Contest

https://www.yorku.ca/research/bccc/CSCA

CSCA 2025

Cybersecurity Cartoon Award (CSCA)

- This year, we received an impressive 263 artworks from 128 talented cartoonists representing 25 countries. After careful consideration, the jury has selected 15 outstanding works for the final round. Here are the top selected pieces:

- The winners of 2025:



- The Honorary Mentions of CSCA 2025:






https://www.yorku.ca/research/bccc/CSCA/

BCCC Behaviour-Centric Cybersecurity Center

CSCA 2024

Cybersecurity Cartoon Award (CSCA)

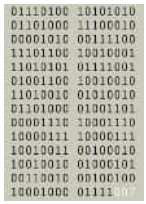
- This year, we received an impressive 258 artworks from 120 talented cartoonists representing 27 countries. After careful consideration, the jury has selected 53 outstanding works for the final round. Here are the top selected pieces:

- The winners of 2024:

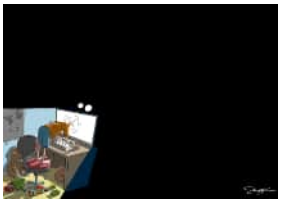


- The Honorary Mentions of CSCA 2024:







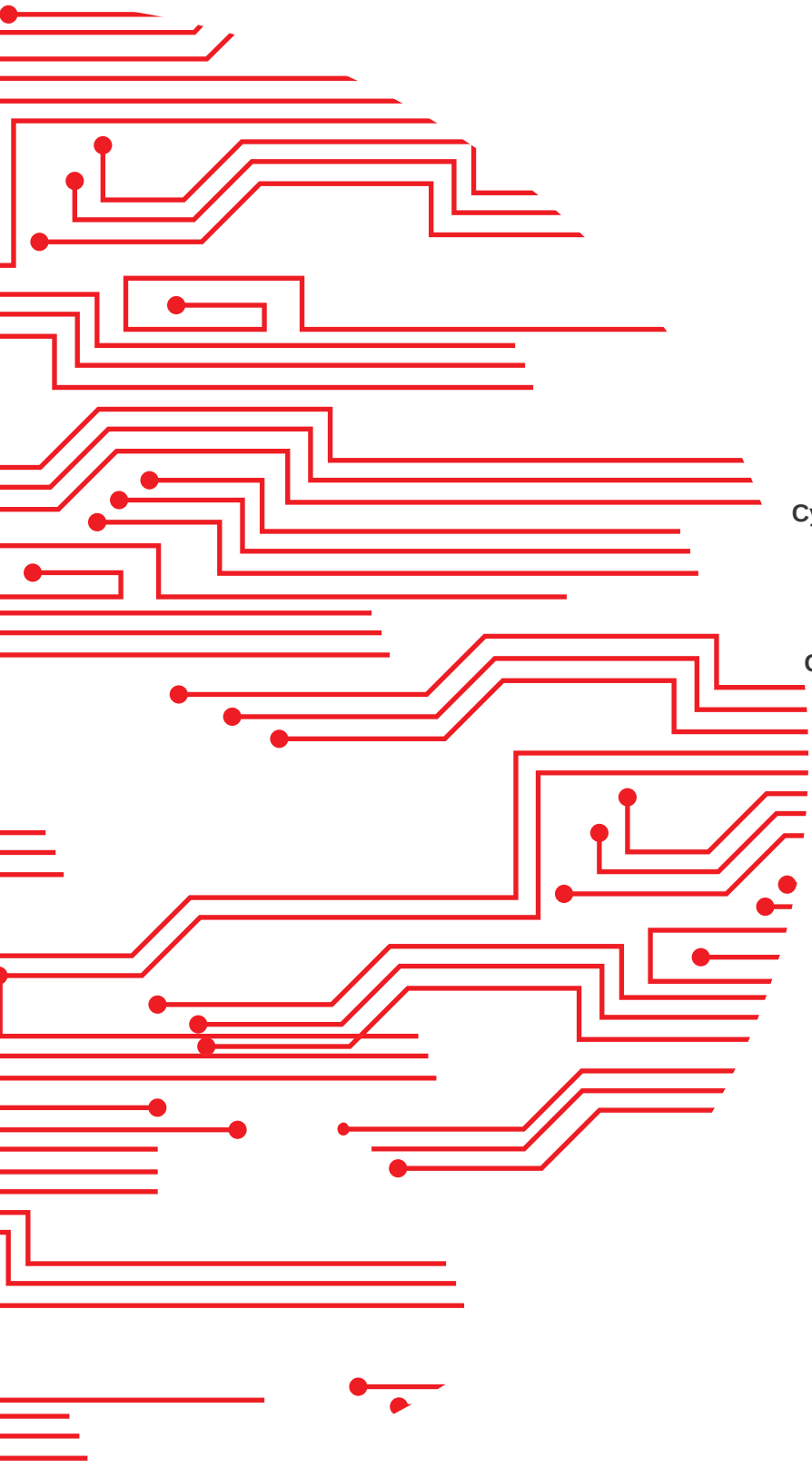



https://www.yorku.ca/research/bccc/CSCA/

BCCC Behaviour-Centric Cybersecurity Center

Understanding Cybersecurity Series (UCS)

Cantest Series



CyberSecurity Cartoon Award (CSCA 2024)

CyberSecurity Cartoon Award (CSCA 2025)

BCCC
Behaviour-Centric
Cybersecurity Center

BCCC
Behaviour-Centric
Cybersecurity Center

Understanding Cybersecurity Series (UCS)
Contributors

Our
Top Talented and Well-Trained
Cybersecurity Team Members:
Driving UCS Forward Together

https://www.yorku.ca/research/bccc/Team/

TEAM MEMBERS

Arash Habibi Lashkari
Canada Research Chair (CRC)
Founder and Director
York University, Canada

Sepideh Hajihosseinkhani
PhD Student
York University, Canada

Sepideh Niktabe
MCS (Graduated)
York University, Canada

Moein Shafi
MCS (Graduated)
York University, Canada

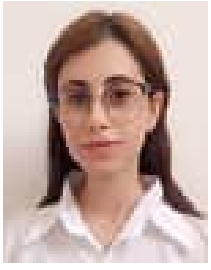
Adit Sharma
MAIST (Graduated)
York University, Canada

Yasin Dehfuli
MCS (Graduated)
York University, Canada

Niosha Hejazi
MAIST (Graduated)
York University, Canada

Arefeh Kouhi
MCS (Graduated)
York University, Canada

Reza Abbaszadeh
MCS (Graduated)
York University, Canada



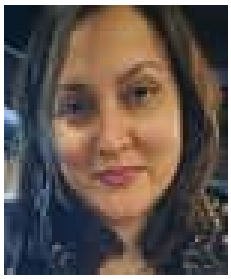
Mahdiyeh Khalaji
MASc (Student)
York University, Canada

https://www.yorku.ca/research/bccc/Team/

TEAM MEMBER

Amirhossein Ahmandnejad Roudsari
MCS (student)
York University, Canada

Ava Ameri
MAIST (student)
York University, Canada



Mona Parizadeh
Postdoctoral Fellow
UCalgary, Canada

Dilli Sharma,
PostDoctoral Fellow
York University, Canada

Barjinder Kaur
Postdoctoral Fellow
UNB, Canada

Samaneh Mahdavifar
Postdoctoral Fellow
McGil University, Canada

Marella Bolton
Research Assistant
York University, Canada

Melissa Lucking
Research Assistant
York University, Canada

Maelle Gautrin
Master Student (Visiting Researcher)
ENS Paris-Saclay, France

Shaila Sharmin
PhD Student (Mitacs GRA)
IIUM, Malaysia

Sepehr Jafari
Research Assistant
York University, Canada

Maryam Issakhani
Research Assistant
York University, Canada

https://www.yorku.ca/research/bccc/Team/

TEAM MEMBER

Borna Ahmadzade
Research Assistant
York University, Canada

Joshua Duarte
Research Assistant
York University, Canada

Pedram Sharifani
Research Assistant
York University, Canada

Xie He
Research Assistant
York University, Canada

Hadis Farrokhi
Research Assistant

Osman Berk Er
Research Assistant
York University, Canada

Isabella Lopez
Research Assistant
York University, Canada

Mehrsa Khoshpasand
Research Assistant
York University, Canada

Hardhik Mohanty
Mitacs GRI
York University, Canada

Abhay Pratap Singh
Mitacs GRI
York University, Canada

Aditya Raj
Mitacs GRI
York University, Canada

Alaa Souabni,
Mitacs GRI
York University, Canada

https://www.yorku.ca/research/bccc/Team/

TEAM MEMBER

Mohamed Aziz El Fadhel
Mitacs GRI
York University, Canada

Bhaskar Joshi
Mitacs GRI
York University, Canada

Mateus Herbele
Mitacs GRI
York University, Canada

Nikhill Vombatkere
Mitacs GRI
York University Canada

Nathan Chow (IT team)
York University, Canada

Oksana Mizgier (IT team)
York University, Canada

Ammar Homidan (IT team)
Learning Resource Coordinator
York University, Canada

Rosananthi Selvarajah
York University, Canada

https://www.yorku.ca/research/bccc/Team/