2021 PROGRAM

2021 Schedule | Saturday September 25, 2021

8:45AM – 9:00AM | Opening words

9:00AM – 9 :30AM | Benoit Dupont
Should Cybersecurity Research Pay More Attention To Criminology (And Vice-Versa)?

9:30AM – 10:00AM | Evan Grant
Bypassing Authentication On 20+ Arcadyan Routers And Rooting Some Buffalo :
A Walkthrough Of My First Router Hacking Experience

10:00AM – 10:30AM | Yuan Stevens & Stephanie Tran
See Something, Say Something? How Canada Does Coordinated Vulnerability Disclosure

10:30AM – 10:45AM | Break

10:45AM – 11:15AM | Olivier Michaud
Automatic Extraction Of Content From Criminal Underground Forums

11:15AM – 11 :45AM | Gabrielle Botbol
Solving Web Security Vulnerabilities With Pentesting

11:45AM – 12:15PM | Bruno Philippe
From fiction to reality, a retrospective of our experiences as an incident response team

12:15PM – 1:15PM | Lunch served in the conference room

1:15PM – 1:45PM | François Labrèche
Semantically-Aware Threat Intelligence From Infosec Underground Discussions And OSINT: A Machine-Learning Approach

1:45PM – 2:15PM | Andréanne Bergeron
Shining Light On The Dark Figure Of Cybercrime: Monitoring Online Offenders Through An Open Source Intelligence Platform

2:15PM – 2:45PM | David Shipley
Do anti-phishing programs even work?

2:45PM – 3:00PM | Break

3:00PM – 3:30PM | Michael Joyce
Not Just Awareness: Educating For Cybersecurity Motivation

3:30PM – 4:00PM | Philippe Arteau
Introduction To Request Smuggling

4:00PM – 4:30PM | Marc-Étienne Léveillé
Poking Around At Scale: One Year Of Scanning The Internet

4:30PM – 7:00PM | Cocktail

2021 Schedule | Detailed Program

9:00AM – 9 :30AM | Benoit Dupont

Should Cybersecurity Research Pay More Attention To Criminology (And Vice-Versa)?

‘Cybercrime’ is an umbrella concept used by criminologists to refer to traditional crimes that are enhanced via the use of networked technologies (i.e., cyber-enabled crimes) and newer forms of crime that would not exist without networked technologies (i.e., cyber-dependent crimes). Cybersecurity is similarly a very broad concept and diverse field of practice. For computer scientists, the term ‘cybersecurity’ typically refers to policies, processes and practices undertaken to protect data, networks and systems from unauthorised access. Cybersecurity is used in subnational, national and transnational contexts to capture an increasingly diverse array of threats. Increasingly, cybercrimes are presented as threats to cybersecurity, which explains why national security institutions are gradually becoming involved in cybercrime control and prevention activities. This presentation argues that the fields of cyber-criminology and cybersecurity, which are segregated at the moment, are in much need of greater engagement and crossfertilisation. I draw on concepts of ‘high’ and ‘low’ policing (Brodeur, 2010) to suggest it would be useful to consider ‘crime’ and ‘security’ on the same continuum. This continuum has cybercrime at one end and cybersecurity at the other, with crime being more the domain of ‘low’ policing while security, as conceptualised in the context of specific cybersecurity projects, falls under the responsibility of ‘high’ policing institutions. This unifying approach helps me to explore the fuzzy relationship between cyber-crime and cyber-security and to call for more fruitful alliances between cybercrime and cybersecurity researchers. The presentation therefore proceeds as follows. First, I consider in more depth the origins of the cyber-criminology and cybersecurity fields. This allows us to not only further explain the divergence between these cyber fields but also provide insights into how these differences can be better navigated. Second, I focus the rest of the presentation on the relational dynamics connecting the cybercrime and cybersecurity fields, including cyber harms and the actors responsible for preventing and controlling such harms. Using the concepts of 'high' and 'low' policing developed by Brodeur, I draw a continuum between crime and security and observe that the middle of this continuum sees a convergence, where crime and security meet. An increasing amount of cybersecurity problems are occupying this territory, which has significant implications for the cyber field as a whole. I conclude the paper by reflecting on these points of convergence and suggest areas for future research in this field.

Bio

Benoît Dupont is the holder of the Canada Research Chair in Cybersecurity and the Research Chair for the Prevention of Cybercrime (www.prevention-cybercrime.ca). He is a Professor of Criminology at the Université de Montréal and the Scientific Director of the Smart Cybersecurity Network (SERENE-RISC), which he founded in 2014. Benoît Dupont He also sits as an observer representing the research community on the Board of Directors of the Canadian Canadian Cyber Threat Exchange (CCTX). He is a member of CATAAlliance's Cybercrime Advisory Council. His current research interests focus on the governance of security and the use of networked initiatives to enhance offline and online safety, the coevolution of crime and technology, and in particular the social organization of malicious hackers, as well as the international comparison and evaluation of effective and efficient cybersecurity policies. He has published extensively in these fields. In 2021, he has worked with criminology students to develop and launch an online cyberfraud clinic to provide cybercrime victims with the support and information they need.

9:30AM – 10:00AM | Evan Grant

Bypassing Authentication On 20+ Arcadyan Routers And Rooting Some Buffalo : A Walkthrough Of My First Router Hacking Experience

In this talk, I will walk through how I rooted my first router, and how during disclosure of those vulnerabilities, I found that one of the issues was much more widespread than I expected and affected 20+ devices across 20 vendors and Internet Service Providers (ISPs) in 11 countries. Inspired by the work of colleagues, I was interested in researching a router, and decided to purchase what was, at the time, one of the best selling models on Amazon Japan. In the talk I will walk through getting a root shell on the Buffalo WSR-2533 models of routers via their UART interface and using that shell to take a closer look at the http server running the web GUI. I will walk through using Ghidra to analyze the httpd binary, finding a path traversal which could lead to authentication bypass which ultimately became CVE-2021-20090 and affected many more devices. We will look at the strange XSRF tokens the web interface uses to validate requests and how they are like something out of a Capture the Flag challenge. We will also look at the final vulnerability discovered in the Buffalo routers (CVE-2021-20091): a configuration file injection vulnerability which leads to a root telnet shell on the device. Additionally, I will talk about the process of discovering many more affected devices and the disclosure that followed, how the additional devices were found using tools like Shodan and BinaryEdge, and how we leveraged the help of the CERT Coordination Centre during disclosure. Finally, I will speak shortly about how a bug like CVE-2021-20090 should not have been able to exist for over a decade in as many devices from as many large companies as it has been able to, and why vendors selling consumer routers, and especially ISPs need to do a better job of testing the security of devices they provide to customers.

Bio

Evan is based out of Halifax, Nova Scotia and works with the Zero-Day Research Team at Tenable. He worked with the Canadian Forces Reserves for 8 years as a Signal Operator while attending Dalhousie University in electrical engineering. He got his start in infosec working with the Canadian Forces Reserves as a member of the CF Blue Team conducting vulnerability assessments. At Tenable, Evan worked on and managed the Vulnerability Detection team in

North America, writing plugins for Nessus and other Tenable products, before moving on to the Zero-Day Research Team. His research interests include anything touching “the cloud”, Microsoft Teams and the Microsoft Power Platform, and more recently IoT devices and consumer routers and modems. Outside of work, Evan enjoys bouldering and if he has time while in Montreal, he will likely be at Allez Up or Bloc Shop, realizing he has gotten a lot weaker during the pandemic.

10:00AM – 10:30AM | Yuan Stevens & Stephanie Tran

See Something, Say Something? How Canada Does Coordinated Vulnerability Disclosure

Canada is falling behind its peers and allies when it comes to facilitating vulnerability disclosure for its systems. According to our research, two-thirds of G20 member countries provide distinct and clear disclosure processes for vulnerabilities involving government systems, with many providing clarity regarding the disclosure process and expectations for security researchers regarding communication and acceptable activity. Our work identifies the need for increased transparency and explicit regulation in Canada's current approach to vulnerability disclosure at the federal level. Unlike its global peers, Canada has yet to adopt a distinct and public coordinated vulnerability disclosure (CVD) process for its government systems. This has left security researchers with no straightforward or transparent path for responsibly disclosing a security vulnerability found in the computer systems used by Canada's federal government — resulting in possible non-disclosure, public disclosure before remediation, or otherwise enabling the use of security vulnerabilities by attackers in ways that could jeopardize the security of Canada's computer systems and the people that they serve. On top of this, there exists no legal or policy framework in Canada regarding security research and vulnerability disclosure done in good faith; that is, done with the intent and in such a way to repair the vulnerability while causing minimal harm. Absent this framework, discovering and disclosing vulnerabilities may result in a security researcher facing liability under federal laws, including criminal and copyright legislation, in turn setting a chilling effect on security research in Canada. This talk discusses the avenues available to security researchers for disclosing vulnerabilities, and the risks that they need to watch out for in terms of liability under current Canadian law. Along with best practices, we'll examine how other countries are leading the way when it comes to providing comprehensive policy and pragmatic solutions for external vulnerability disclosure, and how Canada can learn from these models. We also identify the Canadian policy frameworks that are needed to harness the efforts of security researchers who find and disclose security flaws in Canada's federal government software, web applications, and potentially hardware, vehicles, IoT devices, and critical infrastructures before adversaries do.

Bio

Stephanie Tran is a researcher and policy analyst examining public policy and human rights issues related to digital technologies. In addition to Cybersecure Policy Exchange, Stephanie has contributed research and policy analysis at Citizen Lab, Amnesty International Canada, the United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), Global Affairs Canada's Digital Inclusion Lab, and more. Her research contributions include "See Something, Say Something: Coordinating the Disclosure of Security Vulnerabilities in Canada" (Cybersecure Policy Exchange 2021), "Private Messages, Public Harms: Disinformation and Online Harms on Private Messaging Platforms in Canada" (Cybersecure Policy Exchange 2021), "Unmasked: COVID-KAYA and the Exposure of Healthcare Worker Data in the Philippines" (Citizen Lab 2020), and "Unmasked II: An Analysis of Indonesia and the Philippines' Government-launched COVID-19 Apps" (Citizen Lab 2020). She is a trained computer programmer, having earned a Diploma in Computer Programming from Seneca College. She also holds a dual degree Master of Public Policy (Digital, New Technology and Public Affairs Policy stream) from Sciences Po in Paris, and a Master of Global Affairs from the University of Toronto. She earned her BA degree from the University of Toronto specializing in Peace, Conflict and Justice.

Yuan ("You-anne") Stevens is a legal and policy expert focused on information security and data protection rights. She works towards a world where powerful actors—and the systems they build—are held accountable to the public, especially when it comes to vulnerable or marginalized people. She brings years of international experience to her role at the Ryerson Leadership Lab as Policy Lead on Technology, Cybersecurity and Democracy, having examined the impacts of technology on vulnerable populations in Canada, the US, and Germany. Committed to publicly accessible legal and technical knowledge, Yuan has written for popular media outlets such as The Toronto Star and Ottawa Citizen and has been quoted in news stories for publications across Canada, such as the Global News, CTV News, and the CBC. Yuan is a research affiliate at Data & Society Research Institute and the Centre for Media, Technology & Democracy at McGill University. She previously worked at Harvard University's Berkman Klein Center for Internet & Society during her studies in law at McGill University. She has been conducting research on artificial intelligence since 2017 and is currently expanding her knowledge of Canadian hacking laws and blockchain technology as an LL.M candidate at University of Ottawa's Faculty of Law working under Florian Martin-Bariteau. When she's not examining the role of technology in creating dystopian futures in Canada and abroad, you can find her gardening on her balcony, taking apart hardware around her house, or keeping up with (elderly) family members in Newfoundland.

10:45AM – 11:15AM | Olivier Michaud

Automatic Extraction Of Content From Criminal Underground Forums

With the advent of new communication channels that take advantage of anonymity technologies and cryptocurrencies, the criminal underground has grown significantly over the past 10 to 20 years. Malicious actors within this underground use illicit markets and discussion forums to communicate on and transact increasingly advanced techniques and tools to extort, steal identities and data. Many faclitating platforms are hosted on the Tor network, a communication channel that is part of the dark web. The anonymity that the Tor network provides has made it increasingly difficult for law enforcement agencies and insttutions impacted by these attacks to protect themselves. According to a survey carried out by the CyberEdge Group, 86% of companies with more than 500 employees were victims of a successful cyberattack in 2020. In addition, 60% of non-drug related advertisements for illicit goods and services posted on the dark web were deemed likely to impact a business (Guccione , 2021). Monitoring the criminal underground helps potential victims detect past and future attacks, and put up more effective responses to them. In other words, it helps victims develop a proactive strategy to better face today's threats. In order to automate the process of monitoring the criminal underground, technologies from the field of web Crawling and web scraping have been proposed. Web crawling refers to the process of browsing the web automatically using a robot to index its content. Web scraping, on the other hand, is the set of techniques used to extract content from an HTML page. These technologies usually rely on manual configurations, which further increases operating costs. In this conference, we propose a method to automate data collection of forums in the criminal underground. More specifically, the focus of this presentation is on pages containing forum topics, from which the title, author and publication date of each entry will be extracted. The proposed method makes it possible to transform an HTML page in order to carry out "sequence labeling", a technique in the field of natural language processing. This not only works on forums used during training, but can also be generalized to other unknown forums.

Bio

Olivier is currently a master's student in software engineering with a concentration in artificial intelligence at the École de technologie supérieure (ETS). His achievements allowed him to start this master's degree in his last year of a bachelor's degree in software engineering at the same school. Proud representative of Quebec at the Canadian Competition of Engineering in 2020, Olivier distinguished himself by winning the excellence scholarship from the École de technologie supérieure in order to continue his studies at the graduate level. His interest for artificial intelligence has led him to work with Flare Systems, now a partner in his research. During his undergraduate studies, Olivier was particularly involved with the Lan ETS Club in addition to being tasks with running laboratory classes. You can read about Olivier on Medium (https://medium.com/@oliviermichaud_62658), listen to him on Youtube ((https://www.youtube.com/watch?v=hTGyyMGXe9Y&list=PLYqsEfpltcFd-flEAmp196gFvwjZwm7ys&index=4) and follow him on on Linkedin (https://www.linkedin.com/in/olivier-michaud-ab9393152/).

11:15AM – 11 :45AM | Gabrielle Botbol

Solving Web Security Vulnerabilities With Pentesting

Breaking into cybersecurity can be quite overwhelming. In this session, I will present how I created an open learning program to become a pentester. This program, based on a science education concept called “Apprenance”, allowed me to be hired as a pentester. Cybersecurity is not only about technical skills, it is also about soft skills. During the talk the following questions will be addressed: What is a hacker? What is pentesting? What are the different types of pentest? What are the must have skills to be a pentester (including soft skills)? How do you pentest a target from A to Z? After establishing a basic foundation, a deeper dive into web pentesting with SQL injection, Cross Site Scripting, Directory Traversal and how to exploit them, including a video demo will occur. Participants will learn about the reality of the life of a pentester through anonymized examples from my personal experiences seen in real contexts. They will leave my session with concrete resources and tips useful for practice. An additional takeaway will be about how to break into cybersecurity and how to train to sharpen pentesting skills.

Bio

Gabrielle Botbol is a pentester, cyber security blogger, and podcaster (CS by GB - Cybersecurity By Gabrielle B https://gabrielleb.fr/blog/). She created a self study program to become a pentester. Gabrielle Botbol focuses her efforts on democratizing information security for all. She is Vice President Communications at NorthSec Conference. She was honoured for her career and contribution to the cyber community by being named one of the top 20 women in cyber security in Canada in 2020. She recently joined the offensive security Team of Desjardins.

11:45AM – 12:15PM | Bruno Philippe

From fiction to reality, a retrospective of our experiences as an incident response team

The past year has seen a number of significant ransomware attacks across all business sectors. Based on our experience as members of an incident response team, we will draw from several cases we worked on to identify the trends we have observed in the methods attackers use to infiltrate companies and exfiltrate data, as well as the consequences these infiltrations have had. We will more specifically answer the following questions: what attack vectors are used by attackers? How do attackers move inside of a network, and for how long? How do attackers exfiltrate data? What are the impacts of these attacks on production activities in the short-term? How can we build a more secure infrastructure? We will also discuss the particularities of incident response team tasks, the skills required, as well as the relationships we have needed to establish with other security teams such as SOC analysts and pentesters. This will lead into our mission which is structured around four pillars: to prepare, to detect and analyze, to contain / eradicate / recover and manage post-incident.

Bio

After more than 20 years in the administration of Unix and Linux systems and the design of technical architectures (including the implementation of several consolidation projects in virtualized environments), Bruno reoriented himself in IT security. His various professional experiences spawn many sectors (banking, manufacturing and services) abd give him a broader vision that allows him to better understand the problems of each client. After several mandates in the design of monitoring rules and the implementation of SIEM-type monitoring tools, Bruno is currently working in an incident response and digital analysis team where he is confronted on a daily basis with different types of computer attacks. including ransomware attacks. Passionate about malware analysis, Bruno also contributes to improving the security posture of customers by working, in particular, with team members to define response plans to security incidents.

1:15PM – 1:45PM | François Labrèche

Semantically-Aware Threat Intelligence From Infosec Underground Discussions And OSINT: A Machine-Learning Approach

In cybersecurity, news regarding new vulnerabilities appear continuously every day through an array of various sources, be it news networks, social networks, blogs, security advisories, etc. These fall under the umbrella of open-source intelligence (OSINT). Yet not all vulnerabilities generate the same level of interest and length of discussion. As such, one interesting aspect of vulnerability prioritization is to consider what types of vulnerabilities are currently trending in these OSINT sources and in the dark web, in order to establish the types of vulnerabilities an attacker might favor. For example, if discussions in public sources and underground networks currently mention reflected XSS attacks on particular frameworks more often than usual, then other attackers reading these discussions could be tempted to attack other similar XSS vulnerabilities, or find similar inflection points in other frameworks. Attackers, just like cybersecurity experts, are very much influenced by trends in exploitation methods. In this talk, we will present an approach which identifies the patterns or trends underlying online discussions. These are what we aim to model in order to generalize which vulnerabilities might receive more attention from attackers, regardless of the vulnerability's direct mentions (e.g., its CVE number) in online discussions. The goal is the identification of the underlying concepts associated with online cybersecurity discussions, to assess the importance of existing vulnerabilities. To extract this information, a natural language approach is employed, which uses machine learning, and more specifically, topic modeling. We will start by explaining how topic modeling, specifically LDA, works, and why it is an interesting method to extract information from OSINT sources and underground forums. Then, we will go into how vulnerability data can be categorized automatically using topics, and how they can be matched with online discussions to identify potential targets of malicious actors, by building a model that finds vulnerabilities similar in concepts to currently trending vulnerabilities in online discussions. We will present trends identified by our approach at different points in time, and how important events in the infosec world impact them. More specifically, we will show how trends change following the publication of highly critical vulnerabilities, and how these trends evolve over time and stay relevant to current events.

Bio

François Labrèche is a Data Scientist at Secureworks, who focuses on applying machine learning approaches to research problems related to security vulnerabilities and threat hunting. He focuses on using machine learning, more specifically natural language processing, to improve the prioritization of vulnerabilities, in the context of vulnerability management and remediation. He explores the use of OSINT sources and the dark web in assessing the importance of newly published vulnerabilities. He has a PhD from École Polytechnique de Montréal, and has published research papers on the topics of spam detection, malware analysis and machine learning applied to cybersecurity. He has presented at University College London and École Polytechnique de Montréal, and has published papers in conferences such as the ACM Conference on Computer and Communications Security (CCS). Additionally, he is also part of the NorthSec administration, as VP Finance, and part of the organization of MontréHack, a monthly computer security workshop in Montreal.

1:45PM – 2:15PM | Andréanne Bergeron

Shining Light On The Dark Figure Of Cybercrime: Monitoring Online Offenders Through An Open Source Intelligence Platform

Many cybercrimes go unreported to the police (e.g. Tcherni et al., 2016), thus enhancing the dark figure of crime (Biderman and Reiss, 1967). To shine a light on a part of the dark figure of crime, we developed a tool to gather information on online offenders around the world. DrugRoutes.com is an open-source intelligence platform on illicit drug transactions on the darkweb. The platform is unique for two main reasons. First, it uses self-reports by illicit drug buyers and dealers to measure the success rate of transnational illicit drug transactions. Second, all of its self-reports are made public and can be analyzed by anyone simply by visiting the website. The objective of this presentation is to discuss the usefulness of being creative when it comes to gathering information on cybercrime. More specifically, our goal is to walk through the steps we went through to design, implement, launch and run this platform over the years. We will share our experiences running the platform, with all the challenges that are associated with collecting crowdsourced datasets. The willingness of the Darkweb users to participate in this kind of study will be discussed as it is possible to estimate the level of uncooperative participants through the amount of spam received through the self-reports. Moreover, the presentation will briefly expose some results obtain through the data collected with DrugRoutes. The tool enabled us to monitor darkweb market disruption during the COVID-19 pandemic. Our findings suggest that the postal service, the primary delivery option for online illicit drug shipping, was impacted by the pandemic. Our results also suggest that the level of unsuccessful transaction is higher among vendors residing in countries that are most affected by the pandemic. Self-reported transactions and other user-generated content provides us with almost real-time information on online offenders of all kinds. Through this presentation, we will describe the benefits and limits of using such data to better understand cybercrime, and provide a framework for others to replicate our methodology across other types of cybercrimes.

Bio

Andréanne Bergeron is a Ph.D. candidate at the School of Criminology of the Université de Montréal and holder of the prestigious Vanier scholarship. Her thesis focuses on the dynamic interactions during police interrogation of online sex offenders. She explores and explains the cooperation and power relationships between police officers and suspects. Andréanne also specialized in other types of cybercrime as she works as the coordinator for the Trans-National Organized Crime research project of the Darkweb and Anonymity Research Center. She is involved in her community as the leader of the Student Academic Seminar of the Criminology school. Andréanne helped organize regional and international conferences as the president of the annual Workshop on Research on Police Investigations (CREP) and as a member of the organizing comity for The Society and Criminal Psychology annual conference and for the Open-Source Analysis and Development Research Group (GARDESO). She currently teaches cybercrime at the Université de Montréal.

2:15PM – 2:45PM | David Shipley

Do anti-phishing programs even work?

Do anti-phishing programs even work? This talk explores the millions of phishing emails sent to hundreds of organizations and how these efforts shape human behaviour. During this talk, David Shipley will show the aggregate results of millions of phishing simulations. He'll demonstrate how these simulations, integrated into security awareness efforts, have shown demonstrable behaviour change and reduced risk for organizations. Shipley will provide insights into:

- How to measure success: the phishing metric trinity: The Click, Report, and Ignore Rate;
- Why monthly automated random campaigns generate the most accurate results;
- Why anti-phishing programs are not about zero click rates;
- Lessons that can be learned from the pandemic regarding risk reduction.

Bio

As CEO and co-founder of Beauceron Security, David Shipley is energized by helping people feel in control of technology. David's career has seen him transition from a Canadian Armed Forces officer, to a journalist to a marketing specialist. He ultimately found himself in cybersecurity after he led the incident response team when the university he worked for was hacked in 2012. David often speaks on the international stage about cybersecurity awareness, and one of his favorite topics is the importance of returning to the origin of the word "cyber". His passion drives him to make people not only aware of cybersecurity risks, but to make them care enough about their role in cybersecurity to change their behavior.

3:00PM – 3:30PM | Michael Joyce

Not Just Awareness: Educating for Cybersecurity Motivation

The importance of the human factor and related public awareness for cybersecurity are increasingly being recognised by industry. Within the last decade in particular, the focus within enterprises on cybersecurity education training and awareness (SETA) programs has greatly intensified. However, despite the increase in effort, successful attacks leveraging the human factor appear to be somehow increasing. Given the state of the current status quo, it is clear that innovation is required if SETA is to achieve its goal of effectively equipping the human for their role in cybersecurity. We present the implementation of a novel methodology for designing a security education training and awareness program that leverages motivation and psychology theory. This approach draws from Protection Motivation Theory and Social Learning Theory to establish a set of guidelines for the development of SETA programs. It reflects a pedagogical focus on motivating behaviour over providing awareness and presents a potential improvement on traditional approaches. This design method was implemented in the development of a Massively Open Online Course targeting the post-secondary education sector. This sector represents a potential pressure point for cybersecurity globally, as it is simultaneously targeted by advanced persistent threat actors, is difficult to defend due to the large user bases and relative lack of cybersecurity resources. Consequently, this sector is in great need of effective SETA tools. This program was developed in collaboration with the University of Montreal, The Canadian Centre for Cyber Security, RISIUQ, the Bureau intervention en matière de harcèlement (BIMH), the Canadian Anti-Fraud Centre, and the Montreal hacker community. It provides a basic level of cybersecurity education within three hours, equipping students, staff and researchers to engage with cybersecurity in an academic context. This presentation will not only outline the methodology and provide an overview of its implementation into a real-word product but also share the experience of realising an innovative approach in a cross-sectoral collaborative project. We will also discuss the importance of providing quality free alternatives to commercial cybersecurity products.

Bio

Michael Joyce is the co-executive director for Canada's SERENE-RISC (Smart Cybersecurity Network – Réseau Intégré sur la Cybersécurité) initiative, a national network of researchers and practitioners, which has developed innovations including cybersec101.ca, The Cybersecurity Digest, secrev.org, and Konnect. He has nearly a decade of experience in the development and management of national and international cybercrime and cybersecurity knowledge mobilization programs. In his spare time he is completing a doctorate in criminology at the University of Montreal in the Cybercrime prevention laboratory (https://www.prevention-cybercrime.ca/). He is also the host of the cybercrimeology.com podcast.

3:30PM – 4:00PM | Philippe Arteau
Introduction to Request Smuggling

Load balancers and proxies, such as HAProxy, Varnish, Squid and Nginx, play a crucial role in website performance, and they all have different HTTP protocol parser implemented. HTTP Request Smuggling (HRS) is an attack abusing inconsistencies between the interpretation of requests' ending by HTTP request parsers. What might be considered the end of one request for your load balancer might not be considered as such by your web server. In this presentation, we will see how an attacker can abuse several vulnerable configurations. HTTP Request Smuggling (HRS) enable multiple attack vectors, including cache poisoning, credential hijacking, URL filtering bypass, open-redirect and persistent XSS. For each of these vectors, a payload will be showcased and explained in-depth. Also, a live demonstration will be made to see the vulnerability in-action. Aside from exploitation, we will show how developers and system administrators can detect such faulty configurations using automated tools. By the end of this talk, security enthusiasts from any level will have solid foundations to mitigate request smuggling, a vulnerability that has greatly evolved in the past 15 years.

Bio

Philippe is a security researcher working for GoSecure. His research is focused on Web application security. His past work experience includes pentesting, secure code review and software development. He is the author of the widely used Java static analysis tool OWASP Find Security Bugs (FSB). He is also a contributor to the static analysis tool for .NET called Security Code Scan. He built many plugins for Burp and ZAP proxy tools: Retire.js, Reissue Request Scripter, CSP Auditor and many others. Philippe has presented at several conferences including Black Hat Arsenal, SecTor, AppSec USA, ATLSecCon, NorthSec, and 44CON.

4:00PM – 4:30PM | Marc-Étienne Léveillé

Poking Around At Scale: One Year Of Scanning The Internet

When researching malware, we often find ways to remotely identify if a system is compromised, especially when looking at server-side threats. This requires to thoroughly reverse engineer the network protocol of malware to understand how to properly trigger a behaviour or response that could be used as a fingerprint. Scanning for compromised systems using a fingerprint on a local network is relatively easy but scanning the whole IPv4 internet brings its own set of challenges. Previously, we worked with third parties such as Shodan or Censys to perform scans for us. While these popular internet scanners were very kind to help us out in our research, we realized we couldn't always monopolize their resources. This presentation will start by showing how we built our own internet scanner from scratch and overcame the challenges of performing such scans. Then, we will present cases where our scans revealed needles in the haystack based on in-the-wild malware we analyzed. Lastly, we will provide tips for anyone who wants to perform scans at scale. Since our fingerprints may require performing some form of handshake, there are no ready-made solutions to our problems. We use custom in-house scanners based on the existing zmap and zgrab2 open-source software. Post-processing results is also a challenge given how massive is the amount of data it generates. Nonetheless, existing tools such as jq can help us find the interesting results we are looking for. Our scans found victims for malware families such as Kobalos, PortReuse, ModDir and several IIS backdoors. Those results helped us notify victims and gather important details about each of these threats. For one, we could identify who the victims are and if the attacks were opportunistic or really limited to a small set of targets. Secondly, when sending notifications, we can ask for additional details such as how it was compromised or how the compromised system was used by the perpetrators. Those details can enrich our research and provide better indicators of compromise to other potential victims. Another use for internet scans is uncovering infrastructure used as C&C servers for malware operations. It is common for malware operators to deploy multiple servers to be used as C&C in a similar fashion, perhaps because they are using scripts. We will show how we leveraged this to uncover additional servers used in malware campaigns. There are a number of weird devices connected to the internet, sometimes producing false positives. We will talk about these devices (and either laugh or be worried) and show some pitfalls to avoid when making fingerprints and parsing results.

Bio

Marc-Etienne is a malware researcher at ESET since 2012. He specializes in malware attacking unusual platforms, whether it's fruity hardware or software from south pole birds. Marc-Etienne focused his research on the reverse engineering of server-side malware to discover their inner working and operation strategy. His research led to the publication of the Operation Windigo white paper that won Virus Bulletin's Péter Ször Award for best research paper in 2014. Outside his day job, Marc-Etienne enjoys playing with his two kids and designing challenges for the NorthSec CTF competition. He was also a co-organiser of the MontréHack monthly event. He presented at multiple conferences including RSAC, FIRST, 44con, CARO and Linuxcon Europe. When he's not one of the organizer, he loves participating in CTF competitions like a partying gentleman. Outside the cyberspace, Marc-Etienne plays the clarinet and read comics. He tweets sporadically at @marc_etienne_.