serene risc Digest Volume 2, Issue 2

Cutting Edge Research Summaries for Policy-Makers and Practitioners

Can machine learning help defend cars against hacking?

The security and vulnerability of modern cars is a significant concern. Taylor, Leblanc and Japkowicz sought to develop a framework for detecting abnormal behaviour on vehicle networks. The research team collected 24 hours of internal car network communications from a common, 2012 model family car. They generated indicators of known attack types and inserted them into the remaining seven hours of data. A machine learning neural network was then tasked with detecting these abnormal patterns in the network data. They compared the performance of the neural network against other forms of detection including probability-based calculations and a simple guessing method. The researchers found that machine learning was vastly superior to the other methods, which performed no better than a coin flip. The design and implementation of future systems may be guided by this research in order to increase the safety of drivers and protect them from malicious attacks.

Do consumers of Child Exploitation Material change over time?

The Internet has provided new opportunities for all aspects of human activity, including illicit activities. The consumption of Child Sexual Exploitation Material (CSEM) is no exception. Analysing crime with scripts provides insight into criminal techniques. Fortin et al. surveyed over 500 academic publications and technical reports that contained key terms pertaining to child pornography and the luring of children (grooming). Making use of the script approach, the researchers grouped the behaviours into episodes and noted the context in which individuals transitioned from one episode to another. This study is not without limitations, but it does provide what appears to be a promising tool for the investigation of CSEM related behaviours.

How does cyberbullying affect Canadian indigenous adolescents?

Cyberbullying is a growing concern. Broll, Dunlop and Crooks examined surveys collected over a six-month period between September 2014 and March 2015 that evaluated a Canadian school-based substance use and violence prevention program. They measured the extent to which the 170 Indigenous adolescents in the study identified themselves as being perpetrators or victims of bullying in the preceding month. The study shows that Indigenous adolescents are often the victims of bullying both offline and online. Cyberbullying is a source of harm for one of society's most marginalized groups.

Should websites mine cryptocurrency on your computer while you use them ?

Recently there has been a trend in websites using their viewers' computers to mine cryptocurrency as an alternative source of revenue; often without their consent. Eskandari, Leoutsarakos, Mursch, and Clark surveyed the circumstances that gave rise to browser-based cryptocurrency mining, measured the prevalence and profitability of using Coinhive. They analysed the top million sites in public databases of websites and found in fall 2017, at least 30 000 websites with Coinhive's Javascript code in the body of their page. This practice presents ethical questions as depending on how the mining is implemented, as it may use a persons' resources without their knowledge, consent or without certainty that the person understands the exchange they have consented to. The researchers offer two forms of mitigation in terms of protecting users from non-consensual browser-based mining.

Is the police use of social media data big data analytics services ok?

The nature and scale of the police use of social media data has been evolving quickly. Scassa contends that new approaches to transparency are essential for the public to learn as much as possible on how police use social media data for surveillance purposes. The companies involved facilitate the analysis of publicly available data such as geolocation and posts on social media. A fundamental issue here is the protection of civil liberties, namely the right to privacy and the related rights of free speech, freedom of association, and the right to be free from discrimination. Scassa observes that law enforcement, policy makers and corporations that work in social media and data analytics are three entities that need to recalibrate the level of transparency that characterizes their practices.

Do Smart Cities raise new security concerns?

The increased prevalence of technology in city infrastructure brings new privacy and security concerns. Braun, Fung, Iqbal, and Shah argue that it is necessary to pre-emptively address the privacy and security concerns that Smart Cities raise in order to increase the efficiency, safety, and convenience of city management. Smart Cities create privacy threats due to their reliance on rapid data sharing between multiple service providers. The interconnectivity of smart cities and the inclusion of IoT devices results in many possible points of attack. Smart Cities also raise issues around the collection, management and deletion of data. Preserving the trust of inhabitants is important for the sustainable operation of a Smart City. A thorough analysis of the privacy and security challenges posed by Smart Cities will be crucial in their success.

Is the social media fraud market mostly driven by sales and advertising for products and services?

Generating likes, follows and views on social media services with fake-user accounts constitutes social media fraud. Paquet-Clouston et al. studied the supply and demand of social media fraud services. They positioned themselves inside an Instagram-focused botnet to observe its social media fraud operations. They observed that such services are easy to find and at various prices, making them available to a wide range of customers. Analyzing traffic collected from the Linux/Moose botnet, they suggested that the customer base for such services is varied. It includes individuals, companies and entrepreneurs. The authors suggest providing affordable and legitimate ways for social media users to increase their fan base. In addition, they recommend raising awareness of the illicit nature of social media fraud services among potential consumers.

Can you do anything to reduce the risk from the insider threat?

While a lot of attention is payed to the hacking of networks, threats from inside the organisation have also proven to be harmful.

Williams, Levi, Burnap and Gundur tested the applicability of the criminological routine activities theory to insider cybercrime. The team used data from the Cardiff University UK Business Cybercrime Victimization Survey to measure the impact of routine activities and guardianship practices on insider cybercrime. Almost 10 percent of the respondents reported having experienced insider cybercrime. The organisation size was the greatest predictor of insider cybercrime victimization. Guardianship measures and routine activities each explained up to 13% of the difference in the possibility of an organisation becoming a victim of insider cybercrime. Interestingly, the use of employee's own devices (BYOD) and correlation between victimization likelihood and the use of new technologies such as Wi-Fi, social media or cloud services were not a good predictor of insider crime. While insider cybercrime is still a new research area this study shows that theories from more developed fields such as criminology may provide a theoretical framework to provide insight into this phenomenon.

If you can't run malware, you can't run a 'Rowhammer' attack, right ?

System attacks at the physical level can bypass security software and operating system controls. It has been widely assumed that such an attack required executing a malicious program directly on the targeted computer. This is not necessarily the case. Modern memory packs data storing capacitors very closely together and uses smaller electrical charges because of the demands of greater speed and miniaturization. 'Rowhammer' attacks take advantage of this by aggressively charging and discharging capacitors in the hope their neighbours will induct electricity and change value; form a ,"0" to a "1". Tatar, Krishnan Konoth, Athanasopulos, Giuffrida, Bos and Razavi demonstrated that it is possible to deliver a Rowhammer attack via a network connection. They were able to store sensitive data in vulnerable memory locations; corrupting data and compromising the systems.

Can machine learning help criminal investigations by identifying the authors?

The anonymous nature of the Internet makes it difficult to conclusively identify people online. Stylometry is the study of linguistic style in order to differentiate between authors. This type of analysis has been presented in courts in the form of expert testimony to assist the identification of the authors of texts. Researchers Ding, Fung, Iqbal, and Cheung have developed models to automate the process of selecting subsets of linguistic features to be studied by leveraging machine learning techniques. The researchers tested their automated system against existing systems on databases of texts, novels, and twitter posts and found it to be effective and robust. Advancements in authorship analysis can assist cybercrime investigations as well as provide analysis techniques for market, social network and social sciences research.

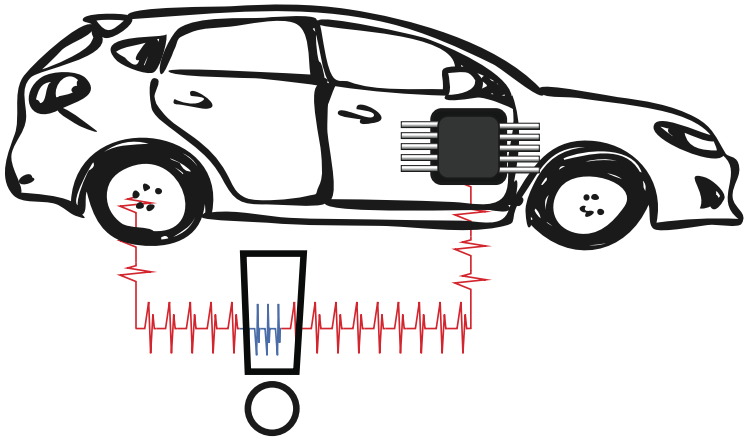
Probing the limits of anomaly detectors for automobiles with a cyber attack framework

The security and vulnerability of modern cars is a significant concern. Computer networks in automobiles can be exploited allowing attackers to control the brakes, steering and engine. Reducing the vulnerability of car computer systems will require a multifaceted approach. Malicious activity inevitably creates unusual behaviour in the internal communication system of cars. The detection of this unusual behaviour in car computer systems provides a last line of defence, and is important for ensuring security throughout the vehicle.

Taylor, Leblanc and Japkowicz sought to develop a framework for detecting abnormal behaviour on vehicle networks. They classified three steps for hacking a car: accessing the vehicle's electronics, connecting to the vehicle's network via those electronics and finally sending control messages on that network. This research focused on the last step. Particularly, to detect malicious messages that directly control physical systems. The researchers tested the capability of machine learning to detect attacks against cars. They assessed its effectiveness relative to other forms of detection.

The research team collected 24 hours of internal car network communications from a common, 2012 model family car. They used a type of machine learning that is adaptable enough to be used with car network data known as Recurrent Neural Networks (RNN). Other uses for RNNs include mapping language to predict the next word in a sentence. Seventeen hours of car data was used to train an RNN so it could recognize normal traffic and make predictions about the next messages on the network. A different message from this prediction could be considered abnormal.

They generated indicators of known attack types and inserted them into the remaining seven hours of data. The trained RNN was then tasked with detecting these abnormal patterns in the network data. They compared the performance of the RNN against other forms of detection including probability-based calculations and a simple guessing method.



The researchers found that RNNs were vastly superior to the other methods, which performed no better than a coin flip. Out of four models used, the RNN model working over longer periods of time had the overall best average performance. The authors found that the longer an effect occurs and the more unusual it is, the more detectable it becomes. The exact meaning of the data on a vehicle network is proprietary and as such remained a mystery to researchers outside of the manufacturer. However, the specific ID and field used by the detector appeared to be very important for its performance.

The design and implementation of future systems may be guided by this research in order to increase the safety of drivers and protect them from malicious attacks.

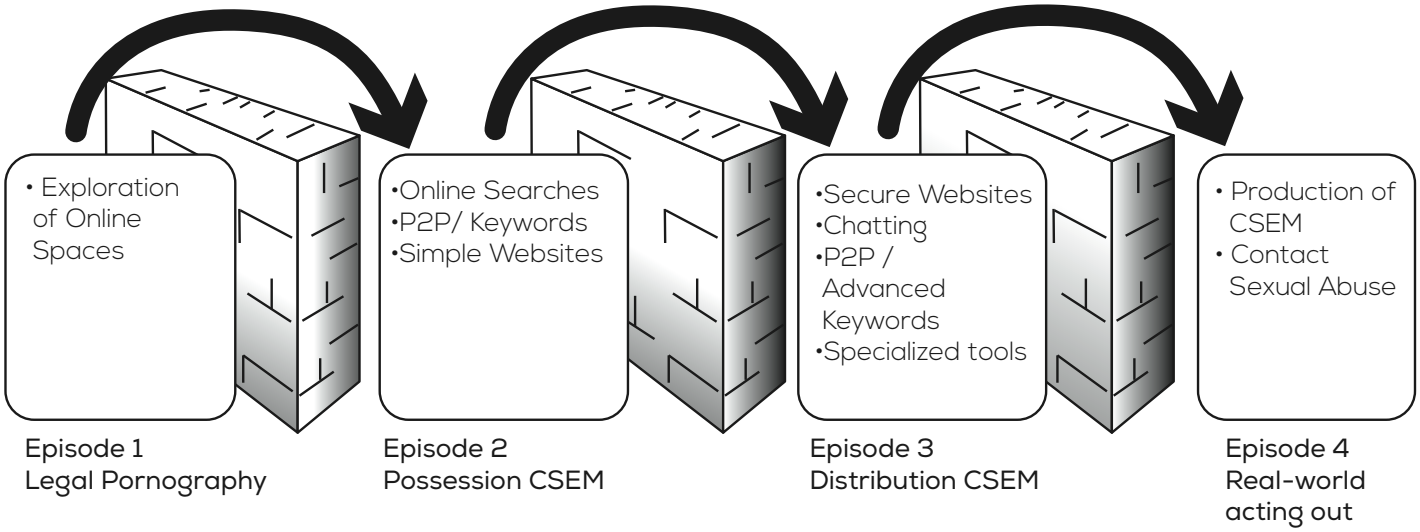
Machine learning appears to be an effective tool for detecting cyberattacks on vehicle communication networks.

Taylor, A., Leblanc, S., & Japkowicz, N. (2018). Probing the Limits of Anomaly Detectors for Automobiles with a Cyber Attack Framework. IEEE Intelligent Systems.

From online to offline sexual offending: Episodes and obstacles

The Internet has provided new opportunities for all aspects of human activity, including illicit activities. The consumption of Child Sexual Exploitation Material (CSEM) is no exception. Classifications of the consumers of CSEM have generally grouped them into static types. However, little is known about how they might evolve and change over time. Scripts can be used in research to document a reoccurring sequence of events or actions. Analysing crime with scripts provides insight into criminal techniques. It could also help understand of how criminals change as their expertise increases.

Fortin et al. surveyed over 500 academic publications and technical reports that contained key terms pertaining to child pornography and the luring of children (grooming). The behaviours and tools of online sexual offenders were reviewed and grouped into four broad categories of online sexual activities. Making use of the script approach, the researchers grouped the behaviours into episodes and noted the context in which individuals transitioned from one episode to another. Each of the transitions were marked by obstacles that must be overcome in order to progress to the next episode.



There are many types of consumers, each with different motivations, interests and consequently, processes. Scripting these provides an outline of general pathways and the transitions to more serious offences.

The first episode begins with the consumption of legal pornography. When some people find that it is also possible to access illegal content, their interest shifts.

The second episode sees the exploration of tools that facilitate the discovery of CSEM. When traditional tools no longer suffice for this purpose, the consumer explores virtual spaces and embarks on a process of socialization.

The third episode is distinguished by immersion, as the person interacts more regularly with others in order to access content that is rarer. These interactions help consumers learn how to acquire content and avoid apprehension by law enforcement agencies.

The fourth and final episode involves acting out, with the objects of collections becoming real world targets. Some aggressors use CSEM to facilitate their assaults, others share this content in a bid for peer approval and community status.

This study is not without limitations, but it does provide what appears to be a promising tool for the investigation of CSEM related behaviours.

The analysis of the patterns that precede the sexual assault of children offline could help when designing programs for the prevention of these crimes.

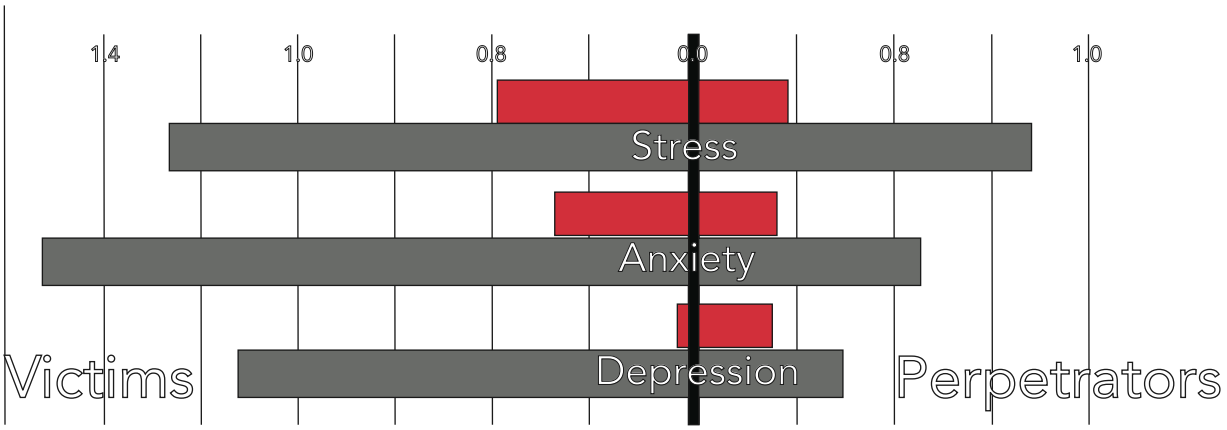
Fortin, F., Paquette, S., & Dupont, B. (2018). From online to offline sexual offending: Episodes and obstacles. Aggression and Violent Behavior.

Cyberbullying and Internalizing Difficulties among Indigenous Adolescents in Canada: Beyond the Effect of Traditional Bullying

Cyberbullying is a growing concern. The effects of bullying and cyberbullying on the health of adolescents have been well documented. However, there is little research about the experiences of Indigenous adolescents with bullying and cyberbullying. The majority of studies on bullying have instead focused on white and middle-class populations. The small number of studies including Indigenous participants suggests that they experience frequent bullying. This is troubling considering known issues that affect Indigenous people such as health inequities, the impacts of colonization and forced assimilation policies, and the need for culturally-relevant programming especially for Indigenous youth.

Broll, Dunlop and Crooks examined surveys collected over a six-month period between September 2014 and March 2015 that evaluated a Canadian school-based substance use and violence prevention program. They sought to identify the effect of both cyberbullying victimization and perpetration on the levels of depression, anxiety and stress among Indigenous adolescents.

They measured the extent to which the 170 Indigenous adolescents in the study identified themselves as being perpetrators or victims of bullying in the preceding month. The study also assessed whether participants had experienced the symptoms of depression, anxiety, and stress in the month prior to the survey. The researchers then analyzed the final results by comparing the responses to identify any associations between traditional bullying victimization, cyberbullying victimization and the levels of depression, anxiety and stress.



The study shows that Indigenous adolescents are often the victims of bullying both offline and online. More than one-third of Indigenous adolescents reported that they have experienced traditional bullying in the last month, and 1-in-6 reported that they experienced cyberbullying. Being a victim of cyberbullying appears to particularly contribute to experiences of depression, anxiety and stress among Indigenous youth. This study does have some limitations but makes clear the need for examination of the particulars of cyberbullying involving Indigenous adolescents in Canada.

Cyberbullying is a source of harm for one of society's most marginalized groups. The need for culturally informed prevention and intervention activities have been established. There is a need for victimization prevention and health promotion programs that are grounded in empirical data and responsive to the particular needs of Indigenous youth.

Cyberbullying victimization contributes to depression, anxiety, and stress among Indigenous adolescents. A better understanding of this issue is needed, as well as culturally appropriate prevention and response initiatives.

Broll, R., Dunlop, C., & Crooks, C. V. (2017). Cyberbullying and Internalizing Difficulties among Indigenous Adolescents in Canada: Beyond the Effect of Traditional Bullying. Journal of Child & Adolescent Trauma, 1-9.

A first look at browser-based Cryptojacking

Recently, there has been a trend in websites using their viewers' computers to mine cryptocurrency as an alternative source of revenue; often without their consent. This form browser-based cryptocurrency mining raises important ethical questions. Cryptocurrency Mining uses computer resources to solve particular computational puzzles, the solution to which provides some monetary value. Mining cryptocurrencies with programs that run inside a web browser started in the early days of Bitcoin. Their use was overshadowed by the relative efficiency of mining programs running natively, making use of Graphics Processors and purpose-built processors. Monero is a more recently developed cryptocurrency alternative to Bitcoin. Mining Monero requires different resources to Bitcoin, it uses more system memory and less processor, which is less suited to using GPU processing. Browser-based mining is consequently better suited to mining Monero. Developed in 2017, Coinhive is a service that allows webpage developers to easily insert Monero mining into their webpages.

Eskandari, Leoutsarakos, Mursch, and Clark surveyed the circumstances that gave rise to browser-based cryptocurrency mining and measured the prevalence and profitability such mining using Coinhive.

They analysed the top million sites in the Zmap database and matched that against the PublicWWW database and found in the Fall of 2017, at least 30 000 websites with Coinhive's Javascript code in the body of their page. It is possible that some of these sites may have had the code inserted into their page without their consent. The researchers found that browser-based mining through Javascript was typically configured to use around 25% of a user's CPU, with this figure at times reaching up to 100% of a computer's processing power. At the time of the study, Coinhive was being deployed on about 11 000 parked or 'cybersquatted' domains. The researchers

used Google Analytics to determine how many people visited these websites in a 3-month period. They then used Coinhive's dashboard to show that the parked domains had accumulated 105 580 user sessions for an average of 24 seconds per session. In total, the amount of revenue earned through these domains during this period was valued at a total of $7.69 USD.

This practice presents ethical questions as depending on how the mining is implemented, as it may use a persons' resources without their knowledge, consent or without certainty that the person understands the exchange they have consented to.

The researchers offer two forms of mitigation in terms of protecting users from non-consensual browser-based mining. The first is quite simply for cryptocurrency mining developers to obtain implicit or explicit user consent before using people's computer resources. The other is for browser developers to intervene in cryptocurrency mining to prevent mining, or to promote mining as an income alternative to online ads. It is also important to assess who is mining and whether they have obtained the consent of the website owner and visitors before mining, which may be beginning vector points in any ethical assessments of browser-based mining.

There is a need for more discussion as to what it means to obtain user consent in browser-based cryptomining.

Eskandari, Shayan, Andreas Leoutsarakos, Troy Mursch, and Jeremy Clark. "A first look at browser-based Cryptojacking." arXiv preprint arXiv:1803.02887 (2018).

Law Enforcement in the Age of Big Data and Surveillance Intermediaries: Transparency Challenges

The nature and scale of the police use of social media data has been evolving quickly. New technologies and industries have sprung up to support innovative explorations into social media supported surveillance, profiling and prediction. Despite these techniques raising privacy and social justice concerns, the regulation of police surveillance through social media data has been limited.

Scassa contends that new approaches to transparency are essential for the public to learn as much as possible on how police use social media data for surveillance purposes. Generally, a police search or surveillance via social media involving information considered private requires a warrant. In the case of information obtained through data analytics performed on the substantial collections of social media data held by private companies, it is unclear whether the data searched is public or private. However, many aspects of the data, its ownership and its processing could be considered to be private.

The companies involved facilitate the analysis of publicly available data such as geolocation and posts on social media. For example, data analytics company Geofeedia offered its services to law enforcement after prominent protests against police violence against African Americans, exacerbating a climate of mistrust, racial division, and the sense that authorities surveilled and targeted minority communities. The commercial motivations of social media companies creates risk for activists facing dictatorial regimes in 'crisis moments' such as public protests as they have little awareness of or control over the data they contribute to the platform.

A fundamental issue here is the protection of civil liberties, namely the right to privacy and the related rights of free speech, freedom of association, and the right to be free from discrimination. The right to privacy and free from unauthorised surveillance has been the traditional lens for assessing the oversight of law enforcement and national security activities. This lens requires transparency so that unreasonable searches or invasions of privacy can be detected. In the context of social media and big data technologies the oversight requires deeper understanding of the technology.

Scassa observes that law enforcement, policy makers and corporations that work in social media and data analytics are three entities that need to recalibrate the level of transparency that characterizes their practices. She proposes a three-part transparency approach, where a commitment to transparency is baked into regulation over the use of social media data for both public and private institutions, particularly as it concerns the 1) creation of policy, 2) the oversight of those institutions, and 3) in instances of redress. Policies around the acceptable use of services that do not permit invasive uses of the services could be helpful in establishing how these services should be used, however in the case of Geofeedia it was a mechanism for passing responsibility to others. Policies for the police use of data would help assert acceptable use. Despite the difficulties of implementation, some transparency/oversight mechanisms have long been part of the legal framework governing such activities. An approach to transparency for these activities could be to require policy for the transparent operation of the police; the platforms with users about how and what information will be used for what; and developers' use of platform data. Oversight is required to ensure that police and social media companies comply with their established policies. These policies should be enforced proactively by companies as well as part of a response to revealed problems.

Scassa contends that our current regulatory systems are inadequate, and that individuals still hold a reasonable expectation of privacy in aggregated data obtained through automation. Increased transparency will facilitate better public knowledge about how law enforcement uses social media data. It will also help decision makers devise appropriate limits and oversight regarding the use of social media data analytics in state surveillance and monitoring programs.

Transparency measures for the use of social media data by law enforcement are increasingly important as existing laws and paradigms may be inadequate to address surveillance

Scassa, T. (2017). Law enforcement in the age of big data and surveillance intermediaries: Transparency challenges. SCRIPTed, 14, 239.

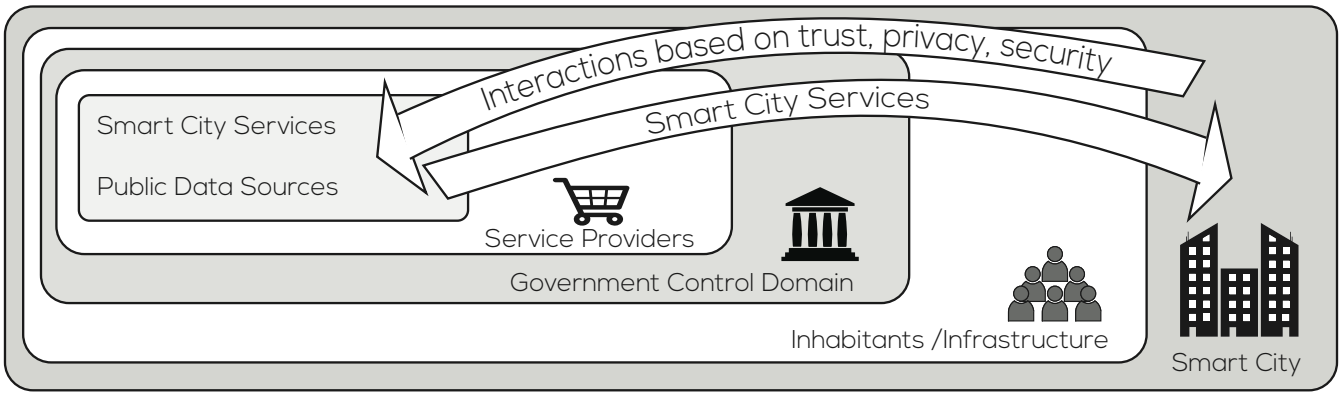
Security and Privacy Challenges in Smart Cities

The increased prevalence of technology in city infrastructure brings new privacy and security concerns. Major cities have already begun implementing 'smart' principles to increase the efficiency, safety, and convenience of city management.

Braun, Fung, Iqbal, and Shah argue that it is necessary to pre-emptively address the privacy and security concerns that Smart Cities raise in order to achieve these goals. They outline the major challenges posed by smart cities that could result in costly disruptions and destabilize personal privacy.

Smart Cities create privacy threats due to their reliance on rapid data sharing between multiple service providers. Combining multiple datasets allows for analysis of the data as a whole, potentially revealing information or identifying persons in ways that the individual service providers could otherwise not have and that consumers might not expect. Differential privacy is a relatively strong model for ensuring privacy and provides a measurable level of protection. An alternative is planning and reducing the types of data that are collected and analyzed, however there are some logistical issues with this approach. An approach to Smart Cities that makes use of privacy frameworks in the planning, design and implementation of technologies and their integration would be helpful.

The interconnectivity of Smart Cities and the inclusion of IoT devices results in many possible points of attack. In addition to layered security on individual devices, security across the city is required. An approach that could work for security within Smart Cities is to separate the network into three layers; known as the 3-Layer Onion



Model. Within this network all network devices have a unique identifying number and operate within the security layers. The governmental control domain layer regulates compliance with policy. The smart city Inhabitants/ Infrastructure Layer authenticates inhabitants and secures privacy. The service provider layer provisions and secures data sharing among service providers.

Smart Cities also raise issues around the collection, management and deletion of data. The quantity and nature of the data needs could be solved using cloud services. However, it is unclear what happens to data collected in a smart city, how data is stored and secured, who is responsible for data breaches, when is it disposed of and whether people are able to truly remove personal data once it is collected.

Preserving the trust of inhabitants is important for the sustainable operation of a smart city. This trust is challenged by concerns about the use of data and what consent looks like for both the subjects of data collection and use. There are helpful systems to preserve trust through computational trust, transparency and clear definitions of consent. In all cases, the inhabitants should be central to smart city design and implementation.

A thorough analysis of the privacy and security challenges posed by Smart Cities will be crucial in their success. Smart Cities must be marked by a carefully planned and holistic system of defence.

The success of Smart Cities may depend on a thorough analysis of their privacy and security challenges followed by a carefully planned and holistic system of defense.

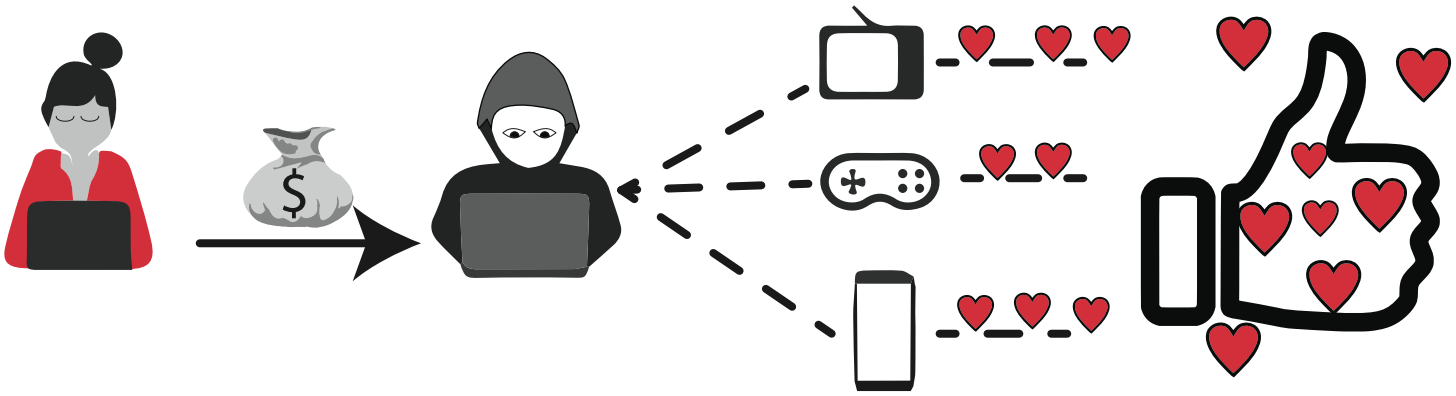
Braun, T., Fung, B. C., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. Sustainable cities and society, 39, 499-507.

Can We Trust Social Media Data? Social Network Manipulation by an IoT Botnet.

Social media fraud is generating likes, friends, views or any other action on social media services to artificially increase a following. While it offers social media users a cheap and easy means to approximate digital influence, it generates considerable costs for social media providers and funds botnet operators. In addition, it erodes the trust of its users.

Paquet-Clouston, Bilodeau and Décary-Hétu sought to gain a deeper understanding of the illicit market for social media fraud. They evaluated the supply of social media fraud services by analyzing their availability and cost. They deployed machines inside the Linux/Moose botnet to observe its operations and profile its customers. It is one of the first-time researchers have analyzed social media fraud from the inside of a botnet.

The team queried Google between January and December 2016 and found over 5,600 ads for social media fraud services. During that time frame, the team collected traffic internal to the Linux/Moose botnet, a botnet that connects to social media services through compromised routers and Internet of Things (IoT) devices. They collected over 273,000 transactions. Most of these transactions were directed at Instagram. By analyzing the transactions, the researchers identified 522 accounts that seemed to have used social media fraud.



The study revealed that social media fraud services are varied and readily available. They are offered at a variety of prices which makes them accessible to any type of consumer. Prices vary depending on the targeted social media platforms. It appears that services that are more difficult to defraud are more expensive. Instagram services were generally less expensive. The researchers also found that the customer base for such services is diverse. Individuals make up the largest category of consumers, followed by companies and entrepreneurs. The fake-user account detection measures on Instagram generally detect and shut down fake accounts within six months of their creation. However, these measures do not prevent Linux/Moose from operating.

The researchers suggested that tackling this issue would require actions on several fronts, including:

- Designing better registration and account-creation barriers.
- Provide social media users with legitimate and affordable solutions to grow their fan base.
- Raise awareness among social media users of the illicit nature of social media fraud services.

Reducing social media fraud requires action from a wide range of actors including consumers, social media platform owners, law enforcement agencies and service providers.

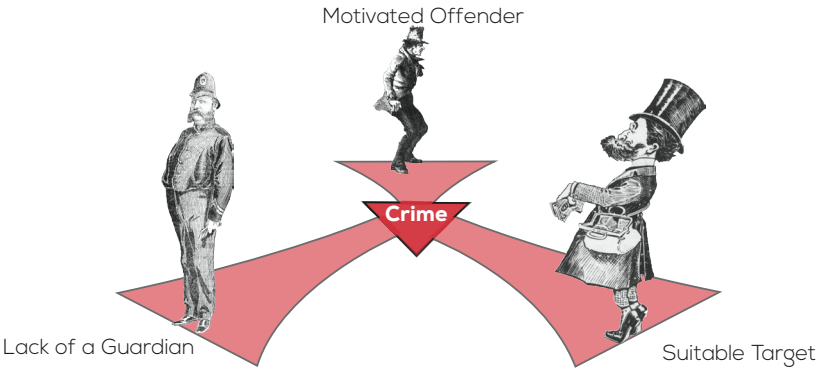
Viable strategies for countering Social Media Fraud could include raising user awareness and hindering supply to drive up prices.

Paquet-Clouston, M., Bilodeau, O., Decary-Hetu, D. (2017). "Can We Trust Social Media Data? Social Network Manipulation by an IoT Botnet". Proceedings of the 2017 International Conference on Social media and Society. Jul 28-30. Toronto, CA.

Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory

Breaches of businesses computer networks security constitute a great threat to the economic UK's security. While a lot of attention is payed to the hacking of networks, threats from inside the organisation have also proven to be harmful.

Williams, Levi, Burnap and Gundur tested the applicability of the criminological routine activities theory to insider cybercrime. Routine activities theory proposes that the possibility of a crime increases when a suitable target and a motivated offender meet at a time and place without a capable guardian being present.



To test the theory's applicability to insider cybercrime in organisations, Williams et al. represented its key components as such:

Routine activities: technological practices including bring-your-own-devices (BYOD), remote working, use of social medias, etc.

Guardianship practices: awareness of insider cybercrime risk, presence of security managers and worry of insider threats.

The team used data from the Cardiff University UK Business Cybercrime Victimization Survey to measure the impact of routine activities and guardianship practices on insider cybercrime. All of the private sector organisations in the United Kingdom were grouped into industry sectors and number of employees. Organisations that had no employees other than the owner were removed from the organisations list and offices other than the head office were also removed in cases where companies had more than one office. A list of companies to survey was randomly generated from the list and 751 companies answered questions about their experience with insider cybercrime.

Almost 10 percent of the respondents reported having experienced insider cybercrime. The organisation size was the greatest predictor of insider cybercrime victimization. 37% of organisations with more than 250 employees had experienced insider cybercrime in contrast to 3% of organisations with less than 10 employees.

Guardianship measures and routine activities each explained up to 13% of the difference in the possibility of an organisation becoming a victim of insider cybercrime. The presence of a dedicated cybersecurity manager, worrying over cybercrime and low security awareness were linked to insider cybercrime victimization. The authors suggested that these guardianship measures could have been implemented after organisations had experienced insider cybercrime. The experience of crime leads to worry, which in turn leads to hiring a security manager. Of the routine activities tested in the study, the storing of confidential data, the use of mobile devices and the ability to remotely access organisations' networks were found to be predictive of the likelihood of victimization.

Interestingly, the use of employee's own devices (BYOD) and correlation between victimization likelihood and the use of new technologies such as Wi-Fi, social media or cloud services were not a good predictor of insider crime. The researchers suggest that these services to not provide a great opportunity for insider crime as they often include security measures.

While insider cybercrime is still a new research area, this study shows that theories from more developed fields such as criminology may provide a theoretical framework to provide insight into this phenomenon.

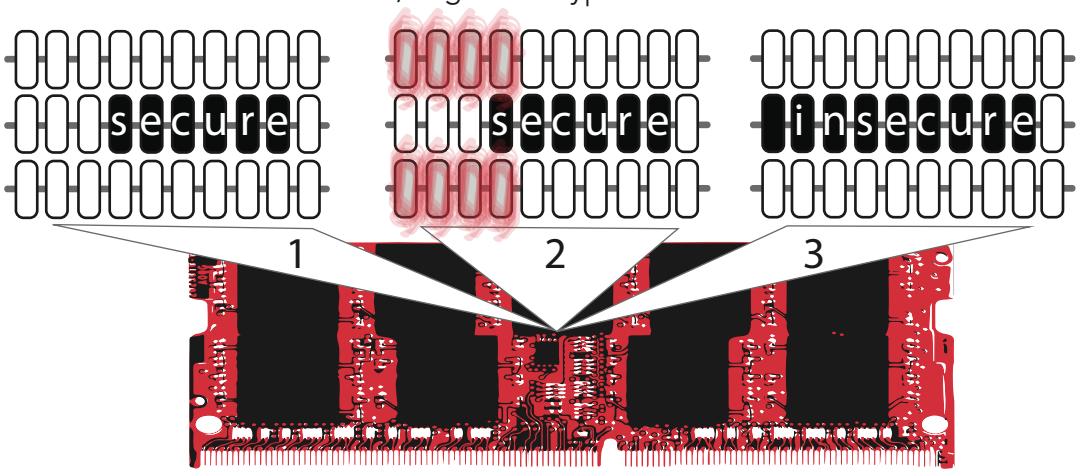
Hiring a Security manager and raising awareness about cybersecurity issues may help more than limiting BYOD and Social Media use in reducing the threat of cybercrime by insiders.

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2018). Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory. Deviant Behavior, 1-13.

Throwhammer: Rowhammer Attacks over the Network and Defenses

System attacks at the physical level can bypass security software and operating system controls. This makes them particularly dangerous as they can make any system vulnerable. It has been widely assumed that such an attack required executing a malicious program directly on the target computer. This is not necessarily the case.

Computer memory makes use of tiny capacitors that temporarily store an electrical charge. An uncharged capacitor stores a '0' and a charged capacitor stores a '1'. These bits of data are bundled together into large arrays to store complex information and instructions for the computer. Modern memory packs data storing capacitors very closely together and uses smaller electrical charges because of the demands of greater speed and miniaturization. The proximity means that it is possible for small amounts of electricity to overflow into neighbouring capacitors. Using smaller charges means that this might be enough to change the value of a capacitor from a '0' to a '1'. Rowhammer attacks take advantage of this by aggressively charging and discharging capacitors in the hope their neighbours will change value. Changing a '0' to a '1' in some memory locations could reverse access restrictions, negate encryption etc.



Tatar, Krishnan Konoth, Athanasopulos, Giuffrida, Bos and Razavi demonstrated that it is possible to deliver a Rowhammer attack via a network connection. Ethernet network cards equipped with remote direct memory access (RDMA) allow devices on a network to exchange data directly in the devices' main memory. This mechanism is used in high-performance networking operations such as data centers or for cloud services. The researchers showed that with a bandwidth speed of 10 Gbps, attackers can deliver 560,000 packets per 64 milliseconds to the memory on a remote computer. At this speed a Rowhammer type attack is possible and by changing data stored in restricted memory locations they could gain the ability to execute commands on a system. Tatar et al. demonstrated the exploitation of this flaw against a RDMA-enabled short-term application memory system on two test machines. They were able to store sensitive data in vulnerable memory locations; corrupting data and compromising the systems.

Tatar et al. proposed a solution that isolates the specific memory bits vulnerable to these attacks. This tool uses a novel memory allocation strategy to insert guard zones around vulnerable bits on a memory card and has a low impact on a system's performance.

Current mitigations based around preventing direct code execution are not necessarily effective against Rowhammer type attacks. This new method of this attack removes the need for direct access on the targeted machine.

Physical attacks like Rowhammer which overcome security controls can now be performed over the network.

Tatar, A., Konoth R.K., Athanasopoulos, E., Giuffrida, C., Bos, H. & Razavi, K. (2018). ‚ÄúThrowhammer: Rowhammer Attacks over the Network and Defenses.‚Äù Proceedings from the 2018 USENIX Annual Technical Conference (ATC, 2018). Jul 11-13. Boston, USA.

Learning Stylometric Representations for Authorship Analysis

The anonymous nature of the Internet makes it difficult to conclusively identify people online. The certainty of network-based identifications, such as IP address can be easily disputed. This presents an issue in the investigation of criminal activity. Stylometry is the study of linguistic style in order to differentiate between authors. This type of analysis has been presented in courts in the form of expert testimony to assist identifying the authors of texts. While authorship analysis is nothing new, previous techniques have relied on the manual selection of linguistic features to be analyzed.

Researchers Ding, Fung, Iqbal, and Cheung have developed models to automate the process of selecting subsets of linguistic features to be studied by leveraging machine learning techniques. Their proposed models for automated authorship analysis incorporate different sets of linguistic attributes for extraction and processing. These attributes include the content of the writing, contextual word choices, and grammatical and syntactical choices. By using an automated feature learning scheme that is guided by multi-pronged subsets of linguistic information, the researchers attempted to mitigate the issues related to the manual feature engineering process in current authorship analysis. Their proposed models are designed to effectively capture the differences of writing styles of different modalities between authors

The researchers used their system to analyze a publicly available database of English texts that is generally used for digital text forensics training and testing and contains hundreds of novels and essays. They compared the results of their model's ability to verify an author to other existing models. They then compared the performance of their model using a publicly available database of Twitter posts.

The researchers' experiment suggests that their proposed multi-pronged models of analysis outperforms pre-existing authorship analysis models and are effective and robust on numerous datasets and authorship analysis problems.

Advancements in authorship analysis can assist cybercrime investigations as well as provide analysis techniques for market, social network and social sciences research. The learning authorship analysis models present an advancement in automated stylometry that may prove valuable in cyber forensics analysis.

Advancements in automated author recognition using the texts they write online may assist cybercrime investigations.

Ding, S. H., Fung, B. C., Iqbal, F., & Cheung, W. K. (2017). Learning Stylometric Representations for Authorship Analysis. IEEE Transactions on Cybernetics.

serene-risc.ca

Smart Cybersecurity Network (SERENE-RISC) is a knowledge mobilization network that aims to be a cybersecurity exchange that is recognized as an open, inclusive, and unbiased forum to unlock the value of knowledge on cybersecurity risks, threats and solution for all Canadians. We are a network of networks that provides publications, tools, events, professional development and education. We are always looking for partners to collaborate to make cybersecurity better, so please contact us to find out more.

konnect.serene-risc.ca

Konnect provides greater access to research, presentations, groups, opinions and events important to improving Canadian Cybersecurity. It brings together the academic, private and public sectors to share and make sense of new understandings. Summaries and articles at the website are shared on Twitter, LinkedIn, YouTube and email. As well as providing relevant content, we facilitate online exchange and provide information on events, employment and resources provided by members and partners.

The website https://konnect.serene-risc.ca provides a searchable, indexed collection of openly accessible content developed for and by the Canadian cybersecurity community. There is new content uploaded every week across four categories, research summaries, partner content, community profiles and videos.

You can help by:

- Subscribing to the regular update online at: **http://konnect.serene-risc.ca/subscribe-abonnement**
- Following **@SERENE_RISC** on twitter and retweeting,
- Joining the Linkedin Group and submitting or commenting on posts, and
- Posting links to **konnect.serene-risc.ca** content on other platforms you are involved with.

cybersec101.ca

Want to provide basic cybersecurity classes but don't know how or have the time to get started?

We have developed evidence-based materials that can help you quickly put on training programs. Find resource sheets, presentation videos, class tools and slides to build basic cybersecurity education and awareness sessions. There are ten modules in French and English with materials to help from basic concepts to practical step-by-steps for better security online.

donate

We are now accepting donations to help us provide more services that are open, accessible, inclusive and unbiased. You can download a donation form at https://www.serene-risc.ca/donation or contact us for more information at info@serene-risc.ca

 @SERENE_RISC  /serenerisc  /serene-risc

The SERENE-RISC Cybersecurity Knowledge Digest

Editor-in-Chief: Michael Joyce
Scientific Editor: Benoît Dupont
Editors: Yuan Stevens, Véronique Ménard

Government of Canada / Gouvernement du Canada
Networks of Centres of Excellence / Réseaux de centres d'excellence

serene risc

Université de Montréal