serene risc Digest Volume 2, Issue 3

Cutting Edge Research Summaries for Policy-Makers and Practitioners

Is everyone getting rich on ransomware?

Ransomware attacks have become a major concern for law enforcement and security professionals around the world. Ransomware attacks offer a valuable opportunity to measure the financial impact of cybercrime that through the Bitcoin cryptocurrency. Paquet-Clouston, Haslhofer and Dupont used an open-source cryptocurrency analytics platform to analyze transaction data from many types of ransomware.

They analyzed Bitcoin transactions related to ransomware attacks that occurred between 2013 and mid-2017.The collector addresses for each ransomware family were found by creating an outgoing-relationships graph for each ransomware family and grouping outputs. The market for ransomware payments for the 35 ransomware families is at least $ 12,768,536 USD; or 22,967.44 in Bitcoin. Interestingly, most of the ransomware appeared to be controlled by a few operators

Can Flow Analysis find hidden traffic on anonymity services ?

Anonymity networks are designed to provide users with privacy and are often used to overcome censorship. these services can masquerade as other types of service, such as a Skype call.

It is still possible to detect different forms of traffic by analysing the flow of the traffic.To better understand the capabilities of this technique Shabar and Zincir-Heywood created a machine learning based approach to flow analysis. Their study explored the application of flow analysis to differentiating anonymity networks from other traffic and each other. Flow analysis calculates statistical information extracted from the header of the packet to describe the communication between two parties.

The study found that the flow analysis has high accuracy in the identification of the encrypted anonymity networks.

How hard is it to make money running a botnet ?

Botnets and Malicious software (malware) being used to make money for criminals have become a serious threat to online security.

Putman, Abhishta and Niewenhuis examined four case studies to analyze the economic structure that supports botnets. The development of a botnet can be divided into three stages, malware acquisition, spreading malware, and botnet maintenance. Readily available malware packages and malware infection service make it possible to set up a profitable botnet business within days. The capital costs for acquiring and spreading malware, and ongoing costs like hosting and transaction fees are relatively minor compared with revenue with set-up costs accounting for a maximum of 1.1% of monthly revenue in three of the four cases studied. Profitability between various botnet related crime services varies drastically.

Can virtual assistants be controlled by voices that you can't hear?

The use of speech recognition to interact with computers is becoming more and more popular. The researchers Zhang et al. developed an attack that can control virtual assistants but is inaudible to humans.

To overcome the filtering of inaudible noise the researchers exploited a property of sound known as 'non-linear effects' in order to produce harmonics within the expected frequency at the microphone from loud but inaudible sounds.They validated DolphinAttack in multiple languages on 7 popular speech recognition systems (e.g., Siri, Google Now, Alexa) and across 16 common voice controllable system platforms. All tests were done with specialized hardware at close range. Speech recognition systems can be made more secure through hardware-based defences (such as microphone enhancement and baseband cancellation) and software-based defences.

What kind of security policy do you need when you operate in an adversarial environment?

Humanitarian organisations operate under conditions that create unique information security challenges. Researchers Le Blond et al. interviewed staff of the International Red Cross to provide a view of the information security challenges they face at the individual, organizational, and legal levels. Operations are affected by the vulnerability of their beneficiaries, as they are often unable to safely access technology, the need for collaboration which requires sharing of data in some form, the threat of coercion of employees in the form of threats, physical security as operations could be located in hostile environments, the use of mobile devices. Operating in adverse and adversarial environments is sometimes necessary in order to reach the goals of an organisation. In this extreme environment security policy must encompass technical, legal, procedural and physical safeguards while also allowing for trade-offs to be made when required.

Does a secure protocol guarantee a secure connection?

Wi-Fi networks are secured using a communications protocol called Wi-Fi Protected Access (WPA/2). The protocol defines how exchange messages to setup and maintain secret (encrypted) communications by what is known as a 4-way handshake. Vanhoef and Piessens identified design flaws in the 4-way handshake. All Wi-Fi clients that they tested were vulnerable to an attack against the handshake.

An interesting characteristic of this attack is that it does not violate the security properties of the handshake method as proven in formal analysis. This research showed the limitations of the WPA security protocol with regards to the implementation of the 4-way handshake. It also highlights an important lesson for the community in showing that a secure protocol does not make for a secure implementation.

Are Repeat Buyers in Cryptomarkets Loyal Customers?

The Internet has proven to be an effective way to buy and sell, even for illegal products. Crypomarkets are an innovation that provides greater protections for venders and consumers of illegal products. Decary-Hetu and Quessy-Dore examined cryptomarkets to better understand the role customer loyalty plays in market function. The researchers developed a custom software tool to monitor the activities of cryptomarket participants by gathering data from cryptomarket pages. On average repeat buyers made purchases from 15 vendors and concentrated a third of their purchases with a single vendor across the entire marketplace. There was a great deal of variation between buyers across the market though, which may be due to purchases across a range of products. Repeat buyers may decide to buy from vendors apart from their main supplier to limit their dependence on a single vendor and to establish their trustworthiness on the cryptomarket. Not all vendors manage to build a loyal customer base and buyers may be careful to maintain a diversity of vendor relationships, but generally favor a small number of suppliers.

Is the abuse suffered in Romance Fraud so different from Domestic Abuse?

The use of online services to meet romantic partners has facilitated the emergence of a type of online crime referred to as Romance Fraud. Criminals develop romantic relationships with people for the purpose of extorting money from them. Cross, Dragiewicz and Richards reviewed the limited research on romance fraud together with that on domestic violence. They aimed to highlight key aspects of psychological abuses in the domestic violence context that could help understand romance fraud.

They interviewed twenty-one victims of romance fraud that were identified in a 2016 study on the experiences and support needs of online fraud victims in Australia. There appeared to be a significant overlap between romance fraud and domestic violence cases. Eight of the nine psychological maltreatment categories were found in the interviews.

The authors noted that romance fraud victims are often perceived as being responsible for their circumstances. They suggested that demonstrating the presence of psychological maltreatment in romance fraud could help victims access a genuine victim status, which is critical in obtaining services and criminal justice support.

Is online location detection good enough for security services?

Location-based services prevent or facilitate access or actions online, such as media streaming, online voting or gambling, fraud prevention based on the physical location of the requesting party.

Abdou, Matrawy, and van Oorschot explain new technique attacks that enable adversaries to accurately manipulate the location indicated by these delay-based techniques. A sender can measure the delay between itself and a receiver by having the receiver respond to special data packets and timing the responses. By selectively manipulating the delay on these packets in a precise manner an adversary would be able to appear to be in a different location. The researchers presented techniques based on a variety of attacker scenarios, to assess the potential for accurately modeling and presenting a fake location to various location detection services. The measured delays used for location services are able to be manipulated.

Security-sensitive applications should not rely on constrained region areas for distinguishing legitimate clients.

What can health teach us about security awareness?

People using the internet for their own personal reasons are largely left to fend for themselves. Although they might be aware of the risks, they don't always act consistently to protect themselves.

Dodel and Mesch examined whether knowledge from the long-established work in health awareness could inform cybersecurity awareness campaigns. The Health Belief Model (HBM) considers the perceptions people have about threats and their expectations when investigating their precautionary activities.

Data were collected as part of a larger a national sample of the Israeli adults was surveyed in October 2014, collecting 1850 completed interviews. The results suggest that methods other than awareness messaging focusing on compliance to avoid threats could be beneficial.

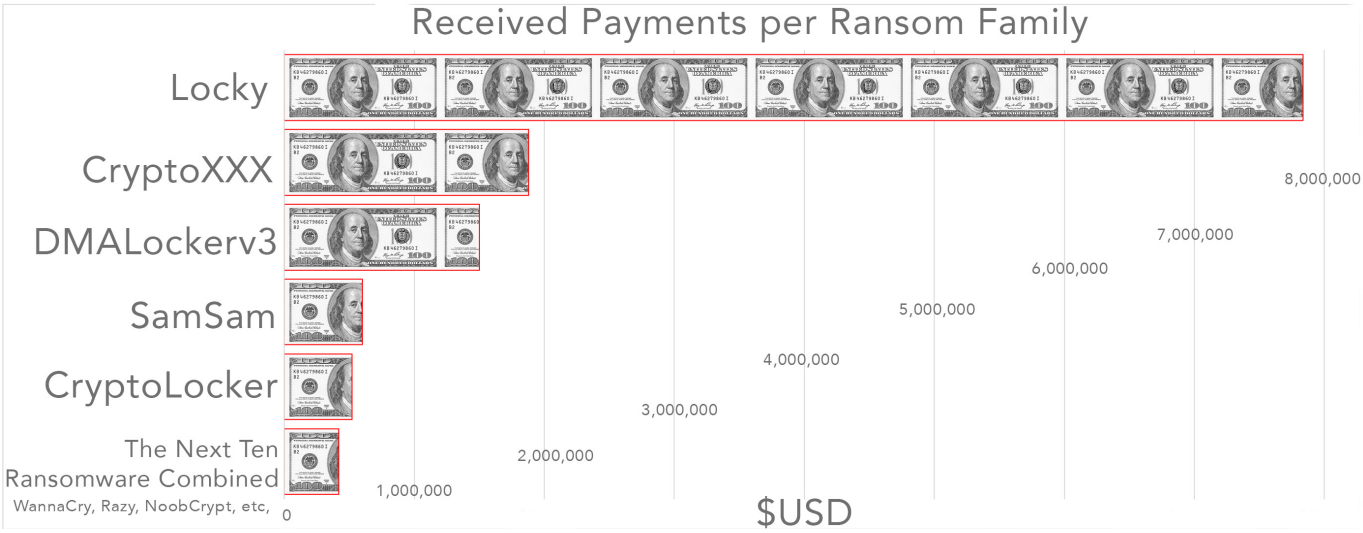
Fear-based messages underscore the susceptibility of Internet users to cyber-attacks and the seriousness of the consequences, which could undermine peoples' belief in their ability to protect themselves.

Ransomware Payments in the Bitcoin Ecosystem

Ransomware attacks have become a major concern for law enforcement and security professionals around the world. Recent prominent attacks by ransomware including WannaCry, Locky and SamSam affected hundreds of thousands of people around the world. Ransomware infects the device of a victim with malicious software that blocks access until they pay a ransom to the attacker, most often by cryptocurrency. Due to this payment method ransomware attacks also offer a valuable opportunity to measure the financial impact of cybercrime by tracing movements of Bitcoin cryptocurrency.

Paquet-Clouston, Haslhofer and Dupont analyzed the transaction data from many types of ransomware using an open-source cryptocurrency analytics platform. They analyzed Bitcoin transactions related to ransomware attacks that occurred between 2013 and the middle of 2017. They extracted 7,222 Bitcoin addresses, each of which identify a Bitcoin wallet related to 67 ransomware families. From these addresses they were able to study 35 ransomware families. They did this by finding the addresses related to each ransomware family, identifying the payer and payee accounts and tracking the flow of money. They have made their data extraction and analysis procedures available for use by other researchers.

The collector addresses for each ransomware family were found by creating an outgoing-relationships graph for each ransomware family and grouping outputs. Characteristics of the relationships and contextual information were used to group the addresses. The collector addresses were not necessarily part of the cluster containing the family's seed and expanded addresses. Some collector addresses are part of larger clusters from Bitcoin exchange services gambling sites, or 'mixer' services, all of which are used to obscure money flows.



The market for ransomware payments for the 35 ransomware families is at least $ 12,768,536 USD; or 22,967.44 in Bitcoin. Interestingly, most of the ransomware appeared to be controlled by a few operators. Three families of ransomware accounted for 86% of the market. Not all ransomware contributes equally to the direct financial costs on victims. More than 50% of the nearly thirteen million dollars was from the 'Locky' strain of ransomware. The methods developed for this research could be applied to other illicit activities using cryptocurrencies to provide evidence-based insights for policymakers.

Identifying Bitcoin transactions used in ransomware attacks can help understand the size of the illicit market of ransomware payments and direct responses more effectively.

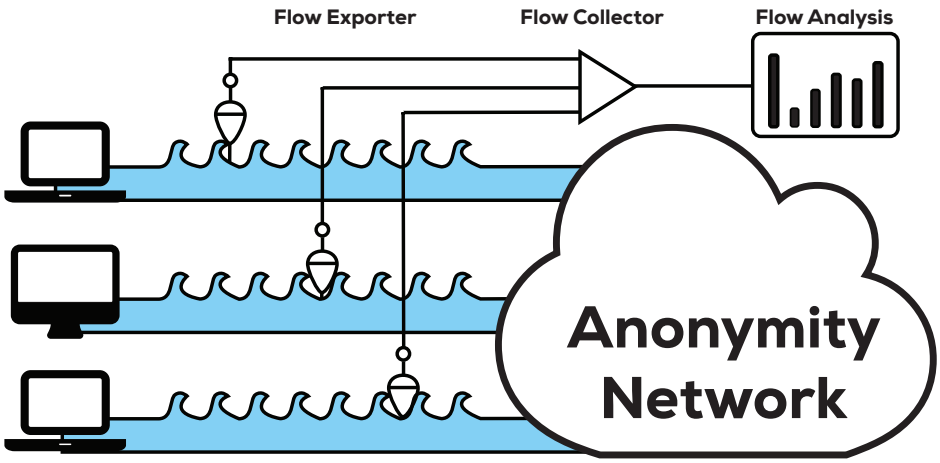
Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2018). Ransomware Payments in the Bitcoin Ecosystem. arXiv preprint arXiv:1804.04080.

How Far Can We Push Flow Analysis to Identify Encrypted Anonymity Network Traffic?

Anonymity networks are designed to provide users with privacy and are often used to overcome censorship. These networks encrypt and relay traffic through multiple destinations to hide the origin of internet traffic to provide this privacy. The networks make private the actions of an Internet user but their operation is not secret, so their service can be blocked. In order to overcome this weakness these services can masquerade as other types of service, such as a Skype call. This is not a perfect solution for those seeking confidentiality however as it is still possible to detect different forms of traffic by analysing the flow of the traffic.

To better understand the capabilities of this technique Shabar and Zincir-Heywood created a machine learning based approach to flow analysis. Their study explored the application of flow analysis to detect data traffic from anonymity networks.

Collecting privacy network data might adversely affect network users' privacy, which presents a complications for researchers of privacy networks. Research has often relied on data collected from a simulated environment or from researchers themselves. This research was based on the Anon17 dataset produced by the NIMS lab over a period of three years and which contains traffic from three well-known anonymity networks, Tor, JonDonym and I2P. The dataset has been modified to anonymize the data while maintaining its research value. This dataset has been made available to other researchers.



The researchers used a selection of machine learning algorithms to identify the extracted traffic flows. They were able to identify the traffic successfully with greater than 90% accuracy, up to 99%. The accuracy of detection varied based on the applications, the anonymity network, and the user's configuration. Since anonymity networks may be diverse and the flow analysis is widely used to study anonymity networks, it is of importance to explore the boundaries of the flow analysis potential in anonymity network analysis. Using a category-based approach, the study found that the flow analysis has high accuracy in the identification of the encrypted anonymity networks.

Flow based traffic analysis can identify concealed privacy network traffic on a connection.

Shahbar, K., & Zincir-Heywood, A. N. (2018, April). How far can we push flow analysis to identify encrypted anonymity network traffic?. In NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium (pp. 1-6). IEEE.

Business Model of a Botnet

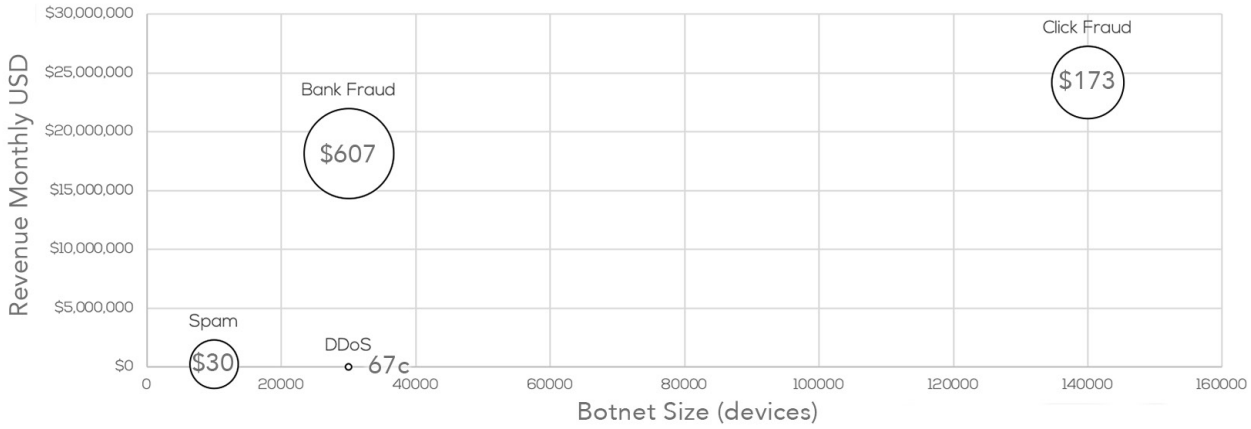
Criminal botnets and malicious software (malware) have become a serious threat to online security. However, little is known about exactly how much and how revenue from this software flows through illicit online industry.

Putman, Abhishta and Niewenhuis examined four case studies to analyze the economic structure that supports botnets. Botnets often are used to provide illegitimate online services. They looked at botnets that offered spamming, bank-credential theft, DDoS attack and click-fraud services. The development of a botnet can be divided into three stages, malware acquisition, malware spreading and botnet maintenance.

To acquire malware, botmasters choose between developing new malware or purchasing ready-to-use botnet packages. New malware can be adopted at a level suiting the technical proficiency of the botnet operator. They can choose to purchase all or part of the malware, or purchase training materials. Each of these options require different levels of investment.

The second stage in creating a botnet consists of spreading the malware to as many devices as possible. There are a number of methods for doing this, all of which attract a cost. An understanding of the costs can be understood from pay-per-installation service providers. They charge between 2 and 10 cents per infected device.

The final stage of maintaining a botnet requires ongoing administration as changes such as software patching and security updates can remove devices from the botnet. Malware must be updated frequently and devices must be reacquired, resulting in additional development and installation costs. The cost of reinfection or replacement of lost botnet devices could again be estimated at between 2 and 10 cents. There are also ongoing costs such as the fees for hosting services need for the botnet management infrastructure. The relative cost of these services is dependent on the services provided. While these costs are significant for DDoS providers, consuming approximately 25% of monthly revenue, they are relatively small for other types of service. Payments for services are often handled by third-party service providers. Of all of the service providers that support botnet operators, money handlers appeared to be the most profitable.



Readily available malware packages and malware infection service make it possible to set up a profitable botnet business within days. The capital costs for acquiring and spreading malware as well as the ongoing costs such as hosting and transaction fees are relatively small, amounting to a maximum of 1.1% of monthly revenue in three of the four cases studied. Profitability between various botnet related crime services varies drastically. DDoS-for-hire (Booter Services) are the least profitable, but appear to be less risky as they last the longest.

Setting up botnet can be quick and cheap but the profitability and management costs can vary depending on the type of illegal services offered.

Putman, C. G. J., & Nieuwenhuis, L. J. (2018, March). Business model of a botnet. In 2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP) (pp. 441-445). IEEE.

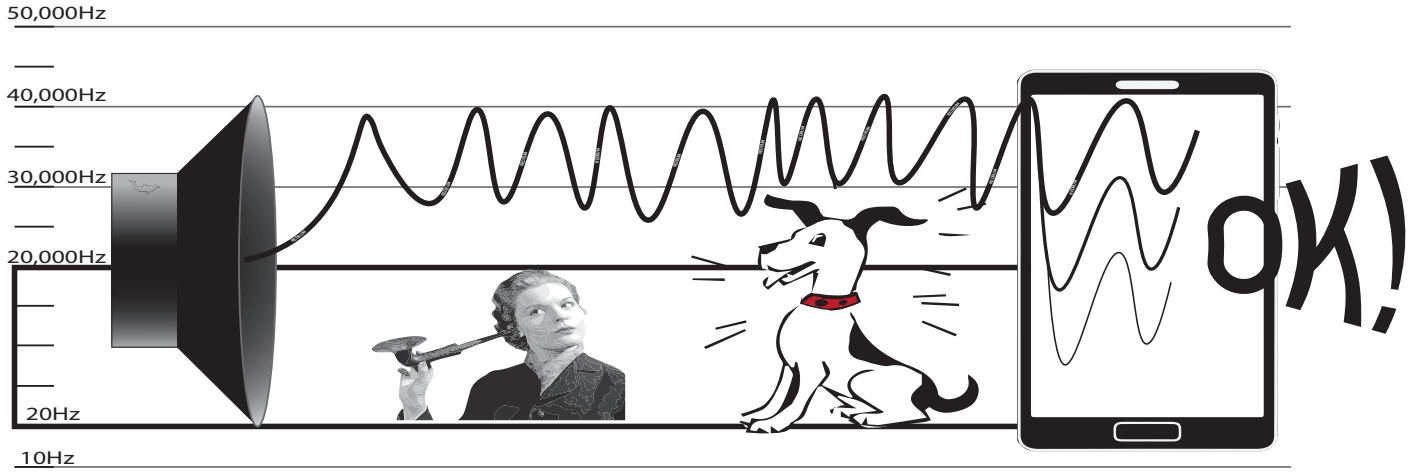
DolphinAttack: Inaudible Voice Commands

The use of speech recognition to interact with computers is becoming more and more popular. Voice control can be used with an increasing number of online services; such as ordering food or scheduling a ride. However, little is known about how these systems respond to malicious and sneaky attacks. It is possible to control these systems with noise that is unintelligible to humans, but they would still hear a noise.

The researchers Zhang et al. took this a step further by developing an attack that is inaudible to humans; which they called DolphinAttack. They were able to initiate a FaceTime call on iPhone, activate Google Now to switch the phone to airplane mode and even manipulate the navigation system in an Audi automobile without being heard by a person.

Humans can hear sounds in the range between the frequencies of 20Hz and 20,000 Hz. Any sounds outside of this range are inaudible to people. Unsurprisingly, audio equipment normally filters out sounds outside of this range. To overcome the filtering the researchers exploited a property of sound known as 'non-linear effects' in order to produce harmonics within the expected frequency at the microphone from loud but inaudible sounds.

Using this technique, they were able to both activate the listening mode and provide instruction by producing harmonics from snippets of the device owners voice or by brute forcing voice tonalities to overcome voice pattern matching authentication.



In an experiment to test the feasibility of this kind of attack they used a specialised speaker placed at a distance of less than 2 metres from the device. The effectiveness of the attacks were reduced in environments where there was greater background noise, or with greater distances or lower attack volumes. They validated DolphinAttack in multiple languages on 7 popular speech recognition systems (e.g., Siri, Google Now, Alexa) and across 16 common voice controllable system platforms. The researchers recommend both hardware-based and software-based defense strategies to mitigate attacks, such as limiting the operating range of microphones and better detecting modulated voice commands.

It is possible to generate voice commands for services like Siri that humans can,Äôt hear to do things on the device.

Zhang, G., Yan, C., Ji, X., Zhang, T., Zhang, T., & Xu, W. (2017, October). Dolphinattack: Inaudible voice commands. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 103-117). ACM.

On Enforcing the Digital Immunity of a Large Humanitarian Organization

Humanitarian organisations operate under conditions that create unique information security challenges. Operating across borders to provide services in disaster areas and conflict zones highlights information security threats and threat actors. The experiences of the International Committee of the Red Cross (ICRC) provide insight into the difficulties and trade-offs faced by multinational, multi-stakeholder organisations.

Researchers Le Blond et al interviewed 27 ICRC field workers, IT staff, lawyers, and managers. Those interviews together represented over 250 years of experience in humanitarian field work, data protection, and management. The responses provided a view of the information security challenges in terms of the individual, organization and the law.

The operations of the ICRC are affected by the vulnerability of their beneficiaries, as they are often unable to safely access technology. This can be unavoidable, as the need for collaboration often requires sharing of data in some form. There is also the threat of coercion of employees by violent or other means, on top of the difficulties of providing physical security for operations located in hostile environments. The safeguards put in place much as possible consider these factors. Measures such as local encryption and offsite storage of data, data access limitations and procedural controls are all used to minimize risk. Further, there are legal factors to consider as there are restrictions on data sharing across jurisdictions. Present loopholes in legal safeguards and regional legal immunities and pressures that need to be considered when designing safe systems and policies. This complexity requires that the ICRC is careful when collecting data, being sure to understand data in terms of its type and sensitivity to ensure it is properly handled. Risk mitigation techniques include data minimization, obfuscation and pseudonymization.

Lessons that could be learned from the experience of ICRC are headed by the importance of coercion resistance in operational security policy. The ICRC worked to address this by providing data access on a need-to-know basis, including citizenship in the consideration of system administrator access policy and by segregating data between delegations. Further, it is important to consider the practical needs for cooperation or capacity building work that may require managed security trade-offs. Despite employing effective and novel security technologies and practices to provide humanitarian services in adverse and adversarial environments it is not always possible to find an optimal outcome. It is necessary to tolerate less than perfect security from third parties and beneficiaries depending on their vulnerability and technical capacities and accept that cross border legal issues may compromise the availability of data.

Operating in adverse and adversarial environments is sometimes necessary in order to reach the goals of an organisation. In this extreme environment security policy must encompass technical, legal, procedural and physical safeguards while also allowing for trade-offs to be made when required.

In extreme environments such as those faced by humanitarian organisations security policy must include technical, legal, procedural and physical safeguards while permitting necessary trade-offs.

Le Blond, S., Cuevas, A., Troncoso-Pastoriza, J. R., Jovanovic, P., Ford, B., & Hubaux, J. P. (2018, May). On Enforcing the Digital Immunity of a Large Humanitarian Organization. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 424-440). IEEE.

Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2

Wi-Fi networks are secured using a communications protocol called Wi-Fi Protected Access (WPA/2). The protocol defines how to exchange messages in order to create and maintain a secret (encrypted) communications service by what is known as a 4-way handshake. Vanhoef and Piessens identified design flaws in the 4-way handshake. All Wi-Fi clients that they tested were vulnerable to an attack against the handshake. This vulnerability (VU#228519) exploitation is known as a Key Reinstallation AttaCK (KRACK) and security patches to resolve the issue are available for many systems.

Under WPA/2, the decryption key is changed constantly to make it harder to guess. The first 2 messages of the handshake exchange counts (nonces and replay counters) so that the wifi access point and client know where in the sequence they are up to. The third message sends a new key based on those numbers. Under real-world conditions messages may be lost so the access point will resend the third message if it did not receive an appropriate response. This makes it possible for the client to receive the third message multiple times. To cope the client will use the key with this message and will reset its exchange count to match. An attacker may collect and resend the third message to a client forcing it to use the same key repetitively and undermine the security of communications. This could allow for the replay, decryption and forgery of messages.

Key reinstallation attacks can be mitigated by implementing a check as to whether an already-in-use key is being used and not reset associated counters in this case or assure that a particular key is only installed once during the handshake.

An interesting characteristic of this attack is that it does not violate the security properties of the handshake method as proven by formal analysis. This provides a lesson from this research that goes beyond the particular attack. It provides a clear example of how a formal proof of protocol security does not guarantee that its implementations are also secure. In this regard, formal proofs of security measures or counter-measures can be counterproductive as the community may lose interest in auditing implementations of a formally verified protocol. It also indicates the importance of precision and explicitness in the specification of protocols, as interpretation may differ from intent.

This research showed the limitations of the WPA/2 security protocol with regards to the implementation of the 4-way handshake. It also highlights an important lesson for the community by showing that a secure protocol does not make for a secure implementation.

A secure protocol does not imply a secure implementation.

Vanhoef, M., & Piessens, F. (2017, October). Key reinstallation attacks: Forcing nonce reuse in WPA2. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1313-1328). ACM.

Are Repeat Buyers in Cryptomarkets Loyal Customers? Repeat Business Between Dyads of Cryptomarket Vendors and Users

The Internet has proven to be an effective way to buy and sell, even for illegal products. Crypomarkets are an innovation that provide greater protections for venders and consumers of illegal products. A cryptomarket is a marketplace that hosts multiple sellers, provides anonymity and additional services such as aggregating customer feedback ratings and comments. Cryptomarkets allow vendors to reach a large number of potential buyers while attracting little police attention.

Décary-Hétu and Quessy-Doré examined cryptomarkets to better understand the role customer loyalty plays in market function. In economic terms, loyalty is the buyer's tendency to repeatedly purchase from the same vendor, despite other vendors being available. A range of factors can affect a buyer,Äôs loyalty to a vendor, such as competition, reputation, product familiarity, purchase experience and perceived transaction value. Resource limitations force organizations to do the same, by prioritizing certain customers. Illicit markets are competitive settings however and so cost still plays an important role in purchase decisions.

The researchers developed a custom software tool to monitor the activities of cryptomarket participants by gathering data from cryptomarket pages. Information of particular interest were product listings, vendor profiles, and feedback. This study included data from an active cryptomarket with 15,873 listings from 1,135 vendors in September 2015. This market made use of consistent and mostly unique usernames for buyers by representing their names with two letters. This allowed for more confident isolation of individual buyer activity.

On average, repeat buyers made purchases from 15 vendors and concentrated a third of their purchases with a single vendor across the entire marketplace. There was a great deal of variation between buyers across the market, which may be due to purchases across a range of products. Within a specific product category, repeat buyers purchase from just three vendors with 60% of their purchases coming from the same vendor, on average.

Vendors do not appear to foster more loyalty from repeat buyers. Furthermore, neither visibility nor customer-base size appear to impact the number of customers loyal to a vendor. Repeat buyers may decide to buy from vendors apart from their main supplier to limit their dependence on a single vendor and to establish their trustworthiness on the cryptomarket. Cryptomaket vendors can disappear without a trace. Vendors generally require a verification of the buyer's intentions through prepayment or an endorsement from another vendor; the latter being less risky for the buyer. This is in addition to normal value-seeking motivations for changing suppliers in a competitive market.

Vendors that provide more information about their products and themselves appear to have the best chance of building customer loyalty. Surprisingly, vendor reputation does not seem to play a great role in establishing a loyal customer base.

Cryptomarkets are competitive and inherent anonymity creates some challenges for vendors. Customer loyalty is positive for vendors as it inspires repeat business. Not all vendors manage to build a loyal customer-base and buyers may be careful to maintain a diversity of vendor relationships, but generally favor a small number of suppliers.

Cryptomarket customers carefully manage a balance between trusted suppliers and needed diversification.

Decary-Hetu, D., & Quessy-Dore O. (2017). Are repeat buyers in cryptomarkets loyal customers? Repeat business between dyads of cryptomarket vendors and users. American Behavioral Scientist, 61(11), 1341-1357.

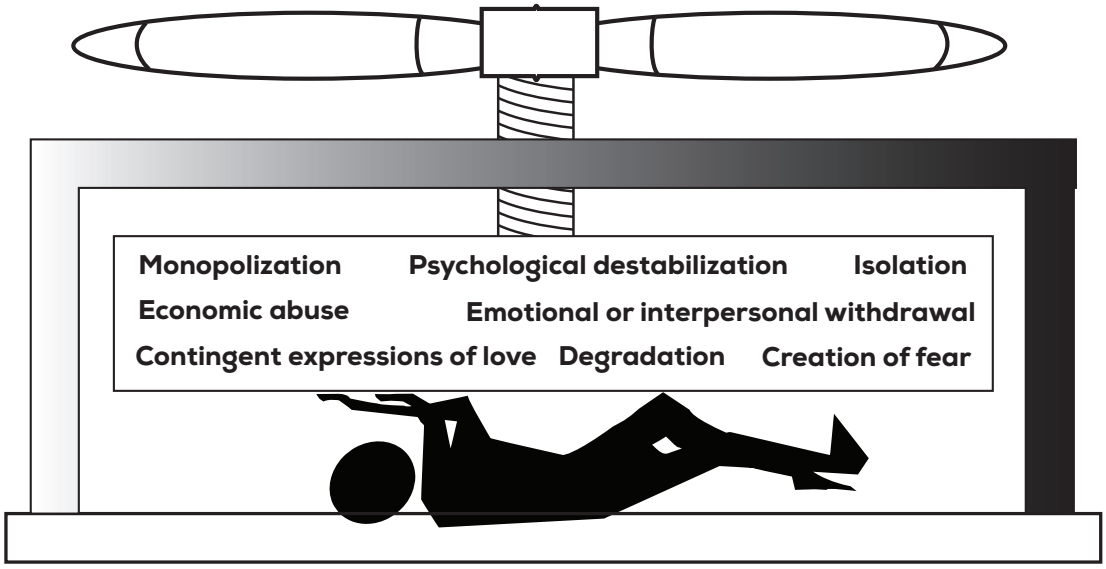
Understanding Romance Fraud: Insight From Domestic Violence Research

The use of online services to meet romantic partners has facilitated the emergence of a type of online crime referred to as Romance Fraud. Criminals develop romantic relationships with people for the purpose of extorting money from them. Research shows that Romance Fraud is widespread across the world. In 2016 alone, the Canadian Anti-Fraud Center (CAFC) received 831 reports of romance fraud cases, with a total loss of more than $20 million. The CAFC estimates that only 10 percent of actual cases are reported. Even in spite of the damage it causes, support services for romance fraud victims are rare.

Cross, Dragiewicz and Richards reviewed the limited research on romance fraud together with that on domestic violence. They aimed to highlight key aspects of psychological abuses in a domestic violence context that could help understand romance fraud. They also interviewed romance fraud victims to gain insight into the non-violent techniques used to compel the affected people to comply with demands for money. By looking at the dynamics of influence in romance fraud, Cross et al. hoped to uncover new information on non-physical abuse in a domestic violence context.

They interviewed twenty-one victims of romance fraud that were identified in a 2016 study on the experiences and support needs of online fraud victims in Australia. 80 online fraud victims had reported losses of AUD$10,000 or more to the Australian Competition and Consumer Commission's ,'Scamwatch' website in 2016. The researchers interviewed romance fraud romance fraud victims from this group. They analyzed the interviews using nine categories of psychological maltreatment.

There appeared to be a significant overlap between romance fraud and domestic violence cases. Eight of the nine psychological maltreatment categories were found in the interviews. None of the interview subjects had experienced rigid sex role expectations or trivial requests. The key difference between domestic violence and romance fraud was the absence of physical violence in the romance fraud cases. This was likely due to the fact that romance fraud offenders are usually based overseas. In the absence of physical violence, Cross et al. observed that offenders used a mix of positive and negative forms of manipulation to control the victims. Some interview subjects still reported experiencing fear of being victim of physical violence during their romance fraud relationships.



The authors noted that romance fraud victims are often perceived as being responsible for their circumstances. They suggested that clarifying the presence of psychological maltreatment in romance fraud could help victims access a genuine victim status, which is critical in obtaining services and criminal justice support.

Romance fraud has a great financial and psychological impact on victims and it deserves to be treated seriously.

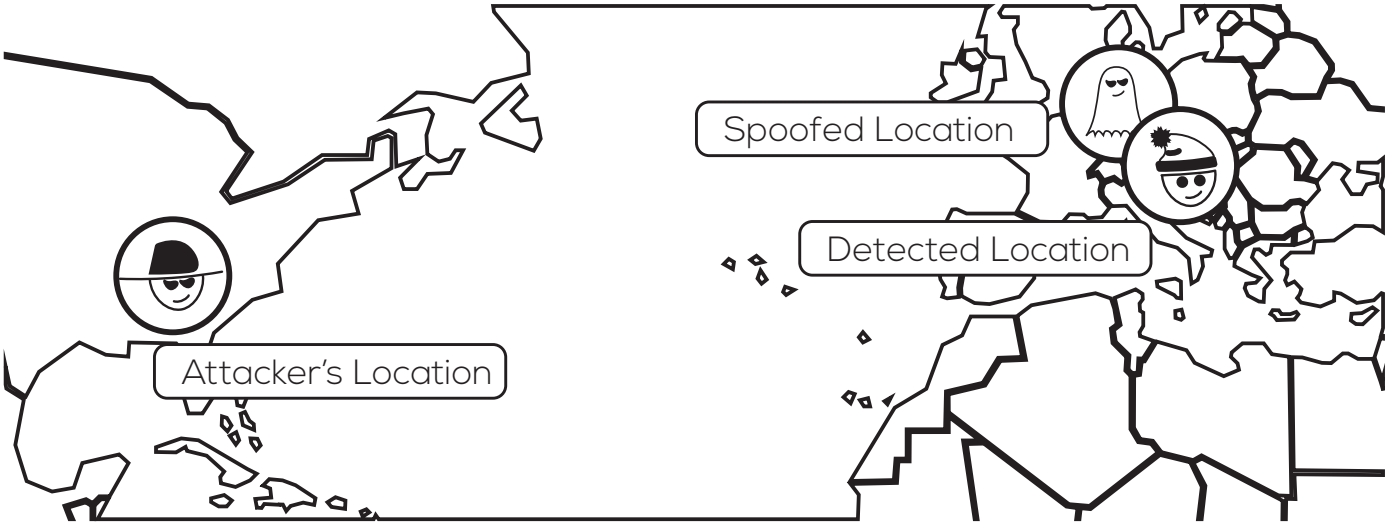
Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding Romance Fraud: Insights from Domestic Violence Research. The British Journal of Criminology.

Accurate Manipulation of Delay-based Internet Geolocation

Location-based services prevent or facilitate access or actions online, such as media streaming, online voting or gambling, fraud prevention based on the physical location of the requesting party. Delay-based techniques of location detection are gaining support as they offer increased reliability when compared to other techniques such as requesting the location from the clients (e.g. GPS) or tabulation-based IP geolocation services. However, this increased reliability may not be sufficient basis for their use in security contexts.

Abdou, Matrawy, and van Oorschot explain new attack techniques that enable adversaries to accurately manipulate the location indicated by these delay-based techniques. They devise new strategies that allow adversaries to fake their location without knowing the delay-to-distance mapping function of the delay-based location detection service.

A sender can measure the delay between itself and a receiver by having the receiver respond to special data packets and timing the responses. This is achieved by recording the time the packet was sent, either in the message itself or in the sender,Äôs memory and comparing that with the time that the packet is returned. By selectively manipulating the delay of these packets in a precise manner an adversary would be able to appear to be in a different location. The difficulty lies in modeling the expected delays to accurately match an intended location precisely enough to fool the location detection system.



The researchers presented techniques based on a variety of attacker scenarios, altering the capacity and information available to each. The novel methods developed by the researchers would be able to able to model delays with sufficient accuracy for a theoretical attacker based in continental Europe to fake a location in the United States of America.

This work makes clear the importance of security not relying on measurements that lack integrity. The measured delays used for location services are able to be manipulated. Security-sensitive applications should not rely on constrained region areas for distinguishing legitimate clients.

Location detection services are not reliable enough for security purposes.

Abdou, A., Matrawy, A., & Van Oorschot, P. C. (2017, April). Accurate manipulation of delay-based internet geolocation. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (pp. 887-898). ACM.

Cyber-victimization preventive behavior: A health belief model approach

People using the internet for their own personal reasons are largely left to fend for themselves. Although they might be aware of the risks, they don't always act consistently to protect themselves.

Dodel and Mesch examined whether knowledge from long-established work in health awareness could inform cybersecurity awareness campaigns. Health behavior models are considered some of the most developed for understanding reactions to threats both in the physical world and online. These theories argue that a small number of beliefs and attitudes are the best indicators of preventive behavior. People could be considered to be rational decision makers, who weigh the potential costs and benefits of taking precautions. However, they do so imperfectly as they may act on outdated or false information and beliefs. The Health Belief Model (HBM) considers the perceptions people have about threats and their expectations when investigating their precautionary activities. The perception of threats is a complicated set of beliefs about the likelihood and harm from an event. The perceived severity of an event is feelings created by the thought of the threat and its difficulties. Precautionary behaviours are judged based on the apparent benefits in reducing their susceptibility to the threat. Regardless of the perceived effectiveness of an action it may still seem expensive, inconvenient or unpleasant. This is also considered along with other perceived barriers such as secondary effects. The willingness to act can be influenced by the confidence or belief in one's own abilities to engage in the protective behavior. It can also by triggered by external cues such as advice or public awareness campaigns, and internal cues such as previous experience with the issue.

Data were collected as part of a larger a national sample of Israeli adults collected in October 2014, totaling 1850 completed interviews. The survey participants were asked about the actions they believed they could take to protect themselves on the internet, whether they had installed and use anti-virus software, their opinion about the risk of getting a virus and their experience with security incidents (e.g. account breach). They were also asked about their awareness of the consequences of a breach and their opinion about their ability to protect themselves.

The results of the survey indicated that peoples,Äô beliefs about digital threats are better predictors of anti-virus preventive behaviors than socio-demographic characteristics or their amount of Internet use. Peoples,Äô expectations about the outcome of a security activity and their opinion about their own ability were also linked to them taking precautions.

The results suggest that methods other than awareness messaging focusing on compliance to avoid threats could be beneficial. Fear-based messages underscore the susceptibility of people to cyber-attacks and the seriousness of the consequences, which could undermine their belief in their ability to protect themselves. Campaigns that reduce perceived barriers to digital safety-related behaviors and which strengthen beliefs in the effectiveness of anti-malware software seem to be clear and cost-efficient policy measures to increase engagement in cyber-safety.

Fear-based messages could turn people off of cyber safety behaviour. Campaigns that reduce barriers and strengthen beliefs in the effectiveness of security software could be more effective.

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. Computers in Human Behavior, 68, 359-367.

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

We are building the Canadian source for summaries of research, opinion pieces, video presentations, fraud bulletins, public awareness materials and more. You can filter the collection by type of content, click on keywords or search. The website provides lots of original conent produced by us and in collaboration with partners. To save your time, ee are sending an email regularly a summary of the new content to save you time and make it easier to find content. You can subscribe to this list online at: **http://konnect.serene-risc.ca/subscribe-abonnement/**

We will be looking for contributions to this page from our community, so if you have an idea for a piece that you would like to share please let us know.

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 at. 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 ubiased. 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, Veronique Menard

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

serene risc

Université de Montréal