serene risc Digest Volume 3, Issue 1

Cutting Edge Research Summaries for Policy-Makers and Practitioners

Where do over 65s get their cybersecurity information?

Older adults are actively targeted for online fraud and tend to lose more money to these scams than their younger counterparts. Nicholson et al. conducted 22 semi-structured interviews with digital citizens over 65, in order to explore their cybersecurity information seeking behaviors. The study identified four subthemes in relation to cybersecurity literacy: legacy knowledge retained from previous employment, low interest in IT amongst participants' social groups, communication difficulties related to cybersecurity vocabulary and the impact of past experiences on cybersecurity perception. Participants appeared to prioritize availability over competence in their choice of information sources. They usually avoided using the internet to seek security information, relying on close relatives and commercial resources instead. Findings suggest that community-organized face-to-face courses, as well as radio broadcasts, would both be great resources for older digital citizens.

Why would someone sell drugs on the darknet?

Cryptomarkets are illicit online platforms which are used to sell drugs, operating in the open thanks to encryption and anonymization technology. Martin et al. interviewed 13 cryptomarket vendors to assess their non-economic motivations. Vendors consistently pointed to the lowered risk from law enforcement as a motivation to sell online. They invested time and energy in growing a professional business identity centered around the provision of quality products and superior customer service. Cryptomarket trade appears grounded in middle-class aspirations and norms of risk aversion, instead of romanticized risk and confrontation.

Are drones susceptible to stealthy supply chain attacks?

Autonomous and Robotic Vehicles (RVs) such as flying drones and roving vehicles are increasingly being used in industrial, warehouse and even space settings. Dash et al. developed and conducted three types of stealthy attacks on RVs, exploiting a vulnerability in their navigation software. Replacing navigation software libraries with ones containing malicious code allows an attacker to inject subtle changes to the RV's interpretation of sensor input, making it deviate or crash. Those attacks are effective against common methods of detection, but could be prevented by more complex detection methods.

Can we know what the Tor network is actually used for?

Despite the common belief that anonymizing networks are used to avoid political censorship and allow freedom of speech, few works have explored how Tor is actually used in the wild. Chaabane et al. analyzed the traffic of six Tor exit nodes they created between December 2009 and January 2010 to characterize worldwide Tor usage. Results suggest that more than half of the traffic on Tor is from BitTorrent activity, related to content restricted under copyright laws. Germany and the United States represented a quarter of all Tor clients, and 70% of the observed traffic came from just ten countries. It so appears that a significant portion of Tor usage is not to overcome restrictive internet and government regulation but rather to avoid detection for content piracy and local network filtering.

What contributes to some people being scammed more online?

The number of cyber-fraud victims appears to be increasing worldwide, and many of them get scammed more than once. Whitty sent an online questionnaire to 10,723 United Kingdom residents, measuring their personality dispositions, socio-demographic profiles and online activities. The study supports the notion that age, impulsiveness, addiction and risky online behaviors are related to victimhood. Surprisingly, educated people and online users with higher self-control are more likely to be scammed, perhaps because of their overconfidence. Repeat victims were likely to have read e-safety websites, which suggests that those sites are counterproductive and should be urgently improved.

How is the advertising and tracking services ecosystem of smart TVs organized?

Despite the increasing popularity of smart TVs, their advertising and tracking services are not well understood. Varmarken et al. conducted a large-scale study of the smart TV advertising and tracking ecosystem. They monitored the network traffic from 41 homes in a major US city, collected the network traffic of 1,000 of the most popular apps on Roku and Fire TV and evaluated the effectiveness of four popular systems that block advertising and tracking traffic. Results indicate that the smart TV advertising and tracking services ecosystem is fragmented, with the exception of Alphabet Inc. which has a strong presence on both Roku and Fire TV. All four tested blocking solutions were ineffective.

What does it mean to be in a constant cyber war?

According to a policy direction detailed in the March 2018 Command Vision document, the US Cyber Command announced it would be moving operations into its adversaries' networks, following a "persistent engagement" approach. This would allow operatives to move in and out of private networks owned by corporations and individuals, crossing national borders and potentially compromising core internet infrastructure. This strategy severely downplays risks, such as the escalation of conflict. Policymakers should insist that further support for persistent engagement is subject to close review.

How effective are cloud services in spotting and blocking IP spoofing?

Cybercriminals have recently turned to public Cloud providers such as Amazon Web Services, Microsoft Azure, and Google Cloud as platforms for launching Denial of Service attacks. Vlajic et al. examined the feasibility of attacks with public Cloud services based on IP spoofing, examining the policies of 35 providers and evaluating their response with experiments. Out of the 14 evaluated providers, only three originally allowed outgoing spoofed IP packets. However, most of them accepted and responded to incoming spoofed packets, which implies that they are potentially vulnerable to spoofed-IP campaigns.

What do we really know about why employees comply with security policy?

Current literature lacks consensus regarding key drivers of security policy compliance. Cram et al. conducted an analysis of 95 research papers, to determine which factors were most strongly predictive of policy compliance. The study revealed many inconsistencies in this literature, highlighting for instance how compliance and violation are not necessarily opposites of each other and how using intended compliance as a proxy for actual compliance is unreliable. Results suggest that managers should focus on hiring employees with attitudes and beliefs consistent with organizational objectives, rather than focusing on punishment and rewards.

Could a police 'raid' stop denial of service attacks from being sold online?

Booter services provide Denial of Service (DoS) attacks as-a-service and advertise customer-facing websites where individuals can purchase attacks. Collier et al. statistically modeled and evaluated the effects of a range of police interventions on the booter services market, combining datasets of DoS attack numbers with a timeline of police interventions reported by the press. Media coverage or taking down individual booter services appeared to have no lasting effect on the overall trend of attack numbers or the structure of the market. Taking down several services at once, to the contrary, caused several booters to leave the market permanently and suppressed user demand for services over a sustained period. Results suggest that deterrence is explained by cultural factors in the booter community, which is particularly reliant on the widespread narrative that booting is not a serious crime.

"If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults

Older adults are actively targeted for online fraud, particularly for pension and romance scams. They also tend to lose more money to these scams than their younger counterparts and are often unwilling to report incidents. Unfortunately, little is known about the sources that this group trusts for cybersecurity information.

Nicholson et al. conducted 22 semi-structured interviews with digital citizens over 65, in order to explore their cybersecurity information seeking behaviors. The study consisted in the construction of a sociogram, a graphic representation of social links, and discussions about information gathering amongst and outside that social group. Starting interviews with graphically representing a support network was done to improve the accuracy of recalled interactions, as directly asking participants about experiences often leads to erroneous and incomplete recall.

The study identified four subthemes in relation to cybersecurity literacy:

1. Legacy Knowledge: Information that has been retained from previous employment.

Users adopted knowledge from their organizations security policies, such as password composition strategies. However, such knowledge may be inaccurate or out of date.

2. Interest in IT: The person and their social group's interest in learning more about Information Technology. Participants had a very limited IT literate social network, with whom cybersecurity information was unlikely to be discussed.

3. Language: The ability to understand and communicate the vocabulary of cybersecurity information. If a person is unable to formulate a recognizable query, they may not receive the appropriate help. A poor language level in participants did undermine their confidence in communicating about cybersecurity.

4. Past experience: Positive and negative experiences that shape the perception of cybersecurity. A software update slowing down a device or changing the user interface, rendering previous experience useless, dissuades older people from further updates. Conversely, good experiences can also work as gateways for more experimentation.

Social sources of assistance were predominantly close friends and family. The participants appeared to prioritize availability over competence in their choice of information sources, given their limited relevant social options and literacy. This prioritization of availability, combined with a predisposition to seek and trust advice from professionals, made them also rely heavily on commercial resources.

Participants were introduced to new cybersecurity risks when friends and family handed them internet-connected devices without appropriate accompanying support. They expressed their difficulty in finding community-organized cybersecurity courses appropriate to their literacy level and age group.

Participants also avoided using the internet to seek security information, because of their limited technology literacy and their general lack of trust for cybersecurity advice found online. Instead, they usually absorbed their cybersecurity information passively via radio and television broadcasts.

Older people are particularly vulnerable to online fraud due to a lack of access to authoritative security information, poor finances, second-hand hardware or low technology literacy. Findings suggest that community-organized face-to-face courses, as well as radio broadcasts, would both be great resources for older digital citizens.

Older people are vulnerable to online fraud due to a lack of access to authoritative security information and low technology literacy. Face-to-face courses and radio broadcasts could help.

Selling Drugs on Darkweb Cryptomarkets: Differentiated Pathways, Risks and Rewards

Cryptomarkets are illicit online platforms which are used to sell drugs, operating in the open thanks to encryption and anonymization technology such as the Tor network, Bitcoin and PGP communication. Cryptomarkets have been growing since 2011, with yearly revenues in the hundreds of millions of dollars. Relatively little is known about cryptomarket drug vendors, with most studies limited to surface-level metrics such as product availability and sales numbers. Research on the motivations of cryptomarket vendors has typically assumed economic calculations of risk and reward, while leaving out the non-economic motivations.

Martin et al. interviewed 13 cryptomarket vendors by email and instant messaging, recruited from an announcement on a news site popular to that group. An elaborated interview protocol established certainty as to the credentials of the research team, with communications secured via encryption tools such as PGP. Vendors sold a wide array of illicit drugs (cannabis, MDMA, cocaine, LSD) and predominantly operated from North America or Central and Western Europe. Two respondents disclosed a yearly income greater than 100,000 USD, two others of less than 10,000 USD, with the remainder of the group taking an amount in-between. For reasons of anonymity, basic demographic information was not sought or collected.

The study suggests that for most participants, the pathway to selling on cryptomarkets was fairly straightforward and involved a calculation of the perceived risks and financial benefits. Nearly half of the dealers had sold drugs offline before shifting to cryptomarkets, which involved additional risks from both law enforcement and bad customers who could be violent or informants. Vendors consistently pointed to the lowered risk from law enforcement as a motivation to sell online. Although cryptomarkets involve new risks, such as platform administrators suddenly leaving with deposited funds, they were considered an unavoidable cost of doing business. In addition to these economic considerations, vendors reported feelings of empowerment, freedom, transgression and emancipation.

Interviewees appreciated the relative safety and control characteristics of online selling, as compared to offline vending. They invested time and energy in growing a professional business identity centered around the provision of quality products and superior customer service. Although some participants missed the status and notoriety associated with street dealing, others reported satisfaction in being recognized among their online peers and customers. The authors observe two complementary forces promoting professionalism among cryptomarket vendors: the freedom to pursue a professional demeanor consistent with one's personal values, and a market structure that demands customer-oriented professionalism as a precondition for commercial success.

Findings indicate that cryptomarkets are different from other forms of drug selling, both in terms of market structure and participant norms, priorities and sensitivities. The immaterial benefits motivating cryptomarket drug trade differ from the seductions of crime usually associated with offline illicit activities. Cryptomarket trade appears grounded in reassuring middle-class norms of risk aversion and conflict avoidance, instead of romanticized risk and confrontation. The lifestyle and materialism to which some participants aspired (a comfortable house, graduate education) also correspond to middle class norms. Findings suggest that these soft seductions attract and motivate people, many of whom would not otherwise sell drugs on cryptomarkets.

Beyond economic concerns, lower risk, professional work practices and a middle class lifestyle were also motivators for cryptomarket drug vendors.

Martin, J., Munksgaard, R., Coomber, R., Demant, J., & Barratt, M. J. (2020). Selling drugs on darkweb cryptomarkets: differentiated pathways, risks and rewards. The British Journal of Criminology, 60(3), 559-578.

Out of Control: Stealthy Attacks Against Robotic Vehicles

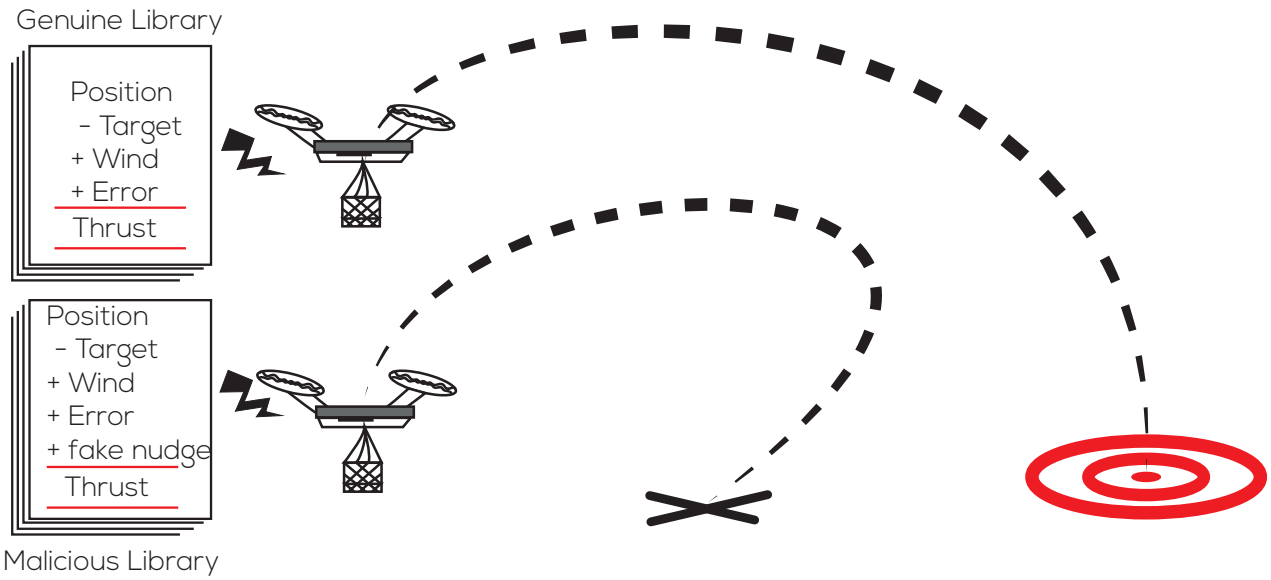
Autonomous and Robotic Vehicles (RVs) such as flying drones and roving vehicles are increasingly being used in industrial, warehouse and even space settings. Unfortunately, these vehicles are subject to both physical and cyber-attacks, even when they should be protected by path-monitoring systems.

Dash et al. developed and conducted three types of stealthy attacks on RVs. They assessed the effort required, the impacts on the subject RVs as well as the efficiency of the attacks. The attackers were assumed to be unaware the specifics of the RV, unable to delete system logs, unable to tamper with the device's firmware or to gain administrator (root) access. They would however be able to compromise the RVs, snoop on control inputs and outputs and replace the libraries used in the RV software.

RVs generally draw from two common libraries of code for their control: sensor and inertial measurement functions. Replacing these libraries with ones containing malicious code allows an attacker to inject subtle changes to the RV's interpretation of sensor input. The researchers identified three methods for attacking an RV: False Data Injection, Artificial Delay and Switch mode attacks. False Data injection alters the measurements from the robot,Äôs sensors to provide an altered image of the actual position of the RV. The Timing Delay attack performs resource-intensive operations, slowing time-critical functions and altering the timing behavior of the system. Switch Mode attacks perform a false data injection when the RV is switching between operation modes, such as from general flying mode to landing mode.

These attacks were stealthy and effective, allowing an attacker to push a drone off-course by 8 to 15 meters over a distance of 35~50 meters and to increase flight time by 30% to 50%. The switch mode attacks appeared to be particularly effective, preventing the drone from landing or causing it to crash. Results suggest that the preparation stage for such attacks could be automated, allowing self-learning malware to be developed.

The research presents the possibility of stealthy attacks against RVs that are effective against common methods of detection. The use of more complex detection methods, such as detection with variable detection windows, could increase the security of RVs.



Robotic Vehicles could be effectively attacked in a manner that is undetectable by inserting malicious code into software libraries.

Dash, P., Karimibiuki, M., & Pattabiraman, K. (2019, December). Out of control: stealthy attacks against robotic vehicles protected by control-based techniques. In Proceedings of the 35th Annual Computer Security Applications Conference (pp. 660~672).

Digging Into Anonymous Traffic: A Deep Analysis Of The Tor Anonymizing Network

Anonymizing networks such as Tor arouse increasing interest in users careful about their anonymity and privacy. Despite a common belief in the research community that anonymizing networks are used to avoid political censorship and allow freedom of speech, few works have explored how Tor is actually used in the wild.

Chaabane et al. analyzed Tor traffic to characterize its actual use and identify potentially undesirable behaviors which could affect the network's operations. Tor clients typically build a communications circuit with 3 computers in the network. Messages are wrapped in successive layers of encryption (like a locked box in a locked box in a...). Each computer is provided with a decryption key so that the message can be unwrapped when it progresses through the circuit in the correct order. The last computer (the exit node) unwraps the message and sends it on to its destination. Each computer passing the message only knows about the computer it received it from. Only the final computer can decrypt the original message, without any information as to its origins.

The researchers created six Tor exit nodes distributed around the world and monitored their use on two separate occasions between December 2009 and January 2010, for a total of 23 days. They used Deep Packet Inspection to analyze both the metadata and the content of messages, to identify the services being used on the network. The researchers were careful to conceal or minimize their use of this technique to the minimum required in order to preserve user privacy as much as possible.

The results showed a significant amount of unknown traffic, that further analysis determined to likely be concealed BitTorrent data. This information, combined with the identifiable BitTorrent traffic already detected on the network, suggests that more than half of the traffic on Tor is from BitTorrent activity. Analysis of what is downloaded through Tor indicates that most of that content is restricted under copyright laws.

Other uses of Tor include web browsing, which appeared to be used much like the open internet, despite the slower performance caused by the anonymization process. As expected, search engine services are the most visited pages, followed by pornography in second. Social network websites are the fourth most visited. The small number of Tor users in politically sensitive countries suggests that this traffic represents American and European employees circumventing restrictions on their work computers rather than political dissidents organizing protest actions. Germany and the United States represented a quarter of all Tor clients, with Russia and China in fifth and sixth place. Although 100 countries appeared to use the Tor network in the one-day period for which data was collected, 70% of that traffic came from just ten countries.

The researchers also detected several systems using the Tor network in a manner that it was not designed for, passing messages through one computer rather than a circuit of three or more. While this reduces the anonymizing power of Tor, it also increases the speed of connections while providing an encrypted tunnel to an exit node. This could be a way for users to overcome connection filtering, such as it is employed within companies. It so appears that a significant portion of Tor usage is not to overcome restrictive internet and government regulation but rather to avoid detection for content piracy and local network filtering.

More than half of the traffic on Tor is likely BitTorrent or illegal content downloads.

Chaabane, A., Manils, P., & Kaafar, M. A. (2010, September). Digging into anonymous traffic: A deep analysis of the tor anonymizing network. In 2010 Fourth International Conference on Network and System Security (pp. 167-174). IEEE.

Predicting Susceptibility to Cyber-Fraud Victimhood

Cyber-fraudsters exploit mass communication technologies like email, instant messaging and social networking sites to trick people out of their money. The number of cyber-fraud victims appears to be increasing worldwide. More concerning is the fact that many of the victims get scammed more than once. Understanding why people are scammed online is critical, given that they often suffer both financial and psychological harm.

Whitty conducted a survey to examine the predictors of cyber-fraud victimhood, leveraging both psychological and criminological theories. An online questionnaire was sent to 10,723 United Kingdom residents, recruited from a paid panel. It measured the personality dispositions, socio-demographic profiles and online activities of the participants. More specifically, the survey measured impulsivity, locus of control, addiction, education, online activity frequency and self-protective or guardianship behaviors.

The study concluded that a predictive model for cyber-fraud victimhood needs to include socio-demographic characteristics, personality traits and online routine behaviors. It supported the notion that age, impulsiveness, addiction and risky online behaviors are related to victimhood. Most importantly, results considering education, self-control and guardianship were also linked, but not in the way that might be expected. Educated people were more likely to be scammed, perhaps because of their particular online activities. Further, they might be more likely to think that they can spot a scam and consequently spend less effort actively monitoring for them.

Online users with higher self-control and confidence were also more likely to be scammed, presumably because they failed to recognize the control others might have over them. Alarmingly, the only variable related to being scammed more than once was a likelihood to read e-safety websites, which actually increased among repeat victims. This suggests that at least some of those educational websites are not only ineffective, but they are counterproductive to security.

All participants had been exposed to a cyber-fraud at some point in their lives, with 7 per cent having lost money in the process. The results indicate the importance of combining research approaches as socio-demographic, personality and routine activities were all risk factors for fraud. The findings also suggest that cyber security education must be urgently improved. As impulsive users are at risk, the awareness information may need to be concise, easily accessible, engaging and actionable. Priming and warnings are not enough: users need practical advice on what to do to protect themselves.

Cyber fraud awareness isn't allways helpful. Bad advice can increase the risk of becoming a victim. Educational websites urgently need to be improved.

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. Journal of Financial Crime.

The TV is Smart and Full of Trackers: Towards Understanding the Smart TV Advertising and Tracking Ecosystem

Smart TV adoption has grown steadily over the last few years, with more than a third of US households owning at least one as of 2018. Most applications on smart TVs are supported by advertising. Despite the increasing popularity of smart TVs, their advertising and tracking services are not well understood by users, researchers or regulators.

Varmarken et al. conducted a large-scale study of the smart TV advertising and tracking ecosystem. They monitored the network traffic from 41 homes in a major US city, collecting the data generated by 57 smart TVs over 3 weeks. They then experimented with the 'Roku' and 'Amazon Fire' TV platforms to obtain more granular information as to which specific apps were generating the traffic. Using an automated testing system simulating user interaction, they collected the network traffic of approximately 1,000 of the most popular apps on each platform. The authors also evaluated the effectiveness of four popular systems that block advertising and tracking traffic from home devices, which are based on DNS blacklists.

Results indicate that smart TVs generate a substantial amount of advertising and tracking traffic. The Roku and Fire TV ecosystems differ substantially. For example, SpotX is a relatively large player on Roku, but is almost absent from Fire TV. In contrast, Facebook has almost zero presence on Roku, but has a reasonable foothold on Fire TV. The exception is Alphabet Inc., which has a strong presence on both platforms. Even apps present on both platforms show little overlap in where they are sending their data to, which further highlights the distinct nature of the advertising and tracking services between these platforms. All four tested blocking solutions were ineffective in filtering advertising and tracking traffic. The authors suggest a few ways in which they could be improved. For instance, they observed that the more apps contact a single destination, the more likely it is for that destination to be an advertising or tracking service. They also note that some obvious domains containing keywords such as ,'ads' and 'tracking' were not blocked by any of the solutions.

The smart TV advertising and tracking services ecosystem appears to be fragmented. It is also different from the mobile ecosystem, which is better understood. More could be done to increase the effectiveness of blocking tools. The authors have made their datasets publicly available, and plan to also share their analysis tools.

The smart TV advertising and tracking services ecosystem appears to be fragmented. Blocking solutions are ineffective.

Varmarken, J., Le, H., Shuba, A., Shafiq, Z., & Markopoulou, A. (2019). The TV is Smart and Full of Trackers: Towards Understanding the Smart TV Advertising and Tracking Ecosystem. arXiv preprint arXiv:1911.03447.

The Implications of Persistent (and Permanent) Engagement in Cyberspace

The United States has seen a significant policy shift on cyber conflict, with profound implications for national security and the future of the Internet. According to a policy direction detailed in the March 2018 'Command Vision' document, the US Cyber Command substantially increased both the scope and intensity of its offensive operations. In response to ongoing cyber attacks, the Cyber Command announced it would be taking the fight to the enemy and moving operations into its adversaries' networks. Persistent engagement, or being constantly present within the IT infrastructure of their adversaries, will purportedly allow US forces to better intercept and halt cyber threats, as well as deter future attacks. This shift marks the end of restrictions imposed on offensive cyber operations during the Obama administration, and represents perhaps the single most important articulation of cyber policy in two decades.

Concretely, the US Cyber Command wants its operatives present within its adversaries' systems to follow them as they access foreign systems. This would allow operatives to kick adversaries out of compromised machines or even take control of their malware. Increased agility in this context means maneuvering in and out of private networks owned by corporations and individuals, crossing national borders. Reducing the operational constraints on US Cyber Command could mean compromising core Internet infrastructure, as we use the same technologies as America's adversaries in our private and professional lives. Pursuing adversaries into American and European infrastructure may also further erode the trust of US corporations and allies, a trust already impacted by the 2013 Snowden revelations.

The Cyber Command strategy, although coherent and compelling, severely downplays potential risks. One major concern is that the new policy invariably advocates for the intensification of US operations, regardless of the strategies chosen by its adversaries. Neither 'escalate' nor 'escalation' appear in the Command Vision document, a major omission which suggests its authors did not consider the full dynamics of conflict. Increased US cyber operations might exacerbate conflict instead of deterring attacks, as adversaries rise to the challenge of those actions rather than backing away. As cyberspace becomes increasingly important for more nations, it elevates the stakes and the risks along with them. Furthermore, persistent engagement as a strategy lacks any practical means of communication to de-escalate cyber tensions, for instance to convince other nations that an intelligence operation is meant for conflict stabilization rather than warfighting.

The imperatives of the Command Vision could be right or wrong; the risks discussed here may or may not turn out to be major concerns. Regardless of the outcome, policymakers should insist that further support for persistent engagement is dependent on four conditions:

(1) A clear timeline and criteria for success: how will we know progress when we see it?

(2) Criteria for failure: what are the indicators of failure?

(3) Political throttle: cyber operations should develop in agreement with current diplomatic activities.

(4) A set expiration date: authorizations allowing more operational agility should expire and their renewal be subject to review.

The "persistent engagement" policy of the US Cyber Command could compromise core internet infrastructure and escalate tensions if not closely monitored.

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. Journal of Cybersecurity, 5(1), tyz008.

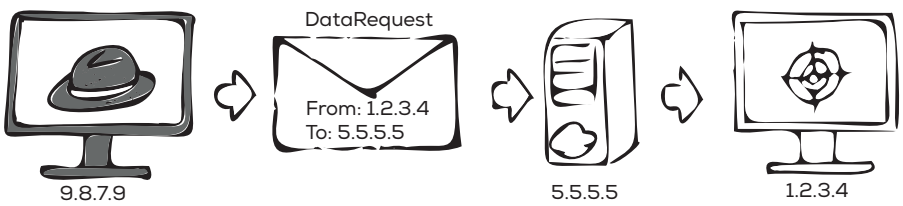
IP Spoofing In and Out of the Public Cloud: From Policy to Practice

Cybercriminals have recently turned to public Cloud providers such as Amazon Web Services, Microsoft Azure, and Google Cloud as platforms for launching Denial of Service attacks. They provide flexible, on-demand capacity and offer bandwidth which can be as much as 1,000 times higher than is possible with compromised home routers or IoT cameras. Internet Protocol (IP) spoofing, that is forging the source address of Internet data packets, is instrumental in many illegitimate online activities. For instance, criminals can initiate distributed denial of service (DDoS) attacks by sending request data packets to amplification servers, with the spoofed address of the victim as the return address. Cloud providers have thus recently implemented anti-spoofing filtering to prevent data packets with an incorrect address from entering and leaving their network.

Vlajic et al. examined the feasibility of attacks with public Cloud services from an offender's perspective, based on real-world experimentation. The research is organized around three questions: 1) How is IP spoofing addressed in the acceptable-use and terms-of-service policies of Cloud service providers? 2) How effective are they in spotting and blocking outgoing spoofed IP packets generated by malicious customers? 3) How effective are they in spotting and blocking spoofed IP packets sent to their servers?

The authors examined the policies of 35 public Cloud service providers, including top players in the field (Amazon, Microsoft and Google) as well as a number of lesser-known companies. They experimented on 14 of those 35 providers, rejecting those which explicitly prohibited IP spoofing, or which required expensive or long-term subscriptions. The experiments evaluated the ability of providers not only to deal with spoofed IP packets, but also to spot and filter out invalid packets and addresses (for instance, private addresses and specific transmissions from Google,'s 8.8.8.8 server). The authors limited their tests to single packet probes, as they did not want to engage in any actual attack-like activity. Although larger volumes of spoofed data packets (as would be more realistic for a DDoS) might have produced different outcomes, the authors argue that there is no reasonable justification to allow any spoofed data packets from certain categories.

Out of the 35 surveyed Cloud providers, 19 (including Google Cloud and Microsoft Azure) make no direct reference to IP spoofing in their policies. Out of the 14 evaluated providers, only three originally allowed the transmission of spoofed IP packets. More concerning are the results of the second experiment, which show that most providers not only accept, but also automatically respond to spoofed IP packets. This implies that even if most Cloud providers successfully prevent potential hackers from using their services to launch spoofed-IP campaigns, they themselves are usually vulnerable to those campaigns, or could be used to reflect attacks on potential targets.



Most public Cloud providers block outgoing spoofed IP packets, but do not block incoming spoofed packets. This makes them potential attack targets.

Vlajic, N., Chowdhury, M., & Litoiu, M. (2019). IP Spoofing In and Out of the Public Cloud: From Policy to Practice. Computers, 8(4), 81.

Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance

Information security policies are formalized employee guidelines for the use of IT. Organizations rely on these policies as employees account for a large percentage of security incidents. Current literature lacks consensus regarding key drivers of policy compliance and is uncertain as to how they perform under different conditions. This study aims to holistically investigate the findings of prior research in order to clarify what is important for security policy compliance.

Cram et al. conducted an analysis of 95 research papers, classifying them into 17 distinct categories. They then determined which of the categories were most strongly predictive of security policy compliance. Conference papers, dissertations and unpublished papers were all included in the studies collection. Four factors explaining inconsistencies within the literature were identified:

1) studies measuring compliance vs others measuring policy violation, which are not necessarily opposites

2) studies measuring actual compliance vs others measuring intended compliance

3) studies concerned with general security policies vs others concerned with specific policies (e.g. anti-virus software and data backups)

4) the location and national culture of the participants

Three of the top five strongest categories in explaining policy compliance are all oriented around employee values: attitude, personal norms and ethics, normative beliefs. In comparison, the categories that are generally seen as being more easily manipulated by management, such as punishment and rewards, are among the weakest in predicting security policy compliance. Activities related to perceptions of security policy usefulness and training present a mid-range importance in predicting policy compliance. The analysis of factors of inconsistency in current literature revealed that:

- Policy compliance and violation should not be considered opposite views of the same construct.
- Past work suggesting the use of intended compliance as a proxy for actual compliance is not uniformly reliable.
- Employees interpret the narrow scope of specific policies to correspond to diminished sanctions, in comparison to more severe punishments for general policies.
- Cultural factors can influence compliance. There are significant differences between the Asia-Pacific, Europe and North America regions.

This study presents practical insights for the management of security policy. For instance, managers may benefit in hiring employees with attitudes and beliefs consistent with organizational objectives, rather than focusing on punishment and rewards. Convincing employees of the value of policies is especially important, for example by sharing anecdotal evidence of how they have mitigated security incidents in the past. Managers can also assign a security champion to each project team to provide accessible training and increase team security effectiveness.

Security policy compliance is motivated more by employee values than punishement and rewards.

Cram, W. A., D'arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. MIS Quarterly, 43(2), 525-554.

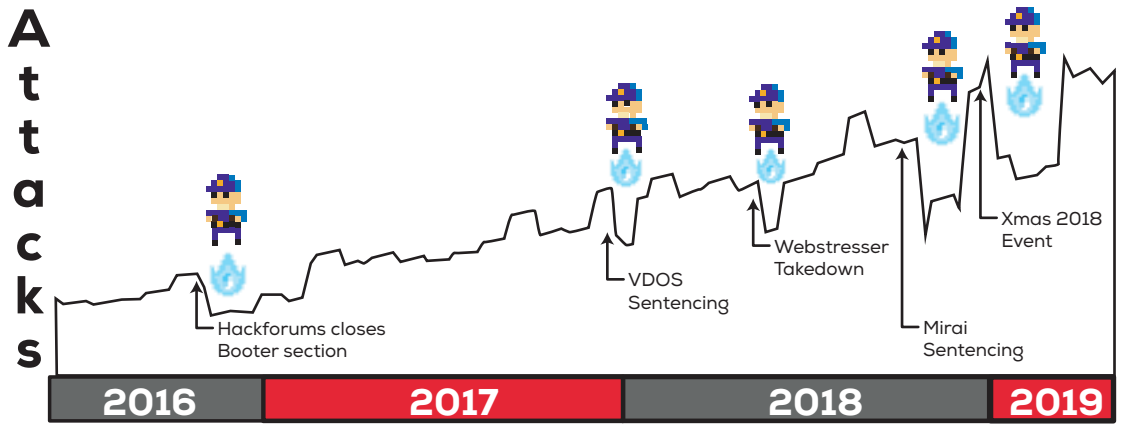
Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks

Booter services provide Denial of Service (DoS) attacks as-a-service. They generate large amounts of traffic which overwhelm end users or web services, taking them offline or making legitimate access impossible. Booter operators advertise customer-facing websites where individuals can purchase attacks, generally targeting gaming related websites and their users.

Collier et al. statistically modeled and evaluated the effects of a range of police interventions on the booter services market. They used a dataset of victims of DoS amplification attacks, a technique widely used by booter services, covering a five-year period from 2014. They added a second dataset of self-reported DoS attack numbers collected from the booter websites themselves since November 2017. Combining the data with a timeline of police interventions reported by the press for the same time period, they established a statistical model to assess their impact on booter services.

Media coverage of the prosecution or sentencing of booter providers appeared to have no consistent effect on the number of attacks. Taking down individual booter services led to short-term drops in attacks, with no lasting effect. Taking down several services at once, to the contrary, caused several booters to leave the market permanently and suppressed user demand for services over a sustained period. The online advertising campaign of the United Kingdom National Crime Agency, warning Google users of the illegality of DoS attacks when they searched for booter-related terms, also appeared to be effective. As the number of attacks grew in other nations, numbers flattened in the UK for a period of eight months, starting with the campaign. This suggests that the rise in attacks comes from new users rather than extra activity by existing users, at least in the UK.

The booter community does not display the deterrent effect typical to offline illicit activities, where interventions affect the risk calculus of actors involved in crime. This study suggests that deterrence is explained by cultural factors in the booter community, which is particularly reliant on the widespread narrative that booting is not a serious crime. Advertising campaigns such as the National Crime Agency's could thus be a key part of a strategy against booting. Arrests have a limited and short-lived effect on attack numbers. It is an open question as to whether they are essential to reinforce the impact of a takedown, aside from preventing a booter operator from starting again immediately. Wide-ranging website takedowns appear to have a structural effect on the market, concentrating booter services and making them potentially more susceptible to further intervention.



Taking down several booter services at once and sensitization campaigns are more effective interventions against booter service operators.

Collier, B., Thomas, D. R., Clayton, R., & Hutchings, A. (2019, October). Booting the booters: evaluating the effects of police interventions in the market for denial-of-service attacks. In Proceedings of the Internet Measurement Conference (pp. 50-64).

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: Louis Melançon

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

serene risc

Université de Montréal