serene risc Digest Autumn 2016

Cutting Edge Research Summaries for Policy-Makers and Practitioners

Does the Internet radicalize extremists and what can we do about it ?

The Internet can play a role in radicalization but it is normally only part of the process. Counter-messaging and education are promising avenues for reducing negative impact from the Internet.

page 5

How can you know if a security tool works?

Unfortunately, there is no way to reliably prove claims about security.

page 6

How hidden are child exploitation imagery websites?

They are not very hidden. There are plenty in plain sight on the Internet.

page 7

When we tell children to be safe online, are they thinking what we are thinking?

Probably not. Children appear to understand the risks that they can perceive so they are more worried about friends and family than the risks that parents are trying to protect them from.

page 8

What does the economy of a country tell us about its problems with malware?

Not a great deal.

Education and infrastructure are better tools to understand the rate of malware infection in a country .

page 9

Are we thinking about security the right way or are we just building castles in the sky?

In practice, cybersecurity doesn't conform to a model based in castles, fortifications and walls.

page 10

Could security tokens replace text-based passwords?

Possibly, but user expectations and concerns must be addressed.

page 11

Is it possible to make messages more [redacted] without encryption?

Introducing vagueness with algorithms can increase privacy by reducing the amount of explicit information in communications.

page 12

Can Bitcoin's blockchain technology help us manage personal information ?

The Blockchain technology offers the possibility of transparent, decentralised and private management of personal information.

page 13

Is it possible to automatically detect security policy issues in Android?

There exists an automated approach that flags all potential problems for closer inspection.

page 14

Does the Internet radicalize extremists and what can we do about it ?

The Internet is increasingly implicated in the radicalization of extremists to the point of violent action. Ducol et al. assessed the current understanding of the role of the Internet in violent extremism. The Internet should not be perceived as a singular pathway or driver to radicalization. It is only one part of a complex multidimensional process. The Internet could play a role in the initial exposure, reinforce offline radicalization, and assist in re-structuring personal networks. There are two major incentives that may explain why some choose to intensify their exposure to online radicalizing environments. The effectiveness of countering violent extremism through censorship is poorly understood and difficult to implement. Countering extremist messages is another approach but it is also difficult to implement effectively due to a lack of solid evidence on how it actually works. The Internet can play an important role in providing cognitive resources and alternative sources of information. This would be perhaps most effective when combined with school programs on digital literacy and critical thinking.

How can you prove a security tool to be ineffective?

Declaring anything to be "secure" is a risky proposition. Something can be shown to be insecure but not the opposite. As Herley explains, it is impossible to prove if a defensive measure is secure for a number of reasons. As we cannot be certain that the future does not bring a new type of attack we cannot be sure that our defenses are sufficient. This renders any claims about the requirements for security untestable. We can define security so that certain things are necessary, but this does not allow us to conclude anything about outcomes. Despite this, we must take some steps towards being more secure. Since there is no mechanism for rejecting measures, they accumulate over time and waste becomes inevitable. Implementing anything short of all of them must be done in an unsystematic way. So we are left with an ever increasing list of security measures, none of which are proven to be any more effective than any of the others.

How hidden are child exploitation imagery websites?

Child Exploitation (CE) imagery continues to be distributed publicly on the Internet. Westlake, Bouchard and Girodat studied how websites providing CE material operate online. The overall purpose of this study was to determine how obvious it was that a website was explicitly CE-focused. They found that many of the explicitly CE-focused websites identified manually were also identified automatically, suggesting that CE-related websites do little to hide their purpose. Despite this, they were no more likely to be taken down than other websites. For autonomous data collection tools to be effective in detecting CE websites, they need to be provided with proper guidance Child exploitation is no longer a hidden realm only accessed by sophisticated, technological masters. This highlights the jurisdictional, privacy, and identification issues for law enforcement.

When we tell children to be safe online, are they thinking what we are thinking?

The rise in youth mobile media use has heightened parental concerns about the safety of children online. Zhang-Kennedy, Mekhail, Abdelaziz and Chiasson conducted semi-structured interviews with parents and their children. The researchers interviewed 14 families of children aged seven to eleven. The researchers found that the children's understanding of external threats was very basic and reflected their experiences with offline safety. They see their greatest security threats as coming from family members. Parents perceived risks differently than children. Parents felt the need to safeguard children by limiting what they could access and who they could talk to online. It is important to take into consideration the differences in the perceived threats of children and parents when addressing security.

What does the economy of a country tell us about its problems with malware?

A computer's vulnerability to malware infections is affected by technological and human factors. Lévesque et al. assessed the risk factors related to malware infections in multiple countries. They determined country infection rates using data from millions of systems running a malware cleaner tool that scans Windows systems for infections. There are better indicators of malware infection rates than economic activity. Education, technological infrastructure and cybersecurity investment seem to have a more consistent impact on malware infection rates. Investment in economic development may not directly impact malware infection rates. It appears that investment in education along with information and communication technology infrastructure may be more effective.

Could security tokens replace text-based passwords?

Text-based passwords are the most common form of authentication. However, they are generally considered to be impractical. Payne et. al investigated factors determining user acceptance and expectations of a token-based authentication scheme that utilizes multiple wearable devices. Issues for the participants included the convenience, design and trustworthiness of the tokens. Participants were concerned about trusting the tokens. In order to make the great changes required to transition to next generation passwords, it is important to consider users' expectations and concerns.

Are we thinking about security the right way or are we just building castles in the sky?

The Castle Model is a cybersecurity metaphor that draws from the idea of a traditional castle. Leuprecht, Skillicorn and Tait argue that the Castle Model is outmoded. The authors feel that there is a need for a more balanced understanding of cybersecurity. Organizations deliberately tear down their own walls and expose themselves to vulnerabilities. Technological developments are getting better at destroying walls and we are beginning to interact with technology in a way that dissolves barriers. A paradigm shift towards thinking of "computing in compromised environments" could be key. Future development should continue looking beyond a singular cybersecurity defence model and consider the use of dynamic and varied responses.

Is it possible to make messages more [redacted] without encryption?

It has become increasingly important for Internet users to know how their information is being used. Gilbert created a method intended for the average user that employs a 'hidden-in-plain-sight' approach to dealing with prying eyes. Messages are transformed by analyzing the text and replacing keywords with words that are generally unidentifiable by unintended recipients, while still seeming like a normal message. The method aims to limit the amount of information that is available to eavesdroppers while keeping text understandable by intended recipients. The algorithm can play a vital role in extending the concept of privacy towards the average user.

Can Bitcoin's blockchain technology help us manage personal information ?

Recent increases in security breaches of private data have led to a growing concern about how companies store private information. Bitcoin could provide an answer. Zyskind et al. applied blockchain technology, combined with off-blockchain storage, to create a more secure and transparent mechanism for storing private information. Using a blockchain allows the user to retain ownership over their data and provides a very resilient data storage solution. If implemented widely, this technology could allow companies to increase security without compromising their data needs.

Is it possible to automatically detect security policy issues in Android?

Certain smartphone resources, like the camera or text messaging service, are sensitive and need to be protected. The Android operating system uses permission-based security. Apps must ask the system in order to use certain resources. Android grants access to these apps on a case-by-case basis, but sometimes permission checks can be wrong or missing. Shao et al. created an automated technique that finds security issues with policy enforcement in large programs like Android. In their tests, they found 14 cases of inconsistent security policy enforcement in 6 different versions of Android. They also give explanations and solutions for the detected security flaws. This technique can be used to double-check security policies to make sure a system is secure and could be beneficial to organizations using large programs.

Assessment of the state of knowledge: Connections between research on the social psychology of the Internet and violent extremism

The Internet is increasingly implicated in the radicalization of extremists to the point of violent action. Radicalization might be understood as the mental component of the process whereby radical ideas develop to the extreme of a willingness to directly support or engage in violent acts. Despite the implication, there appears to be a gap in our understanding of how this happens and how to resolve this as a problem. Ducol et al. assessed the current understanding of the role of the Internet in violent extremism. They analysed existing research and used their findings to inform a study of fifteen cases of radicalization where the Internet is assumed to have played a role. They then discuss possible options for dealing with radicalization.

The Internet should not be perceived as a singular pathway or driver to radicalization. It is only one part of a complex multidimensional process any part of which alone may not lead directly to the adoption of violent extremist beliefs. It could play a role in the initial exposure to radical ideas, beliefs and universes of socialization that legitimize the moral conviction to carry out violent actions. The Internet could reinforce offline radicalization processes by providing additional resources. It could also play a role in re-structuring personal networks, with individuals spending more time online filtering moderate influences from their social circle. More important elements in radicalization are social bonds and personal networks, the development of which can be facilitated by the Internet.

There are two major incentives that may explain why some choose to intensify their exposure to online radicalizing environments. First, they are able to find appealing answers to existential questions online from an increasing number of more credible sources. Second, they are able to find like-minded individuals who support their views. In this circumstance, the Internet becomes an echo chamber for intellectual and cognitive fantasies, reinforcing polarized worldviews. This allows individuals to cognitively self-intoxicate on perceived threats to their group and the urgent need to take violent action. Finally, the Internet may provide inspirational and operational knowledge to actualise violent action.

Countering violent extremism (CVE) in the Canadian context includes the recently proposed 2015 Anti-Terrorism Act which includes provisions intended to “remove terrorist propaganda from the Internet.” However, the potential effectiveness of such measures is questionable. There is simply too much content on the Internet to feasibly analyse and censor. Even if it were possible, there are issues surrounding what properly constitutes “extremist content” as only a tiny fraction of what is considered extremist content is actually illegal.Attention has increasingly turned to counter-messaging as a central response to violent extremism. Counter-messaging is a proactive approach that focuses on reducing the demand for extremist content by offering credible alternatives to undermine its appeal. Counter-messaging may be realized through counter-narratives. Counter-narratives represent attempts to directly or indirectly challenge violent extremist messages challenging assumptions, exposing fallacies, and dismantling conspiracy theories. The idea behind counter-narratives is relatively straightforward, but their practice is much more complicated.

The CVE programs reviewed generally lacked the means by which to distinguish the role of the Internet in the radicalization process for the violent extremists they targeted. Understanding the radicalization process is greatly complicated by a lack of consensus on the causes of radicalization. In the absence of solid evidence, we are left with only pet theories and speculation to develop strategies. There appears to be a substantial gap between what is known about the factors that are may animate the radicalization process and the factors that CVE interventions attempt to address. Much more research is needed on CVE programs to understand their impact. CVE programs should be firmly grounded in the “causes” of radicalization to violent extremism.

An overemphasis on Muslim radicalization has also been noted by CVE critics. Singling out Muslims in an effort to make them feel less alienated is counterproductive. Further, if individuals are not motivated by ideology but by needs rooted in identity, belonging, recognition and respect, then challenging their beliefs would be ineffective in diverting them from a path to violence.The findings from the case study analysis also emphasized the role of the Internet in serving as a cognitive resource to learn about religion. The Internet may also serve as a tool to prevent these processes by providing alternative resources. This would likely be best accompanied with school programs that address digital literacy and foster critical thinking regarding ideological content.

The Internet is only part of the problem of extremist radicalization so it can only be part of the solution. Censorship is difficult to implement effectively but counter-messaging could help.

Ducol, B., Bouchard, M., Davies, G., Ouellet, M. & Neudecker, C. (2016) “Assessment of the state of knowledge: Connections between research on the social psychology of the Internet and violent extremism.” Canadian Network for Research on Terrorism, Security and Society Working Paper Series.

Unfalsifiability of security claims

Declaring anything to be ‘secure’ is a risky proposition. Something can be shown to be insecure but not the opposite. Hence, claims of security are impossible to prove wrong empirically. This results in situations where nothing is secure, no countermeasure is unnecessary, and we are left to unsystematically accumulate defenses in an impossible struggle. It’s unsurprising that some simply give up on security.

As Herley explains, it is impossible to prove if a defensive measure is secure for a number of reasons. The future is not certain, not all attacks have been attempted against all systems, and not all attacks that will exist have been invented. Consequently, no amount of use without something bad happening rules out the possibility that a bad outcome has simply not happened yet. Because of this possibility, we are unable to test any security measure, as we are unable to observe that it will always be effective in all possibilities. Any condition claimed as being necessary for security is as such untestable, making it impossible to prove as it being otherwise. In order to make assertions in the face of uncertainty, we can make claims based on assumptions. For example, we might say that random passwords of length of more than 40 characters are secure against guessing. This is not an observation, but a deduction based on an assumption about attacker limitations. However, deductive claims are limited to their premises and cannot be generalized. In this case, a 40 character password is only secure against guessing if and while our assumption about the attacker’s limitations are true. As we cannot say with certainty whether the assumption is true or not, we cannot validate or falsify if the measure is needed. Further, the claim only refers to security only in as much as password guessability relates to security outcomes and not more generally.

We can define security so that certain things are necessary, but this does not allow us to conclude anything about outcomes. Reality may not coincide with our assumptions about what will occur. For example, if we define a password of greater than six characters as necessary for security, we are forced to assume that an attacker can and will attempt to guess all such passwords. If no attempt is made to guess all possible passwords, a five-character password may be as secure; however, it is impossible to be sure. This results in conditional security claims. If either the claim or the condition is vague, such as ‘given a sufficiently motivated attacker’ then we can never convincingly refute the claim. The inability to test claims means there is no way to discover if they are wrong.

Speaking of necessary conditions implies a binary security view: things are either secure or not. A necessary condition is a universal generalization about the things that are. There are many cases where the ineffectiveness of a security measure may not impact the actual experience of security. The ineffectiveness of any part of a defence-in-depth measure is irrelevant unless the main defence fails. A vulnerability might not be exploited if it is undiscovered or relatively expensive as attackers can adapt. If the rate of occurrence of an attack is sufficiently low, the effective outcome of not defending against it may be difficult to observe.

Despite this, we must take some steps towards being more secure. One approach is to start with a set of security goals that are to be met in order to be sufficiently protected from bad outcomes. The goals might be arrived at based on assumed or observed attacker capabilities, or a threat modelling exercise. That the goals are sufficient to avoid bad outcomes, can be falsified by finding an outcome not considered when devising the goals. This happens when an attacker ‘steps outside’ the model and uses an attack that hasn’t been considered, or wasn’t previously known. Thus, in this approach, the claim that those goals are sufficient can be falsified, but the claim that they are necessary cannot. The general response to this problem is an ever expanding set of goals and an unending search for attack opportunities.

Since there is no mechanism for rejecting measures, they accumulate over time and waste becomes inevitable. The idea of allowing all unfalsifiable claims seems unworkable, as it is incompatible with a limited budget for countermeasures. However, we lack a mechanism for ordering unfalsifiable claims by importance. Implementing anything short of all of them must be done in an unsystematic way. Without testable claims, and consequently nothing to compare, we end up balancing assumptions. While neglecting any defense might be an unacceptable risk for some, most Internet users confronted with impossible lists of security measures appear to simply tune out.

Nothing is secure but there is no way to disprove claims about security. To limit waste, we must be careful to not mistake sufficient security measures for necessary security measures.

Herley, C. (2016). “Unfalsifiability of security claims.” Proceedings of the National Academy of Sciences of the United States of America, 113(23), 6415-6420.

How Obvious Is It? The Content of Child Sexual Exploitation Websites

Child Exploitation (CE) imagery continues to be distributed publicly on the Internet. More than three-quarters of child sexual abuse imagery identified by the Internet Watch Foundation in 2014 was located on common domains, and not hidden. The accessibility of illicit media online is a significant concern for both parents and governments. Despite this, little is known about public CE websites.

Westlake, Bouchard and Girodat studied how websites providing CE material operate online. They attempted to determine how open CE website operators were about their illegal activities and whether they used any tactics to hide the content. They analyzed 634 websites distributing child sexual exploitation material, or hyperlinking to such a website. These websites contained at least one known CE image, or seven known CE keywords for a hyperlinked webpage. They then compared their review to an automated study of the same websites.

The overall purpose of this study was to determine how obvious it was that a website was explicitly CE-focused. The answer to this question lies in how well the websites were able to conceal their purpose from an automated data collection process. Consequently, there were two data collections for this study. The first was by an automated webpage collection tool. The second was a manual investigation of each website's homepage conducted over a period of two months, with a 14-month follow-up.

They found that many of the explicitly CE-focused websites identified manually were also identified automatically, suggesting that CE-related websites do little to hide their purpose. The presence of CE images or an explicit CE focus did not impact the survival of a website. 14 months after the initial study, 80% of the CE websites were still online, compared with 84.9% of all websites, including those not related to child exploitation.

The websites with CE images did not try to hide their intentions. Despite this, they were no more likely to fail than other websites. This reinforces the assumption that conducting illicit activities in public on the Internet generally does not increase the risk of failure.

For autonomous data collection tools to be effective in detecting CE websites, they need to be provided with proper guidance. Language and terminology evolve over time. The use of 'code words' is perhaps still even more fluid. Offenders must adapt quickly to avoid terms that have become commonplace. This means that autonomous tools need to extend beyond searching for only the code words used specifically to identify CE content to more descriptive language.

Child exploitation is no longer a hidden realm only accessed by sophisticated, technological masters. CE websites are easy to detect. This highlights the jurisdictional, privacy, and identification issues for law enforcement. Through understanding the layout, accessibility and the readily available content of CE websites, governmental agencies can more effectively use current tools to remove the content from the Internet.

Child Exploitation Websites don't appear to need to hide. Law enforcement seem to need better tools to overcome the current jurisdictional, privacy, and identification barriers.

Westlake, G. B., Bouchard M. & Girodat A. (2016). How Obvious Is It? The Content of Child Sexual Exploitation Websites, Deviant Behavior, doi:10.1080/01639625.2016.1197001

From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats

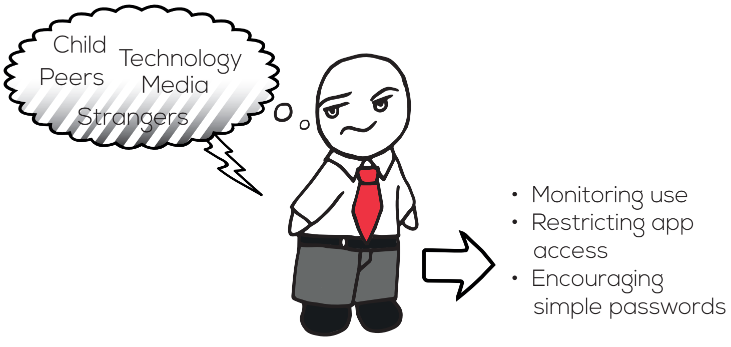
The rise in youth mobile media use has heightened parental concerns about the safety of children online. This raises some interesting questions about how children conceptualize privacy, whether children and parents' perceptions of online threats differ and how parents protect their children from threats. Zhang-Kennedy, Mekhail, Abdelaziz and Chiasson conducted semi-structured interviews with parents and their children. They wanted to explore the perceived privacy and security threats faced by school-aged children and what they do to protect themselves.

The researchers interviewed 14 families of children aged seven to eleven. The interview questions were chosen to gain insight into children's use of mobile devices. They also looked at parents' and children's understanding of privacy related risks They applied 'Grounded Theory' methodology to systematically and progressively classify and reclassify the results until a structure and then broader explanation was revealed.

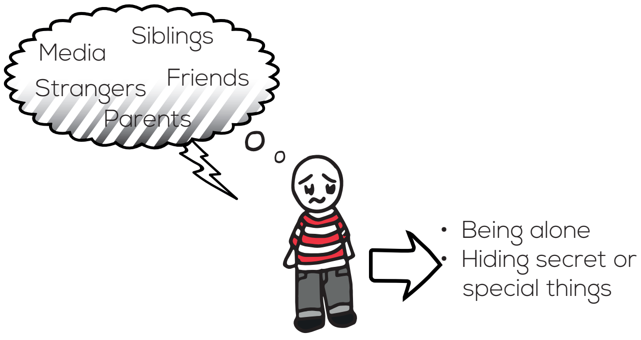
The researchers found that the children's understanding of external threats was very basic and reflected their experiences with offline safety. This included privacy models such as 'to be alone' or 'to hide secret or special things'. Children have specific threat concerns. Most children thought friends and siblings posed a threat because they could tamper with their device, compete for screen-time, 'mess up' their game, or get them into trouble with adults. They were concerned about exposure to bad words, violence, and other adult content. Consequently, they worried about punishment from adults for viewing 'bad' content. Only a small number of children raised the threat from strangers, but the risks perceived were limited to getting teased or bullied. However, parents perceived risks differently than children. They perceived more severe external risks from peers, media and strangers, as well as from technology and from the children themselves.

Parents protect children against potential threats with a variety of protection strategies which include: monitoring use; reviewing, restricting or prohibiting access to particular services or applications; increasing their own and their child's education about threats; and reviewing and configuring privacy and authorization settings for devices and applications. Unfortunately, some of their protection strategies put their children at further risk. Some examples include writing down the child's passwords, encouraging simple passwords that are easily guessable or creating password protected accounts for children that go unused.

As it might be expected, there is a clear gap between threats perceived by children and adults. Children showed less concern for online dangers because they do not yet know how to apply the concept of privacy online. Young children have underdeveloped models of privacy based on knowledge of the physical environment. They see their greatest security threats as coming from family members. Parents felt the need to safeguard children by limiting what they could access and who they could talk to online. They used many different methods to protect the safety of their children. However, these efforts sometimes unintentionally placed the children at greater risk. Interestingly, the results of this study suggest that security and privacy risks from family members or friends are far more common than harm from outsiders. It is important to take into consideration the differences in the perceived threats of children and parents when addressing security.



Parental Fears and Security Behaviours



Child Fears and Security Behaviours

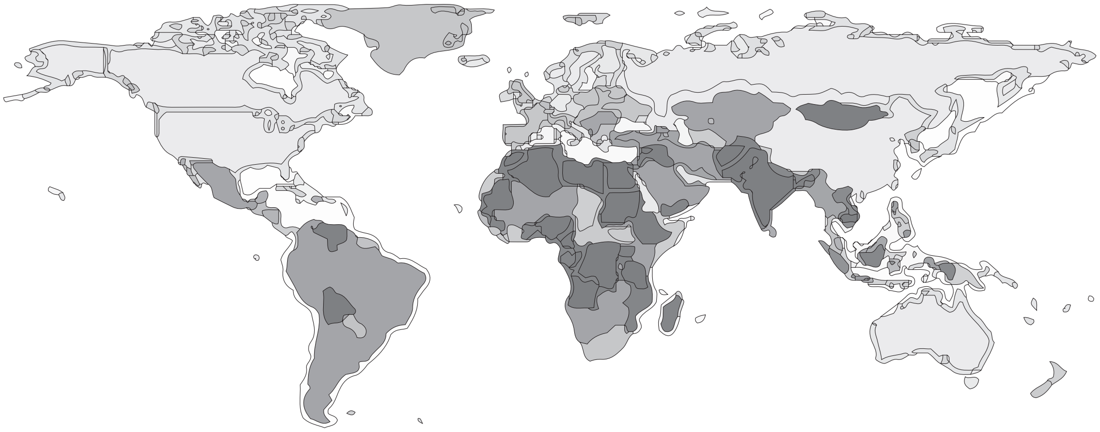
Children appear to define risk by the dangers they can understand and not those they are faced with. They behave differently to parents in ensuring their safety.

Zhang-Kennedy, L., Mekhail, C., Abdelaziz, Y. & Chiasson, S. (2016). "From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats." Proceedings of the The 15th International Conference on Interaction Design and Children, 388-399.

National-level risk assessment: A multi-country study of malware infections

A computer's vulnerability to malware infections is affected by technological and human factors. Technological factors include computer hardware, operating systems and applications, while human factors are related to the person using the computer, such as their computer expertise or safety habits. National policy could impact these factors and reduce the rate of malware infection, but there is little evidence or agreement on what exactly has an effect This lack of understanding and disagreement is a problem for cybersecurity policy makers.

Lévesque et al. assessed the risk factors related to malware infections in multiple countries. They determined country infection rates using data from millions of systems running a malware cleaner tool that scans Windows systems for infections. The researchers looked at the influence of factors related to economics, education, technology and cybersecurity on each country's malware infection rate. The Microsoft Malicious Software Removal Tool (MSRT) scans for and cleans specific malware infections. Microsoft randomly samples 10% of all machines running the MSRT on Windows XP, Vista, 7, 8 and 8.1., providing data on over one hundred million machines. Only systems without dedicated anti-virus software were selected for this study in order to avoid results biased by different anti-virus products. Gross Domestic Product (GDP) and Gross Domestic Product per capita by purchasing power parity (GDP-PPP) were used to measure a country's economic status against data from the International Telecommunications Union indicating national technology development.



Global Map of Infection Rates

There are better indicators of malware infection rates than economic activity. Education, technological infrastructure and cybersecurity investment seem to have a more consistent impact on malware infection rates. Internet connection quality seemed to influence the rate of malware infections. High broadband speed was associated with fewer infections in highly developed countries but more infections in newly industrialized countries. Individual security investment, such as the percentage of anti-virus protected machines, as well as global cybersecurity measures also seemed to protect against malware infections.

Investment in economic development may not directly impact malware infection rates. It appears that investment in education along with information and communication technology infrastructure may be more effective. However, technological and user education advancements affect countries of different socio-economic statuses differently. Therefore, to maximise the effectiveness of policy change, it is important for decision-makers to keep socio-economics in mind when investing in these protective factors.

Investment in education along with information and communication technology infrastructure may be more effective than economic development in reducing malware.

Lévesque, F. L., Fernandez, J. M., Somayaji, A. & Batchelder, D. (2016). "National-level risk assessment: A multi-country study of malware infections." Presented at the 15th Workshop on the Economics of Information Security, 1-30.

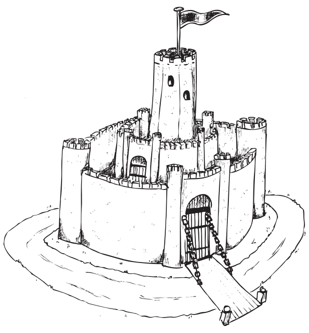
Beyond the Castle Model of cyber-risk and cyber-security

The Castle Model is a cybersecurity metaphor that draws from the idea of a traditional castle. High 'walls' create an 'inside' that is safe from threats 'outside.' However, this mindset impedes cybersecurity progress, as it keeps governments and organizations from cooperative opportunities. New technology, such as the automation of attack scenarios and use scenarios such as people bringing their own devices, are incompatible with the Castle Model. Spending a lot of money on this model does not necessarily come with a higher degree of protection.

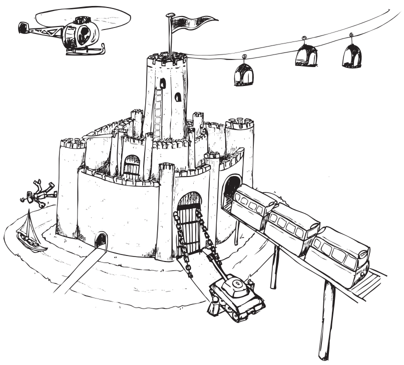
Leuprecht, Skillicorn and Tait argue that the Castle Model is outmoded. The authors feel that there is a need for a more balanced understanding of cybersecurity. Using key concepts from the Castle Model, they introduce three main arguments to explain their position: organizations are tearing down walls from the inside; technological developments are destroying walls from the outside; and changes in human interaction are blurring the distinction between inside and outside.

Organizations deliberately tear down their own walls and expose themselves to vulnerabilities. There are also high financial and temporal costs associated with the creation and upkeep of walls. Having weaker boundaries in a connected world creates more opportunities to do things faster and better. Second, technological developments are getting better at destroying walls from the outside. As cyberwalls are often bought off-the-shelf, they may contain vulnerabilities that can be broken into by adept attackers. It is becoming increasingly difficult to provide strong boundaries when it is easier than ever to detect and attack vulnerabilities in pre-existing walls. The model also fails to address the possibility of attacks coming from within the walls. It is also difficult to know when exactly a cyberwall is needed. Third, more recent generations, such as millennials interact with technology in a way that dissolves the line between a safe 'inside' and a dangerous 'outside'. They might not have such a strong physical sense of "being at work". This might lead them to work on confidential subjects in publics locations, unaware of security risks. They are also more likely to provide their own devices to work on, fusing the concepts of an inside and outside based model.

Castle Model of Security



Castle Model in Reality



The solution may be not to "fix" the current situation, but instead to respond to these forces differently. A paradigm shift towards thinking of "computing in compromised environments" could be key. This switches the focus from creating and securing a designated safe zone to masking and protecting data while it is at rest and in flight. This could be achieved through the dynamic technologies such as virtual machines and networks, or software and behaviour modelling.

Given the current situation, learning how to operate securely in compromised environments seems more promising than continuing to build higher and thicker walls. Future development should continue looking beyond a singular cybersecurity defence model and consider the use of dynamic and various responses. Modern technologies combined with better authentication may encourage a shift away from the Castle Model and towards a more secure way of thinking.

Thinking of security as a series of defendable walls creates an understanding that doesn't match the real world and leads to inferior decisions.

Leuprecht, C., Skillicorn, D. B. & Tait, V. E. (2016). "Beyond the Castle Model of cyber-risk and cyber-security." Government Information Quarterly, 33(2), 250-257.

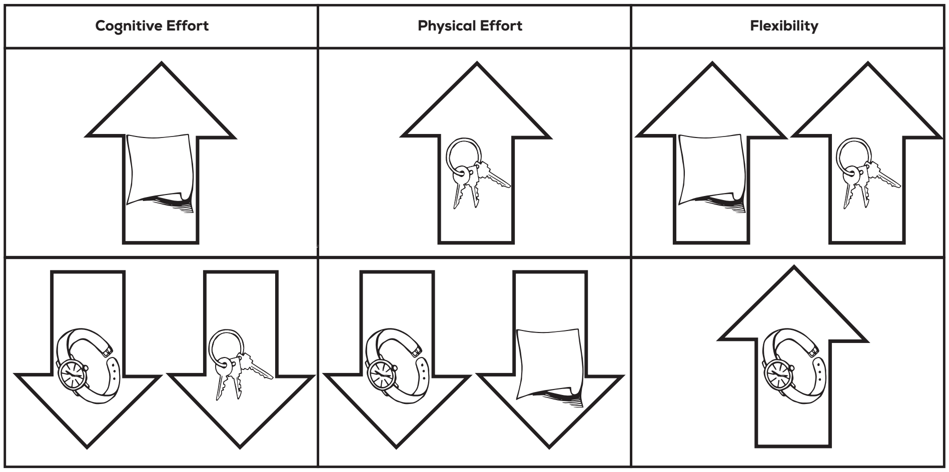
Responsibility and Tangible Security: Towards a Theory of User Acceptance of Security Tokens

Text-based passwords are the most common form of authentication. However, they are generally considered to be impractical for many reasons. Their complexity makes them hard to use. Users often struggle to manage many different, forgettable passwords. Furthermore, even strong passwords can be compromised through malware and phishing attacks. These factors support the idea of using physical devices or 'tokens' , instead of text-based passwords. This could help to achieve the goal of a practical security solution.

Payne et. al investigated factors determining user acceptance and expectations of a token-based authentication scheme that utilizes multiple wearable devices. Twenty semi-structured interviews were conducted lasting between fifteen and thirty-five minutes among a group diverse in age, (20-57), gender, and occupation. During the interview, participants were asked to identify the items they would prefer to carry as tokens and answered questions about the items they chose.

Participants were concerned about the convenience, design and trustworthiness of the tokens. They considered tokens more convenient when they could be used with many services and devices, made logging in quick and easy, and could be integrated into a something they already carry. Participants were comfortable with token designs that were familiar and easy to use, hold, and carry. Particularly, they preferred card-shaped tokens with fewer mechanical parts that fit easily into a pocket, wallet, or purse. Below shows participants perceptions about three types of tokens: Dual-Purpose (e.g. a watch), Practically Convenient (e.g. a keyring), and Flexible (e.g. a sticker).

Participants were concerned about trusting the tokens. They worried they would lose access to their accounts as a result of the tokens not working; tokens running out of battery, or breaking from everyday wear and tear. However, the main obstacle to using tokens as passwords is the participants concern about their security. They worried about who controlled the data, and whether their data could be misused. They also had particular concerns about tokens being lost or stolen.



In order to make the great changes required to transition to next generation passwords, it is important to consider users' expectations and concerns. Products that are both secure and practical are required to avoid repeating the failures of text-based passwords. Physical passwords should be convenient such as tokens that are attachable to things that people already carry. There must also be guarantees addressing concerns about the risks of the new technology. Service providers and regulators can play an important role in supporting public confidence by reducing the risk of using token-based authentication.

Security tokens must be convenient and their security must be guaranteed before the public will be confident in next-generation passwords.

Payne, J., Jenkinson, G., Stajano, F., Sasse M., A. & Spencer, M. (2016) "Responsibility and Tangible Security: Towards a Theory of User Acceptance of Security Tokens." arXiv:1605.03478

Open Book: A Socially-inspired Cloaking Technique that Uses Lexical Abstraction to Transform Messages

It has become increasingly important for Internet users to know how their information is being used. Very little of what we do on the Internet is private. When information travels through the Internet, it is readable at numerous points along the way because it is unencrypted. Communications can be collected for analysis; something social media companies might do for marketing information purposes. Encryption is a possible solution for security, but it is tedious and time consuming, as keys must be exchanged. Slip-ups can leave security compromised and users also have to convince their contacts to install the required software.

Gilbert created a method intended for the average user that employs a 'hidden-in-plain-sight' approach to dealing with prying eyes. This approach appropriates a technique generally used to counter eavesdroppers by transforming outgoing messages to be more vague. The system was implemented for use with Gmail by creating a browser-based tool to demonstrate how this tool can increase privacy.

The method aims to limit the amount of information that is available to eavesdroppers while keeping text understandable by intended recipients. Messages are transformed by analyzing the text and replacing keywords with vaguer terms; for example 'New York City' becomes '[location]'. The Sender has the opportunity to approve the transformation before sending and make modifications if the message is too abstract. The underlying assumption here is that the correspondents have enough history together to be able to decipher each other's messages with relative ease. Ten participants were enlisted to examine the workings of this assumption. Each participant, having received no training, was tasked with writing an email to be transformed using the Gmail browser plugin. The transformed email was then sent to their five most emailed, personal contacts, thus creating a group of 40 remote participants. The intended recipients were able to correctly interpret the keyword in 95.2% of cases, with relative ease. The same task was posed to unintended human recipients , who were only able to correctly interpret 2.3% of the keywords and reported high stress associated with the task. Testing with machines revealed that machine-learning algorithms have trouble recovering authorship information from the email corpus to which the method is applied.

The algorithm can play a vital role in extending the concept of privacy towards the average user. For many, encryption is viewed as being too technical, cumbersome and perhaps unnecessary. The program presents the average user with the ability to limit the amount of information available to communications analyzers, without the technicalities of encryption.

Security is currently limited to the technologically adept. Delving into this method in depth could drastically change how the general public views their privacy.

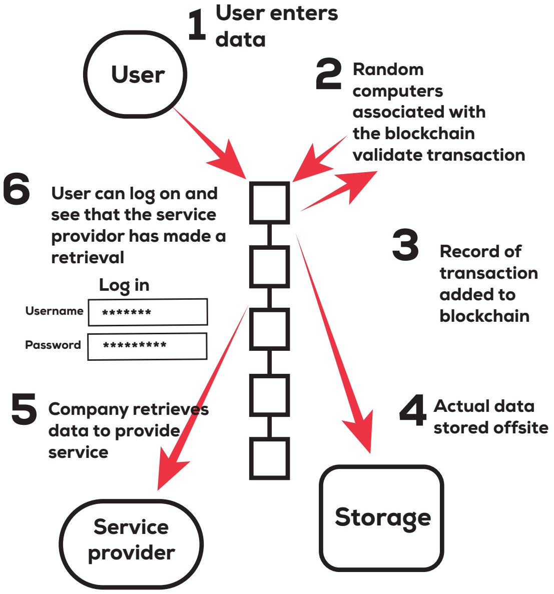
Private information exchanged between friends can be hidden in plain sight by introducing vagueness that can be deciphered without complex keys.

Gilbert, E. (2015). "Open Book: A Socially-inspired Cloaking Technique that Uses Lexical Abstraction to Transform Messages." CHI '15 Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 477-486.

Decentralizing Privacy: Using Blockchain to Protect Personal Data

Recent increases in security breaches of private data have led to a growing concern about how companies store private information. Large organizations, including banks, communications and social media companies, collect information to aid in their provision of services. Recent cases of malicious leaks have called into question the safety of storing large quantities of data in one place, which is the status quo for these companies. Recently consumers have called for greater ownership and transparency over the uses of their data, while still receiving the same high quality service as before. Bitcoin could provide an answer. The digital currency provides a system of decentralized and transparent online transactions. At the heart of BitCoin lies the blockchain technology. This provides a ledger of transactions in the form of a distributed and tamper resistant database that records all transactions.

Zyskind et al. applied blockchain technology, combined with off-blockchain storage, to create a more secure and transparent mechanism for storing private information. The authors suggest that a decentralized system built on the foundations of blockchain would answer all these concerns. The proposed system has three main components: the users, services and nodes; which are processing locations such as computers. All these actors interact in the blockchain.


1 User enters data
User
2 Random computers associated with the blockchain validate transaction
6 User can log on and see that the service providor has made a retrieval
Log in
Username *******
Password *********
3 Record of transaction added to blockchain
5 Company retrieves data to provide service
4 Actual data stored offsite
Service provider
Storage

There are two types of transactions accepted by blockchain: changes to who can access the data and data storage/retrieval. Both the user and the service provider have access to this data. However, the user retains ownership and can revoke the service provider's access if the user senses a security breach. The entire system is based on a series of approved transactions. Each one can be thought of as a building block. Because every single transaction is recorded as part of a chain of blocks known as the 'blockchain' and is validated by a random selection of nodes, it is nearly impossible to tamper with.

Consider this system at work when a person downloads an app that requires access to their email, location and contact list. When the user signs up for the first time, a new identity shared between user and service provider would be generated and sent to the blockchain with the associated data and permissions. This transaction is then verified by a set of random computers with the blockchain maintaining a record documenting this transaction. The blocks in the blockchain retain a record and timestamp every transaction, which enables both parties to track the use. The data is then stored separately. Now, both the user and the service provider can access the data by sending a retrieval transaction to the blockchain, which verifies the permissions and identity of the access-er. Users are able to view their data transaction and change access control through an online dashboard similar to the centralized wallets used for Bitcoin.

The blockchain allows the user to retain data ownership and provides a resilient data storage solution. Because the stored data can be distributed, a hacker cannot gain access it all in a single breach. Even if someone were to gain access to the blockchain, there is very little harm that could occur. Only "pointers" recording transactions are stored and the data locations are encrypted. In the case that a hacker gains access to both the user's digital signature and encryption key, only a single set of data is affected since all user-service pairs have their own unique identity,

If implemented widely, this technology could allow companies to increase security without compromising their services data needs. Companies who implement this system would be able to focus on maximizing data utility without having to dedicate large amounts of resources to network resiliency, as the blockchain protects itself. While this technological application is still in the development phases, it appears that blockchain and decentralized trust systems are becoming an increasingly prominent mechanism in the realm of cybersecurity.

Using a blockchain for personal information allows the user to retain ownership over their data and provides a resilient data storage solution.

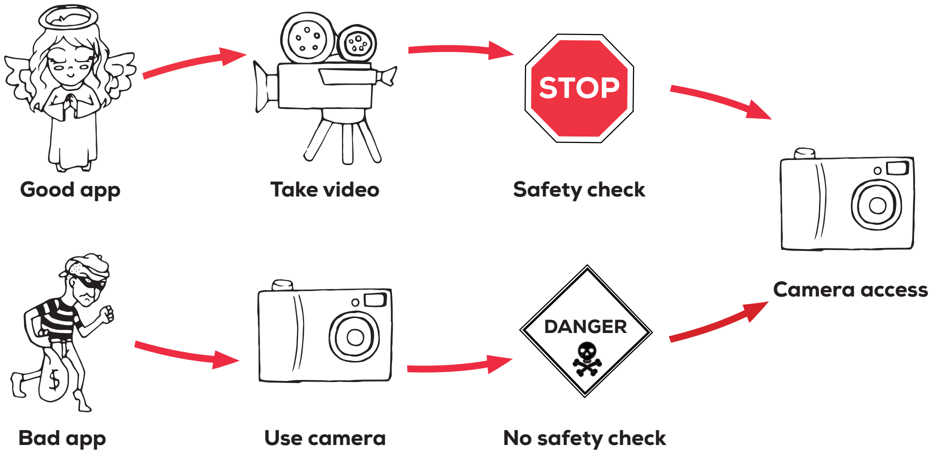
Zyskind, G., Nathan, O. & Pentland, A. (2015). "Decentralizing Privacy: Using Blockchain to Protect Personal Data." Security and Privacy Workshops (SPW), 2015 IEEE.

Kratos: Discovering Inconsistent Security Policy Enforcement in the Android Framework

There are resources on smartphones that are sensitive and need to be protected. For example, the camera or the ability to send a text messages are sensitive because they can be used maliciously. The Android operating system gives permission to applications to access sensitive resources on a case-by-case basis, based on a predefined security policy. In permission-based security, an app asks the system to use these resources. The permissions are enforced by code written by the programmers of Android. However, Android is a large piece of software written by hundreds of people over many years. As a result, there can be places where the permission checks are wrong or missing. This can lead to apps being inappropriately able to use resources or blocking valid apps from accessing resources.

The review of the security policy of a large program such as Android requires finding all the places in its code where permissions are granted. This is usually not possible to do manually. In order to tackle this, Shao et al. created and tested a technique for finding problems with policy enforcement in a large program. They developed an automated approach that produces a ranked list of problems for an expert to review.

Android controls access to resources like the camera by using "system services". System services get requests from Android apps and do safety checks before allowing access to the resources. Android has a central service manager which controls access to all system services. The policy checking method uses this central manager to find all places where policies should be enforced. Then it finds all the possible ways the program can get to these services. Once the paths to these services are known, the security checks on these paths can be identified. To detect problems with the security policy, they compare the checks from different paths to the same sensitive resource. Any differences are flagged as potential problems for manual review.



They found 14 cases of inconsistent security policy enforcement in 6 different Android versions that could allow attacks. They discovered that there are more problems with newer versions. This is probably because of an increase in the number of "system services" as more features were added. They also found that disabling "hidden interface" access to resources for applications would reduce the number of flaws in Android. Many weaknesses in Android also exist because multiple "system services" control the use of one resource. They recommend having only one service to protect each resource.

Any organization that has large programs could use this approach to find problems with security policies. Programmers can make mistakes, so double checking policy enforcement is recommended to make sure a system is secure. Limiting access to sensitive resources and disabling the use of hidden interfaces can also reduce the number of problems.

Automated techniques can help find problems with policy enforcement in large permission-based programs like Android.

Shao, Y., Ott, J., Chen, Q. A., Qian, Z. & Mao, Z. M. (2016). "Kratos: Discovering Inconsistent Security Policy Enforcement in the Android Framework." Proceedings of the Network & Distributed System Security Symposium (NDSS), San Diego, CA.

serene risc

Smart Cybersecurity Network (SERENE-RISC) is a knowledge mobilization network that organises six key activities intended to reach its various audiences: workshops and seminars, a relationship brokers' forum, quarterly knowledge digests, Konnect - online knowledge-sharing platform, a public website and a professional development program.

Workshops & Events.

Cyber challenge	🕓 November 2016 🏢 Ottawa
Bi- Annual Workshop	🕓 April 2017 🏢 Montreal

Knowledge Digest

More than 80 pieces of research on cybersecurity summarised.

Opportunities available to network partners to help empower future professionals with practical knowledge translation skills through mini-scholarships.

Konnect Platform

Find the presentation videos and slides from workshops and tutorials and much more.

Over 600 selected articles and research pieces on cybersecurity for and by Canadian experts.

Website

Find out the latest news, tips and job postings at:

www.serene-risc.ca

Connect with us on Twitter, Facebook and Linkedin:

@SERENE_RISC /sereneriscc /serene-risc

Cybersecurity Public Awareness Tools & Library Outreach

Cybersecurity is an issue for everyone so we see a role for everyone in addressing the issue. We are aware of the tremendous role libraries play as educators and trusted sources of knowledge. We found that libraries are doing great work to support technology. They are doing such a good job that they are often the primary source of Internet access, technical support and practical information for not only the public generally, but those that might be at greater risk online. With the support of Public Safety Canada, we have developed interactive training tools using leading edge Canadian research provided by our national network of academic, government and industry partners. The training program is available free of charge to enable libraries and community centres across Canada to deliver instruction to the public on the best practices for staying safe and secure online.

The program consists of a number of flexible modules that can be either presented together as a course or combined to augment existing information technology training sessions where appropriate. The resources will be freely available and include trainer guides, classroom handouts, planning tools and a multimedia website with videos, mini-quizzes etc. We are currently working with libraries across the country to deliver train-the-trainer sessions to enable a sustainable system of disseminating the best advice to the people who need it in a form they can access. Find out more at:

www.cybersec101.ca

The SERENE-RISC Quarterly Cybersecurity Knowledge Digest

2016 Autumn

Editor-in-Chief: Michael Joyce
Scientific Editor: Sonia Chiasson
Editor: Shannon McPhail

Gilbert E. *summarised by* Khadija Baig *sponsored by* SERENE-RISC
Zyskind, G. et al. *summarised by* Lauren Craik *sponsored by* SERENE-RISC
Payne J. et al. *summarised by* Masoumeh Shafienejad *sponsored by* SERENE-RISC
Shao et al. *summarised by* Mariana d'Angelo *sponsored by* SERENE-RISC

Links to external sources for papers are provided for convenience only and do not represent an endorsement or guarantee of the external service provider.

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

serene risc

Université de Montréal