serene risc Digest Spring • 2015

Cutting Edge Research Summaries for Policy-Makers and Practitioners

Does requiring users to regularly change their passwords really improve security ?

A common security policy is to require that users regularly change their passwords but the actual benefit from this practice has never been evaluated. Using the length of a password expiration period and the estimated time for an attacker to do their work, Chiasson and van Oorschot assess the degree to which password expiration policies can actually add any security advantage. In the best case scenario, such as with randomly generated passwords, the security benefits are minor and may not outweigh the cost to the user. In real world conditions, recognizing passwords often follow predictable patterns, the benefit is even smaller. To be effective, the duration of an expiration period must match users` ability to comply with the rule.

Are your friends accidentally tweeting your location ?

Even if an individual has chosen not to share their location, the location of their common contacts can reveal their whereabouts. Compton et al. have designed a method that estimates the location of a large number of users. This approach compiles information that an individual provides, either in a user profile or through device GPS readings, alongside information from a user`s contacts. For users who choose not to share their location information an algorithm infers their whereabouts based on the city of their friends who have made their information public. This approach to mining publicly available data is an improvement on other known methods for deriving location information, and can assist with attribution by increasing the effort required to conceal a social media user`s identity.

Is one man's security is another man's insecurity ?

Different approaches to security, or 'security mindsets', influence how threats are perceived, how security is conceived, and these ideas can lead to conflicting responses. A security mindset informs how each person thinks and speaks about security, but also shapes how we solve problems. In this way, the security mindset influences what means and methods of protection are seen as appropriate, while gradually shaping institutions and structures in society; such as the legal system. Kremer explores two security mindsets in depth: the military security mindset, concerned with broad strategic considerations such as national security, and the liberal security mindset, which focuses on the balance between security and individual rights. The striking differences between these mindsets make clear why some debates about security remain unresolved. To foster open lines of communication, however, these perspectives can be understood as mindsets, rather than operational imperatives.

What is surreptitious encryption weakening and how can we prevent it?

Cryptographic systems must resist overt attack, but also be resilient against sabotage and covert weakening. To better understand how unknown weaknesses in cryptographic systems are successfully exploited, Schneier et al. create a taxonomy to describe the properties of cryptographic weaknesses. Secrecy, utility, and scope are the three major domains. When these factors are present and strong, the attacker is more likely to be successful. These dimensions can be used to explore historic cases of cryptographic weaknesses that were successfully exploited, and also point to strategies for strengthening cryptographic systems, including public review and publishing of encryption code.

What is the harm in cybersecurity hype ?

Cybersecurity has generated a lot of interest and activity, a flurry that sometimes obscures the real threats and viable solutions. Because this misrepresentation can do damage, Lee and Rid present the case for exercising restraint in discussions about cybersecurity. The article elaborates thirteen reasons why `hype` about cyber is a problem for achieving true security. Responsibility for an accurate picture of the true risks is shared across: senior officials, who should hold basic technical knowledge and value personnel with hands-on experience; the press, who can emphasize accuracy in reporting and specialty knowledge; and researchers, who must collaborate across disciplines in clear and accessible language.

Are implanted 0days worth the cost ?

The reaction to flaws in computer software and hardware has traditionally been defensive, however, in cyber operations these vulnerabilities can also be exploited for offensive gains. Sigholm and Larsson use the Heartbleed vulnerability as a case example to illustrate this type of cyber operation, as though the vulnerability was intentionally implanted to reach an intended target. Three different scenarios are explored for the rate of adoption. The time required to reach global adoption, representing the probability of compromise of the intended target, varies with each scenario. Under all scenarios, more than half of all users will have adopted the vulnerability after three years, and more than three quarters after four years. The spread of vulnerabilities is a slow process. Before implanting or exploiting a vulnerability, military operations must consider the available time. Crucially, the operation must also consider mitigate any risks of collateral damage caused by the imprecise nature of this tool.

Are security seals all they cracked up to be ?

A webshop owner needs to provide safe channels for customers to transact, but also convince customers of the security of those transactions. A security seal from a trusted third party provides a visual symbol that can reassure potential online customers of the trustworthiness of a website. Goethem et al. tested whether these security seals actually represent greater security and found that those websites are not necessarily more secure than their counterparts. In fact, seals can actually facilitate attacks by flagging vulnerable targets, providing a method for discovering specific issues, and offering easily mimicked signs to deceive potential customers. To ensure the integrity of a symbolic certification, website owners and seal providers must both ensure rigorous testing and respond promptly to identified issues.

What will motivate people to be safe online ?

Despite warnings about potential threats from online activity, many users do not follow basic safety practices. Influencing people to step up to online security means communicating the seriousness of threats in a way that motivates action. Shillair et al. examined a number of factors related to human motivation to find those that influence people`s online safety decisions. Some people need only the information about risks and some guidance on safe practices, but others will need additional support to integrate the knowledge into everyday routine. It is not only knowledge that gets people moving, but also confidence in their ability to deal with the safety issue. Some people are more likely to step up when they're reminded of a personal responsibility for their own, and others, online safety. There are many factors that work in different ways for different people, and so an understanding of the audience should shape online safety messaging.

How much doubt is reasonable for attributing cyber attacks and for whom ?

Attribution is fundamental to cyber security. Attribution in digital forensics faces some added challenges because of the mythology surrounding cyber capacity. Like any investigation, there are pressures to maintain reputations and affiliations on a larger scale. Investigating cyber attacks fully requires coordinating multiple specialties, proceeding through judicial levels, and prevailing in legal proceedings against competing evidence. Rid and Buchanan developed the 'Q Model' to illustrate the complexity of the process of attribution. The model emphasizes the need to question the results of an investigation or attribution process. This safeguard is built in to the process in the model by the communication between the levels.

Are Digital Investigators countering anti- forensic techniques ?

The evidence used in forensic investigations is increasingly digital; with the proliferation of electronic devices, digital evidence is relevant in a wide variety of crimes, but is inherently fragile and easily altered. Anti-forensics is the intentional hiding or destruction of evidence, and can significantly impact the practice of digital forensic investigators. de Beer et al. examine how digital forensic investigators are coping with anti-forensic activity in the South-African context. They find a generally low level of knowledge about the full range of anti-forensic threats and inconsistent use of countermeasures. It is important that effort is made to further skills training for digital forensic investigators as a greater fluency with anti-forensic methods might broaden the tools for countermeasures, as well as enhancing their confidence and efficacy.

Quantifying the Security Advantage of Password Expiration Policies

A common security policy is to require that users change their passwords at regular intervals. The actual benefit from this practice has never been closely evaluated. Although a regular change in password might improve security in some scenarios, for example by ending access of an adversary who has already breached the account, any added resistance against new attacks is not clear. As a strategy against modern attack methods, on the other hand, a strict password change policy may not significantly improve security.

Chiasson and van Oorschot assess the degree to which password expiration policies can add a security advantage. Their model relates the length of the password expiration period to the time required for an attacker to test all key ciphers, and considers both the best case and real world conditions of password use. A randomly generated password is the best case scenario for security policies. In real-world conditions though, passwords are often of varying length and are usually not randomly generated. Instead, real-world passwords often follow predictable patterns, such as a variation of a previous password or one of a set of commonly selected passwords. Consequently, these are more easily guessed. This points to the importance of usability in security policies. It is reasonable to expect that users will resist changing their password. As such, an effective expiration period must match the users`ability to comply.

When an attacker guesses repeatedly, their chance of success is greater; an adversary is almost certain to succeed by continually cycling their password guesses. Under best case conditions, there is a small security benefit from requiring regular changes in password. The likelihood of successful attack can be reduced from 100%, to a 63% probability of successful attack. In this best case, the security benefit from password expiration policies are minor and may not outweigh the cost to the user.

The capacity of users to manage password changes should be considered in the design of a password expiration policy, in particular the length of time before a password must be changed.

Overly frequent password changes do little to reduce the risk of compromise and could result in users choosing simpler, more guessable passwords.

Chiasson, S., & van Oorschot, P. C. (2015). Quantifying the security advantage of password expiration policies. Designs, Codes and Cryptography, 1-8.

Geotagging One Hundred Million Twitter Accounts with Total Variation Minimization

Although many users choose not share their location information, there are methods to estimate the city of a Twitter user with a high degree of accuracy. Social ties in online networks often reflect geographic closeness in the physical world. So even if the individual has chosen not to share their locality, the location of their common contacts can reveal their whereabouts. This is the principle behind a new method for inferring the city of Twitter users.

Compton et al. have designed a method that estimates the location of a large number of related users. This approach relies on multiple sources of public information, depending on how much detail each user has revealed:

- Users that have activated the GPS functions on their devices provides location information directly.
- Users that have reported a 'home' location in their Twitter profile provide approximate location information.
- Users that have declined to share location information, an algorithm infers their location based on the location of their friends who have made their information public. Friends are determined by the number of reciprocal mentions between users – that is, how many times two users tag one another in tweets.

The method isn`t perfect, providing poor information on users who move often and far, or on those with a geographically dispersed network. However, the method can provide accurate location information by factoring in individual movement and the spread of the network. From over one billion mentions between 110 million users, the algorithm correctly identifies the tweeter's city in 89.7% of cases. This is an improvement on other known methods for deriving location information.

Mining publicly available data in this way can leverage the connections between a large volume of social media contributors to support better understandings of activity and behavior in physical space. Even a user who takes steps to keep private their whereabouts can be found through the location information of their network. This research provides a potential method of deriving the approximate location or movements of twitter users based on their contacts. This approach can assist with attribution by increasing the effort required to conceal a social media user`s identity.

The connections between and use of twitter accounts can reveal the approximate location of the users.

Compton, R., Jurgens, D., & Allen, D. (2014, October). Geotagging one hundred million twitter accounts with total variation minimization. In Big Data (Big Data), 2014 IEEE International Conference on (pp. 393-401). IEEE.

Cyberspace holds promise but also risk as an evolving channel for communication. Security activities help to balance the positive and negative, ensuring potential benefit and managing potential harm. In this article, Kremer explores how different approaches to security, termed 'security mindsets', influence how threats are perceived, how security is conceived, and how these ideas can lead to conflicting responses.

A security mindset informs not only how each person thinks and speaks about security, but also shapes how we solve problems. In this way, the security mindset influences what means and methods of protection are seen as appropriate and necessary and gradually shapes institutions and structures in society; such as the legal system. Understanding these positions as contestable and contextual mindsets, rather than as unquestionable truths, can provide a foundation for critique and debate.

Jens Kramer explores two security mindsets in depth: the military security mindset and the liberal security mindset. The military security mindset is defined by concern with strategic considerations of national security. The liberal security mindset is interested in balancing security with individual rights. Some distinguishing features are shown below:

	Military security mindset	Liberal security mindset
Source of threat	External enemy	Individuals
Target of threat	Community or key infrastructure, national interest	Individuals
Focus of protection	National security	Individual, as well as collective security interests
Nature of response	Military, tactical, strategic means and methods, exceptional means	Policing means and methods, justified within legal frameworks
	Distinguishing which need military countermeasure	

> "Looking at the dangers of cyberspace with a military mindset of security means to suspect a potential existential threat to society or country in every malicious act, which is then regarded as an act of warfare coming from an external enemy. Looking at cyberspace with a liberal security mindset allows differentiating between the threats. It allows differentiating cybercrime from cyberwar, enabling different responses to threats. "

A liberal security mindset will privilege privacy, but there is a lack of diverse tools for countering threats. As such, even intervention within the rule of law may expand legal or police control.

The striking differences between the mindsets make clear why some debates about security remain unresolved; on some points, the perspectives cannot be reconciled. However, these perspectives can be understood as mindsets, rather than operational imperatives. Different security mindsets may actually lead to a similar outcomes, such as the increasing overlap between national security and internally-focused criminal law.

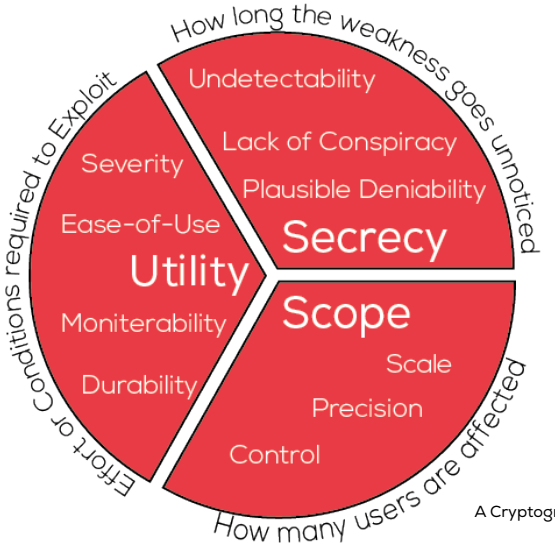
Understanding conflicting approaches as an outcome of differing mindsets provides a tool for finding complementary security efforts.

Kremer, Jens. (2014). "Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace." Information & Communications Technology Law. 23 (3): 220-237.

Surreptitiously Weakening Cryptographic Systems

Cryptography is critical to modern information security. In addition to resisting overt attack, cryptographic systems must also be resilient against sabotage and covert weakening. These more surreptitious attacks can include errors built in to cryptographic systems in the design stages, or vulnerabilities introduced during implementation or later. There is a desire to better understand how unknown weaknesses in cryptographic systems are successfully exploited, beyond a description of how past attacks have been performed.

One way of understanding similarities and differences is to arrange examples according to specific properties. A taxonomy is a set of consistent rules for organizing content. Schneier et al. create a taxonomy to describe the properties of cryptographic weaknesses. Secrecy, utility, and scope are the three major domains of weakness. Each domain has several components that can be used to characterize a weakness in more detail.



A Cryptographic weakness taxonomy

When these factors are present and strong, the attacker is more likely to be successful.
These dimensions can be used to explore historic cases of cryptographic weaknesses that were successfully exploited. When the taxonomy is used to categorize examples of attacks, it is possible to see patterns. An example is seen in the tradeoffs faced by a saboteur. For example, if precision in targeting and control over who shares access to the weakness are high, conspiracy must also increase, which reduces deniability. The taxonomy can also be applied to look at attack approaches more abstractly. What are the characteristics of various strategies, such as building in a low resistance to cryptanalysis or choosing backdoor constants, and of flawed implementation approaches, such as involving bad randomness or leaking key data?

This analysis reveals strategies to minimize weakness and defend against cryptographic sabotage:

- Look for cryptographic systems with publicly available encryption code.
- Before deploying new systems, test against multiple security models to ensure broader coverage against threats.
- Consider whether standards for cryptographic systems have had sufficient public review.
- Remember that sabotage can be built right into the design, in full view.

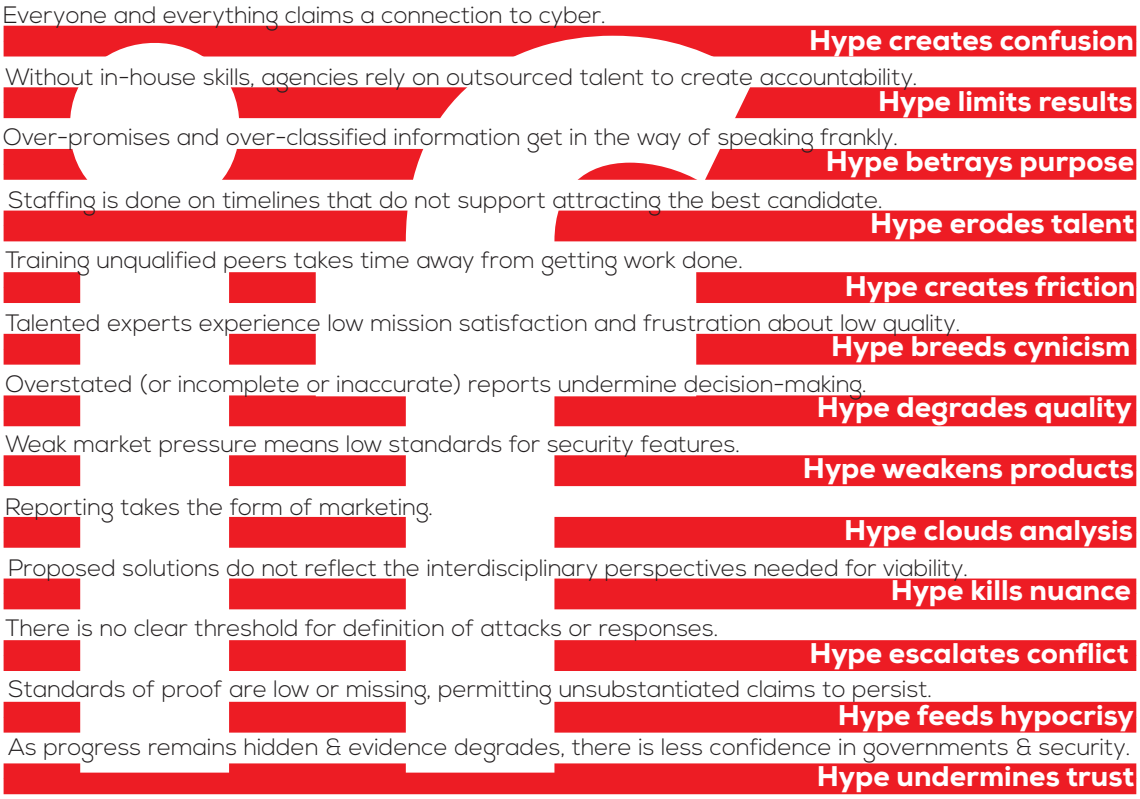
Cryptographic weakness taxonomy helps identify potential forms of exploitation and assist choosing an encryption scheme that is suited to a particular need.

Schneier, B., et al. (2015). "Surreptitiously Weakening Cryptographic Systems."

OMG Cyber!: Thirteen Reasons Why Hype Makes for Bad Policy

Cybersecurity is a high priority issue. It has generated a lot of interest and activity that sometimes inflates the real situation. Some of the current discussion about cybersecurity does not accurately represent the threats or solutions, and this misrepresentation can do damage.

Lee and Rid present the case for exercising restraint when representing cybersecurity. The article elaborates thirteen reasons why `hype` about cyber is a barrier to achieving true security, shown below.



If we don't exercise restraint, Hype causes thirteen problems.

The hype about cyber can lead to specific complications.
Inaccurate understandings of cyber contribute to unnecessary confusion about true risks. This negatively affects decision-makers trying to understand threats, measure responses, and evaluate performance. It also hinders experts tasked with doing highly skilled and technical tasks, while working in teams with non-experts. Further, cyber hype complicates the task of public consumers seeking to understand risk, choose tools for protection, and – ultimately – hold governments to account.

Misunderstandings about cyber are counterproductive to achieving real security. In the quest for more informed and informative debate, hype should be deflated by ensuring:

- Senior officials in cybersecurity should hold basic technical knowledge,
- Military value personnel with hands-on experience,
- Press ensure journalistic accuracy, specialist writers and editors, and
- Scholars communicate clearly, across disciplines.

Hype around cyber brings problems caused by simultaneously under-informing and over-pressurising decision-makers.

Lee R.M., and Rid T. (2014). "OMG Cyber!: Thirteen Reasons Why Hype Makes for Bad Policy". RUSI Journal. 159 (5): 4-12.

Determining the Utility of Cyber Vulnerability Implantation: The Heartbleed Bug as a Cyber Operation

The reaction to flaws in computer software and hardware has traditionally been defensive, seeking to correct errors and protect assets against potential threats. Alternatively, these vulnerabilities can also be exploited for offensive gains in cyber operations. The overall utility of this type of cyber operation must consider the potential benefit relative to the potential costs of not correcting a potentially harmful flaw. These costs can include economic outcomes, as well as impacts on human lives, or political ends, such as the security and stability of states.

Sigholm and Larsson use the Heartbleed vulnerability as a case example and develop the situation as though the vulnerability was intentionally implanted to reach an intended target. Three different scenarios are explored for the rate of adoption of the flawed software, with time to reach global (100%) adoption representing the probability of target compromise. If the vulnerability is adopted by 100% of users, the intended target has been reached, whereas if 50% of users adopt the vulnerability, the probability that the intended target is reached is 50%.

In the first scenario, the rate of adoption of the vulnerability is similar to the actual initial spread of the Heartbleed vulnerability. With that assumption, the vulnerability is adopted by 91% of users within four years. The second scenario assumes a high adoption rate and reaches 100% of users in 39 months. The third scenario, deemed the most realistic, uses an initially high but decreasing rate of adoption, affecting 76% of users at four years. Under all scenarios, more than half of all users will have adopted the vulnerability after three years, and more than three quarters after four years.

Vulnerabilities can be leveraged for military use, but only when time is plentiful. The spread of vulnerabilities is a slow process, so not a viable strategy for time-sensitive operations. The lack of precision results in a large number of potentially critical systems being vulnerable increasing the risk of collateral damage. Before implanting or exploiting a vulnerability, military operations must also consider and mitigate the risks of collateral damage, including to critical infrastructure or services and threats to the general public.

When considering the overall utility of leveraging a cyber vulnerability for military effect, it is important to evaluate ways to mitigate adverse impacts. These impacts should include determining whether deliberately concealing risk to the public will affect other social goals, such as accountability or democratic aims.

Implanted vulnerabilities are a slow and imprecise tool for compromising targets and the use of such tools should be weighed against the increased risk to society.

Sigholm, J., & Larsson, E. (2014). "Determining the Utility of Cyber Vulnerability Implantation: The Heartbleed Bug as a Cyber Operation." In Military Communications Conference (MILCOM), IEEE.

Clubbing Seals: Exploring the Ecosystem of Third-party Security Seals

The success of e-commerce depends on secure channels for business. Webshop owners must not only provide safe ways for customers to transact, but also convince customers that their transactions are secure. Certification from a trusted third party is one way of earning this trust. A security seal provides a visual symbol that can reassure potential online customers of the trustworthiness of a website. A visible security seal often indicates that a website has been tested for issues such as known vulnerabilities or implanted malware, although the criteria for earning a certification vary, as does the rigour of the testing.
Goethem et al. tested whether these security seals actually represent greater security, with a combination of three methods, summarized below.

What they did	What they found
Comparison of sites currently certified to those without seals:	Sites with a seal are not more secure.
Researchers examined 2238 websites with seals, and as many without seals, and counted the popular security mechanisms (including secure cookies, HTTPOnly cookies, Content Security Policy) present on the main page and ten other pages in the same domain.	For most of the security best practices tested, there is no significant difference in adoption between sites that do and do not have seal. Certified sites are more likely to use HTTP-Only Cookies, but those without seals are more likely to have X-Frame options and anti-CSRF tokens.
Manual penetration test:	Sites with a seal are not more resistant to attack.
With permission of the website owners, researchers purposefully tried to find common vulnerabilities in sites certified as secure.	Seven out of the nine websites have severe and high risk vulnerabilities, including some that are not covered in scanning for certification (which shows limitations of the scanning methods), also some identified 'easily discoverable vulnerabilities in six out of nine websites that were missed by the seal providers.
Analysis of certification methods:	Certification investigation methods are not thorough.
Researchers created a sample webshop with multiple well-known vulnerabilities, and then tested the website with scans from eight seal providers.	All eight scans found less than half of the vulnerabilities in the sample webshop. Two found none (also learned that these two did not actually use scanners to discover vulnerabilities. Of the four that check for malware, only two found malware.

Websites with security seals are not, in fact, more secure than their counterparts. Beyond simply failing to detect issues with websites, seals can actually facilitate attacks by:

- Identifying vulnerable targets. When a certification is suspended, the seal provider often changes the image on the client`s website until the issues are remedied. That change, discoverable by web-crawling technology, indicates a site with a vulnerability that can be exploited.
- Providing a method for discovering vulnerabilities. The scanning techniques used by seal providers is a series of requests that can be exploited to find issues with websites.
- Deceiving potential customers. A security seal can be mimicked on a phishing site to provide false reassurance about website validity.

Website owners should carefully consider their choice of third-party seal provider, while also performing their own due diligence in security testing. Seal providers could more rigorously test their scanning tools against known vulnerabilities, to improve the coverage of potential threats. Further, when a security issue is identified, seal providers can provide a grace period for website owners to remedy the problem before removing the seal as a penalty; this could prevent some use of the seals as a vulnerability scanner.

Security seals can be far from a guarantee of safety and could be subverted for nefarious purposes.

Van Goethem, T., et al. (2014). "Clubbing Seals: Exploring the Ecosystem of Third-party Security Seals." In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM.

Online safety begins with you and me: Convincing Internet users to protect themselves

People rely on the Internet for a whole range of business and pleasure pursuits, but this tradition is not entirely free of risk. Despite warnings about potential threats, many users do not follow basic practices to stay safe online. Do people not understand the risk? Are the instructions too complicated? Or do they think someone else has them covered?

Motivating people to step up to online security is a significant challenge. It is no small task to communicate the seriousness of the threats in a way that motivates participation in taking manageable, accessible precautions. Shillair et al. examined a number of factors related to human motivation to find those that feature heavily in online habits. Through a web-based survey, 161 participants were assigned to one of four groups. Each of the four groups saw different messages: some were encouraged to accept personal responsibility, others were assured responsibility lies elsewhere; some participants were shown a step by step demonstration of performing safety habits (called 'vicarious experience), while others were given messaging to boost their confidence in handling online risks, but without being shown how (known here as 'persuasion'). This use of groups allows a comparison of those factors in people's online safety decisions.

After reviewing the messages, participants in all groups responded to a questionnaire asking their:
• intention to perform online safety behaviours (e.g. read license agreements before downloading software)
rating of personal responsibility (e.g. 'online safety is my personal responsibility' vs. 'online safety is somebody else's job, not mine')
• response efficacy and coping self-efficacy (e.g. confident could identify terms in agreements or privacy policies that pose threat)
• measure of prior knowledge (e.g. questions about knowledge of spyware and Trojans)
• technology awareness (e.g. 'I follow news and developments about malware tech')
• message involvement (e.g. 'how carefully did you read the online safety information')

People with prior knowledge of online safety problems tended to have higher levels of coping self-efficacy; the confidence in their ability to deal with the problem. Those who were shown how, through vicarious experience, had a stronger sense of their ability than those who were merely encouraged. The emphasis on personal responsibility had no effect on people's safety behaviour intention or on coping self-efficacy. However, among those who had only a little online safety knowledge, the messages about personal responsibility had a different role; in the high personal responsibility group, being shown how (vicarious experience) resulted in greater safety intentions compared to persuasion. In contrast, among the low personal responsibility (and low prior knowledge) group, persuasion was more effective in changing intention. The relationship was different among those with greater prior knowledge – for those who were reminded of a personal responsibility, self-efficacy had no effect, while those in the low personal responsibility (but high prior knowledge) group, were more influenced by vicarious experience.

These findings reinforce the importance of understanding your audience when creating security messaging. Some people need only the information about risks and some guidance on safe practices, but others will need additional support to integrate the knowledge into everyday routine. Ultimately it's clear which mechanisms work; the important decision is how to combine them for different groups.

Telling Internet users that they have to be safe online has little effect on their intention unless the message and education is appropriate for that user.

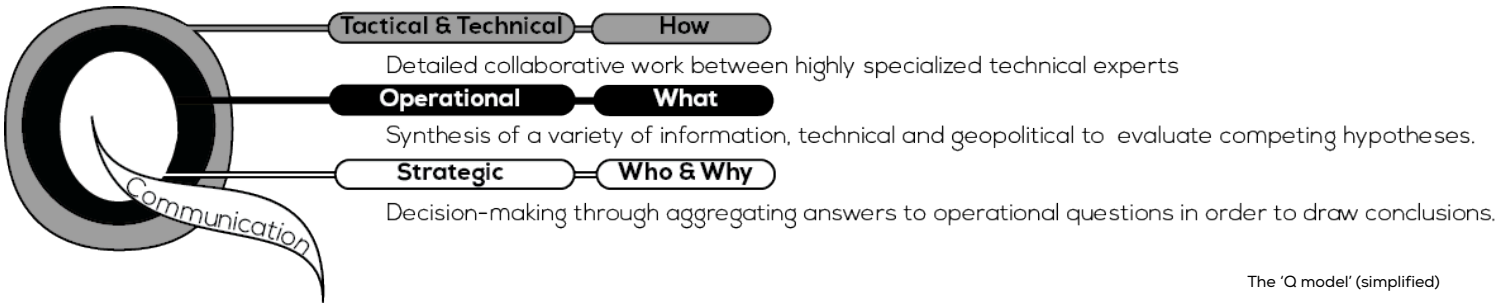
Shillair, R., et al. (2015). "Online safety begins with you and me: Convincing Internet users to protect themselves." Computers in Human Behavior, 48, 199-207

Attributing Cyber Attacks

Attribution is fundamental to cyber security. An appropriate response to any cyber offence requires first identifying the offender. Finding 'who did it?' is often seen as a purely technical problem, a puzzle to be solved with forensic evidence. Attribution in digital forensics faces some added challenges because of the mythology surrounding cyber capacity. It is important that attackers are not allowed to operate with an expectation of anonymity. This anonymity is a myth; even if the attribution problem cannot be solved, it can be managed.

Attribution problems are fundamentally different to those of cyber security. The large scale of connected industry and infrastructure can be seen as a vulnerability – an expansive attack surface – but developed nations have the advantage of resources for identifying and concealing cyber operations. Further, the pressure for constant precision is transferred from the defender to the attacker, as a single mistake can be sufficient for attribution. The quality of attribution is a function of the available time, available resources and the adversary's sophistication. But attribution is not just a question of traces revealed in technology. Like any investigation, there are pressures to maintain reputations and affiliations on a larger scale. Investigating cyber attacks fully requires coordinating multiple specialties, proceeding through judicial levels, and prevailing in legal proceedings against competing evidence.

Rid and Buchanan developed the 'Q Model' to illustrate the complexity of the process of attribution. This model collects the aspects of an investigation into a unified framework, which provides context and shape, as well as a checklist of things to watch for in investigations. The model distinguishes three levels of analysis, as shown below.



The 'Q model' (simplified)

Each level relies on different sources of information for analysis, but success depends, in part, on strong communication between the levels. The degree of uncertainty and use of assumptions with judgment may increase as analysis moves away from the tactical and technical level.

This model can be applied in practice across many levels of an investigation. It is important to

- Ensure there is significant capacity to draw on multiple sources of information for attribution, including forensic analysis of the clues left behind by intruders. This technical task, and all levels of the attribution process, need experts with the right skills, time to investigate.
- Understand that attribution involves various levels of analysis, and each needs to understand how they fit in a bigger picture.
- Recognize attribution is not just a technical exercise but a political and strategic balancing of available resources against perceived risk.
- Be aware of expectations about attribution exercises. Balance the detail provided in messages, whether communicating among levels or out into the public; provide what is significant and useful without being overwhelming.

The Q Model emphasizes the need to question the results of an investigation or attribution process. This safeguard is built in, with communication between the levels. Communication also extends beyond the layers of the investigation to the surrounding space; law enforcement tend towards secrecy, but communicating with stakeholders can increase credibility, enhance the quality of the outcome, and strengthen defenses. This is with the clear caveat that any communication must emphasize the gradual nature of the attribution process and the degree of uncertainty that remains.

Attributing cyberattacks is a complex art that combines technical, operational and strategic level investigations with managed communications in a delicate process over time.

Rid, T., & B. Buchanan. (2015). "Attributing Cyber Attacks." Journal of Strategic Studies 38 (1-2).

Anti-Forensics: A Practitioner Perspective

Forensics is the science of investigating artefacts and interpreting their relevance to an investigation. Increasingly, the evidence used in forensic investigations is digital. With the proliferation of electronic devices, digital evidence can be relevant in a wide variety of criminal investigations, to identify an attacker or their actions, as well as identify how and why they perpetrated the alleged crime. Judicial processes rely on the expertise of Digital Forensics investigators for the proper collection and analysis of digital evidence. Fragile by nature, digital evidence can be easily altered, sometimes without any trace. When done intentionally to hide or destroy evidence, this act is known as anti-forensics (AF). Often Anti-Forensics activities are carefully hidden and many may remain undiscovered, so the full impact of Anti-Forensics on investigations is unknown. Before a Digital Forensics practitioner can fully evaluate the impact of Anti-Forensics activity on an investigation, they must first detect the tampering.

The study by de Beer et al. surveyed 35 South African Digital Forensics practitioners to establish the extent and impact of Anti-Forensics activity on investigations. They found several factors that influence Digital Forensics practice:

- Degree of implementation

Digital Forensics investigators place a high importance on Anti-Forensics, for the contribution to judicial proceedings, but most do not always employ significant efforts to identify Anti-Forensics activity in their investigations.

- Level of knowledge

Digital Forensics investigators know about some common Anti-Forensics techniques and tools – such as data hiding, data destruction, and encryption), but are less familiar with more complex Anti-Forensics methods, like data contraception, trail obfuscation, and data fabrication. Practitioners report that the better-known methods are the ones impacting forensic cases. However it is unclear if this is because they have the greatest impact or because these are the methods that are most well-known and are hence more often detected.

- Training, experience, and confidence

There is a connection between participation in Anti-Forensics training and a respondents rating of their own knowledge of Anti-Forensics tools and techniques. Those Digital Forensics practitioners who have training are more likely to rate their knowledge as good or excellent. Also, Digital Forensics practitioners with two or more years on the job rate their own abilities with Anti-Forensics as higher than those with less experience.

This study highlights the need for specific Anti-Forensics knowledge and skills development as a component of Digital Forensics training. Greater fluency with Anti-Forensics tools and techniques might broaden the tools for counter-Anti-Forensics work by Digital Forensics investigators, as well as enhancing their confidence and efficacy.

Digital Forensics Investigators take anti-forensics techniques seriously but only the ones they know well. Formalised implementation of anti-forensics detection and training and mentoring on countering techniques could improve investigations.

Van Belle, J. P., de Beer, R., & Stander, A. (2015). "Anti-Forensics: A Practitioner Perspective." International Journal of Cyber-Security and Digital Forensics (IJCSDF), 4(2).

SERENE-RISC Six Key Activities

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

The latest developments and upcoming activities for each of the six key activities is shown below.

The SERENE-RISC Quarterly Cybersecurity Knowledge Digest

2015 Spring

Editor-in-Chief Michael Joyce; **Editor** Emily Maddocks; **Scientific Editor** Benoît Dupont

To receive the latest issue and access back issues apply for a free membership at info@serene-risc.ca