serene • risc

Digest

Autumn • 2015

Cutting Edge Research Summaries for Policy-Makers and Practitioners

What do security experts and novices do and think differently ?

Most computer users are aware of online security threats, but their lack of expertise in computer security leads them to rely on advice. While most users take precautions to protect themselves from attackers, the practices they employ might not be effective and don't match the practices used by experts who understand computer security in greater detail. Ion et al. studied this issue by conducting a survey of security experts and non-experts to determine the security practices that they follow and deem effective. While both groups agree that using strong passwords is an effective security practice, results show that there is a significant difference between their views on other practices. Organizations and experts who are trusted to provide sound security advice need to ensure that their advice is up-to-date and effective against current malware.

What is private and personal information to a transparent government?

Governments have ever-increasing capabilities for data collection and analysis. Also increasing are expectations for public access to that data. This move toward open government brings new opportunities for open data and proactive disclosure, beyond the traditional and post-hoc access to information requests. This heightens tensions between the competing principles of privacy and transparency. Underlying the complexity are a few key issues, principally recognizing personal information and understanding transparency. To support transparency, shared data must be accompanied by metadata and support for users to determine appropriate use. Government organizations need guidance on effective ways to make decisions about releasing data, as well as guidance on communicating about their disclosure decisions with clear explanation of expected benefits.

How do we regulate privacy in the Internet of Things?

In the current age of connectivity, more information is collected by technologies than most people are aware. Cunningham posits that privacy legislation has not kept pace with the circumstances created by new technologies; as a result, people and their privacy are left unprotected. In the current paradigm, legislation presumes to control how information is collected; what sort of information and by whom. As privacy legislation for the current context, the EU Directive is "at once fatally over-inclusive and under-inclusive." Instead of scrambling to control collection, the rules that protect personal privacy should focus on reducing harms from the use of that information. Legislation should be based instead on limiting the potential risk of harm from the use of data. In this paradigm, use of data would be considered in context for the likelihood and severity of impact on the individual.

My pacemaker has Wi-Fi, what could possibly go wrong?

Implantable Medical Devices (IMDs) are electronic devices inserted into the body to treat, monitor or improve the function of a body part. The wireless communication capabilities in IMDs and the development of Intra Body Networks (IBN) of medical devices present new security risks and challenges. Carmen Camara, Pedro Peris-Lopez, Juan E. Tapiador present a survey of security and privacy issues in IMDs. Providing security for IBNs present additional challenges, as an IMD must operate under two different modes: normal and emergency. Security solutions become more complex because of the need to manage the severe restrictions on the use of energy, storage, and computing power. The trade off and tension between solutions mean that the optimal choice is not certain. The computer security industry has to be ready to provide robust solutions at the design phase and avoid the develop-then-patch approach currently utilized in other devices.

Can organizations do more to prepare their Security Incident Responders?

The current challenge of Advance Persistent Threats (APTs) requires cyber incident handlers to make decisions every day that can have real strategic impact on companies. Yet, they are poorly equipped to make such strategic decisions. Lemay, Leblanc and De Jesus argue that cyber incident response is undergoing a shift in operating environment that is similar to that experienced by modern militaries. Military forces have increasingly been called upon for operations besides combat. The new reality is a frontline "Strategic Corporal" making decisions that consider operational, tactical and strategic realities. Cyber security professionals also face dynamic and time critical decision-making scenarios securing company assets and operations. In many ways, cyber incident handlers are thrust into the role of "Strategic Corporal" whether they are adequately prepared to be so or not. Cyber incident handlers need to be provided with the tools to tackle the challenges introduced by this strategic reality. The solutions put forward for similarly dynamic management environments – training, communication skills awareness, decentralized vision and purpose achieved through decentralized decision making – provide suitable avenues to make cyber incident responders ready to meet current challenges.

Can my phone hear my password?

The capability of audio hardware in mobile devices is improving and supporting higher definition sound. In particular there has been a great improvement in recording and digitization hardware and the use of microphone arrays for stereo recording and noise cancellation. Liu et al. explored the question of keystroke snooping and show the feasibility of keystroke snooping with a technique that works without prior training of the device, established context and is based on a single phone. The researchers developed a method that exploits the geometry-based information and unique acoustic signatures of keystrokes to pinpoint their positions on a keyboard. The attack is currently only possible with the few mobile devices that expose stereo recording and have large microphone separation. Even at future higher audio sampling rates there is still only a moderate chance of accurately capturing a long password on the first attempt.

When professionals need to offer confidential communications, can they do it?

Security weaknesses in the information and communications technologies, while enhancing the communications between individuals, have also increased the risk of a violation of confidentiality of communications. This has put professionals that require such confidentially for the performance of their trade at risk. McGregor et al., conducted interviews in both the United States and France to investigate computer security practices and needs of journalists from a computer security perspective. 15 journalists from a range of well-respected institutions participated in the study. The organization is able to play a crucial role in the understanding and competent implementation of communications security and related behaviours of professionals. However this is only part of the problem, professionals make decisions on how to communicate on the level of comfort their client has with securing technologies. Ensuring the confidentiality of these forms of communication requires a greater security awareness and competence of the wider public.

Why does phishing still work?

Phishing is an ever-present threat. A new study evaluates the effectiveness of recent modifications in browser design that assist users to identify fraudulent websites. The interactions of participants were recorded with the help of eye tracking. This study reveals that a decade of user education and browser security indicators enhancements has improved detection rates by a mere 6%. Even in this best-case scenario where users were asked to identify fraudulent websites the success ratio was only 53%.

The most efficient phishing detection strategy was a combination of using a search engine and brute forcing website functionality. But these strategies require users to prioritize security in real world use. Regardless of their use security indicators provide a poor solution, as fake websites are able to satisfactorily imitate indicators of security. In absence of reliable indicators and tools, users should not be entrusted with detecting phishing attacks and we should look towards more automated phishing detection.

How good are malware detectors for Android devices?

The growing use of the Android platform has been accompanied by an increase of mobile malware. Anti-virus software forms part of the effort to overcome malware on mobile devices. However, the effectiveness of anti-virus programs is under question. Statistical investigation provides a first step to show the state of the art in anti-virus solutions for the mobile application ecosystem to identify the current gaps and issues. Allix et al. analyzed a set of both benign applications and malware in Android ecosystem that were developed over the last few years and downloaded in 2014.

The results show that no single antivirus product can identify all existing malware. In active app markets the scanning results show that only a small subset of malware were recognized by a majority of anti-virus software. There is a huge need for more consistent and stronger anti-virus products since the large number of anti-virus products evaluated showed little agreement on detection in a real world environment. If malware is developed in mass produced batches from an industrial process as this study suggests, the detection industry has to improve the general standard of detection.

Does Geopolitics matter in the borderless cyberspace?

The myth of the borderless cyberspace is simply not true. The omission of the geopolitical dimension of cyber power limits our understanding of the struggles and attacks in this space between countries around the world. Cyberspace is inextricably linked to a geographic setting, because the underlying infrastructure is physically based somewhere. The system that supports online actions is owned and regulated by an existing international power. Using a geopolitical framework can help identify the motivations underlying cyber attacks between countries and enable decision-makers to respond more effectively. Assessments of the possession or application of power revolve around the questions of ‘who’, ‘why’ and ‘how’. Establishing ‘where’ is still often the key to answering these questions for cyber security.

"...no one can hack my mind": Comparing Expert and Non-Expert Security Practices

Most computer users are aware of online security threats, but their lack of expertise in computer security leads them to rely on advice. This advice can vary greatly, causing confusion among the general public regarding how they should best protect themselves online. Additionally, users often ignore or circumvent these safeguards if they are time-consuming or require a great deal of effort, which leaves them vulnerable to attack.

Ion et al. studied this issue by conducting a survey of security experts and non-experts to determine the security practices that they follow and deem effective. While most users take precautions to protect themselves from attackers, the practices they employ might not be effective and don't match the practices used by experts who understand computer security in greater detail. Furthermore, while experts may consider some practices more effective than others, there is still a question of whether users will actually comply with them.

A two-stage survey was conducted to determine the security practices that are deemed most effective and to investigate whether these practices are actually followed. In the first stage, researchers interviewed security experts who each have at least 5 years of experience working in computer security. These interviews determined the top 3 pieces of security advice they would give to a non-tech-savvy user and the responses were used to generate questions for the second stage. An online survey was then conducted of 231 security experts and 294 non-experts, posing the question: "What are the 3 most important things you do to protect your security online?" A variety of additional questions were also asked to determine their views on common security practices and whether they employ these practices in their everyday computer usage.

While both groups agree that using strong passwords is an effective security practice, results show that there is a significant difference between their views on other practices. The most commonly mentioned practices by experts were the least common among non-experts and vice versa. The discord between the security practices of experts and non-experts suggests that there is significant room for improvement when providing security advice and that most users are not as safe against online attacks as they may think, despite their precautions.

Top Security Practices from Experts		Top Security Practices from Non-Experts	
Practice	Non-Expert View of Practice	Practice	Expert View of Practice
Install updates	Distrust in update mechanism; Reluctance to introduce changes	Use antivirus	Simple to use; Not useful against sophisticated malware
Use password manager	Distrust in password software	Visit only known websites	Not realistic

Organizations and experts who are trusted to provide sound security advice need to ensure that their advice is up-to-date and effective against current malware. It is important to consider the benefit vs. effort ratio to ensure that their recommendations provide the most security benefits without requiring great effort on the part of the user. Security practices are not practical if users do not trust them or do not find them usable. In addition, those creating security tools need to account for usability and user trust when designing their software to increase adoption by the general public.

Security experts need to better identify practical best practices for their users and the general public.

Ion, I., Reeder, R., & Consolvo, S. (2015). ,"no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In Symposium on Usable Privacy and Security (SOUPS) (pp. 327-346).

Promoting Transparency while Protecting Privacy in Open Government in Canada

Governments have ever-increasing capabilities for data collection and analysis. Also increasing are expectations for public access to that data. This move toward open government brings new opportunities for open data and proactive disclosure, beyond the traditional and post-hoc access to information requests. This heightens tensions between the competing principles of privacy and transparency. In Canada there are no provincial or federal legislative frameworks to address this balance.

To question the current balance, Conroy and Scassa examine a Supreme Court of Canada decision. In the case in question, a journalist requested disclosure of edited information from the Ontario Sex Offender Registry of the Ministry of Community Safety and Correctional Services. The request was denied by the Ministry, which adjudicated and then appealed all the way to Supreme Court. In each ruling, the decision was to release the data.

The case unfolded over several years, with intricate arguments elaborated by Conroy and Scassa. Underlying the complexity are a few key issues:

Recognizing personal information

Based on the principle of identifiable data as personal (and therefore protected from release) the court required evidence of identifiability in the same circumstances and with the same type of information; a generic presentation of the risk was insufficient. This may not adequately weigh a number of realities of the current data context: the rapid growth in the number of data sources; the number of sources that are not publicly available or even known to the public; changes in technology to manipulate data; and the growing potential to identify data that was previously thought to be anonymized.

Understanding transparency

Transparency is often used as a rationale for releasing information, although not often with a clear explanation of whether transparency is a reasonable goal. For example, when data is released to be used for other purposes, such as research, or to inform the public, there is no guarantee that the data will improve the public's understanding. To support understanding, data must be accompanied by metadata that explains the parameters and limitations of the information.

This case points to guiding principles that may support this balancing in future:

1. The concept of transparency that is part of the balance must be nuanced and meaningful;
2. Re-identification risks should be assessed with regard to the big data context into which the data will be released;
3. Although de-identified data may offer a compromise between transparency and privacy, consideration must be given to whether the data remains meaningful after deidentification;
4. To maximize the potential benefits of releasing quality data accompanied by appropriate metadata, steps must be taken to improve not just digital literacy, but also data literacy.

Legislation must recognize the open government shift from access to information in response to pointed requests to proactive disclosure and open data. In this context, government organizations need guidance on effective ways to make decisions about releasing data, as well as guidance on communicating about their disclosure decisions with clear explanation of expected benefits. To support transparency, shared data must be accompanied by metadata and support for users to determine appropriate use.

Responsible transparency isn't possible when practical privacy is opaque. Expert-led, risk-based, privacy aware disclosure decison-making is needed to manage the balance.

Scassa, T., & Conroy, A. M. (2015). Promoting Transparency While Protecting Privacy in Open Government in Canada. Alberta Law Review, Forthcoming.

Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming

In the current age of connectivity, more information is collected by technologies than most people are aware. Devices capture everyday movements and actions, often without the knowledge of those being observed, and these seemingly discrete data can be combined in a way that make anonymity a myth. The location capabilities of smartphones and other GPS devices are well known, but we seldom consider what library books, smart meters, and traffic cameras reveal about personal life. This data flows internationally and information has become a high value in industry.

Cunningham posits that privacy legislation has not kept pace with the circumstances created by new technologies; as a result, people and their privacy are left unprotected. In the current paradigm, legislation presumes to control how information is collected; what sort of information and by whom. The example used to illustrate this point is Directive 95/46/EC of the European Parliament (the Directive) and 2014 Regulatory Amendment. The EU Directive relies on a broad definition of personal information and requires consent from an individual before it is permissible to collect their personal information; the Directive doesn't even broach the phenomenon of data collected without individual's knowledge. With the threat of exclusion from EU markets for noncompliance, the Directive restricts transfer of personal information to entities that comply. The international reach of the legislation is a strength. However the Directive includes some innocuous information and harmless purposes while leaving notable gaps; for example, exceptions can be made for national security, permitting national governments to collect and use personal information seemingly without limits. Further, a safe harbour provision sets a lower standard for compliance by US firms, one that is voluntary and largely unenforced. As privacy legislation for the current context, the EU Directive is "at once fatally over-inclusive and under-inclusive."

The experience of the EU Directive suggests an alternative approach to regulation. Given the extent of passive information collection, the requirement for individuals to consent is impractical; so too are limits on the myriad forms of data collection. Legislation should be based instead on limiting the potential risk of harm from the use of data. In this paradigm, use of data would be considered in context for the likelihood and severity of impact on the individual. Implementation would be incremental, starting with the greatest risk or known violators.

It is important to recognize that, when combined, even the most trivial data can be personal. Widespread collection of that personal information – without consent – is probably here to stay. Instead of scrambling to control collection, the rules that protect personal privacy should focus on reducing harms from the use of that information. This risk management approach could be used both in legislation and in corporate policies on information

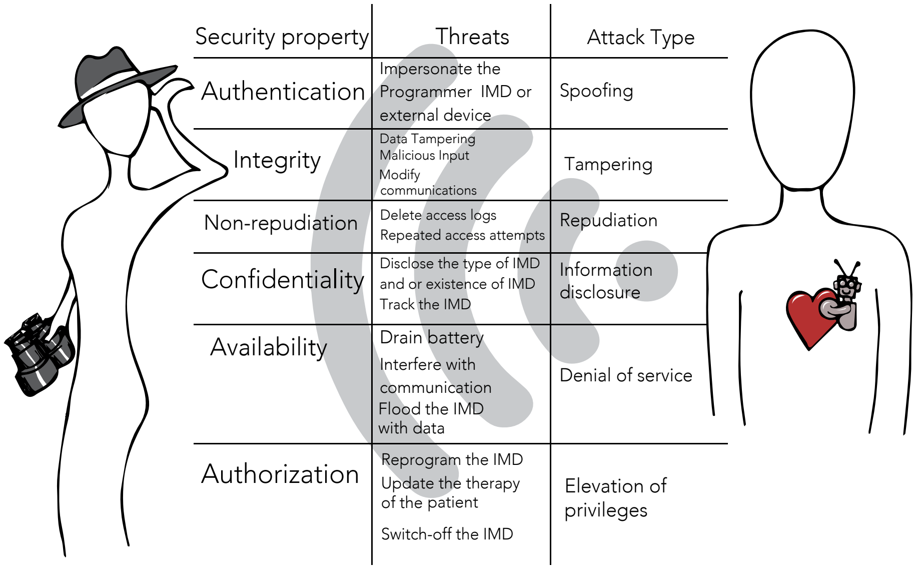
Focusing on the harm of a privacy breach is a better guide for regulation of data flows in the Internet of Things

Cunningham, M. (2015). Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulation by Risk of Harm. Groningen Journal of International Law, 2.

Security and privacy issues in implantable medical devices: A comprehensive survey

Implantable Medical Devices (IMDs) are electronic devices inserted into the body to treat, monitor or improve the function of a body part. IMDs can monitor part of the body and electrically stimulate organ function such as the brain and heart. Drug Delivery Systems (DDS) supply medication in a controlled, localized, and prolonged way. New IMDs have started to incorporate more advanced communications and computing capabilities to reduce cost and provide new diagnostic and treatment capabilities to healthcare providers. The wireless communication capabilities in IMDs and the development of Intra Body Networks (IBN) of medical devices present new security risks and challenges. Besides the magnification of existing threats to wireless networks such as eavesdropping and unauthorized data or operation access or modification, the mere existence of an IBN means the implant is no longer "invisible", as its presence could be remotely detected breaching the patient's privacy.

Carmen Camara, Pedro Peris-Lopez, Juan E. Tapiador present a survey of security and privacy issues in IMDs, discuss the most relevant mechanisms proposed to address these challenges, and analyze their suitability, advantages, and main drawbacks. Providing security for IBNs present additional challenges, as an IMD must operate under two different modes: normal and emergency. Under normal operating conditions an IMD must ensure the security of its operation and preserve the privacy of the patient. Nevertheless, during an emergency the medical personnel must be able to access the implant rapidly and without restrictions.



Security property	Threats	Attack Type
Authentication	Impersonate the Programmer IMD or external device	Spoofing
Integrity	Data Tampering Malicious Input Modify communications	Tampering
Non-repudiation	Delete access logs Repeated access attempts	Repudiation
Confidentiality	Disclose the type of IMD and or existence of IMD Track the IMD	Information disclosure
Availability	Drain battery Interfere with communication Flood the IMD with data	Denial of service
Authorization	Reprogram the IMD Update the therapy of the patient Switch-off the IMD	Elevation of privileges

IMDs have limitations on how security is implemented due to the severe restrictions on the use of energy, storage, and computing power. These limitations are strict as device failure or even communication latency due to security controls puts the patient's safety at risk. Managing the trade-off between safety and security is critical in the design of IMD security mechanisms. Security solutions are more complex because of the need to manage these practicalities.

Auditing, a basic security provision for recording events on a device, requires additional processing and storage either on the device or via an external device. It is also possible for an external device to control access to the IMD based certificates and lists, blocking or jamming unauthorized accesses. While the external device may overcome the resource limitations of the IMD they introduce complexity, make emergency access more difficult and are not totally effective. Communication channel and authentication processes could be abused to produce a Denial-of-Service attack or to deplete battery and memory resources; as a Resource Depletion (RD) attack. Solutions such as encryption are also resource expensive and do not prevent these attacks. The existing research on RD attacks in sensors networks are not directly applicable to IMDs since implants have more severe resource restrictions. Other security options such as proximity based controls, either using bounding protocols or switching though subcutaneous buttons or magnetic switches. Another option is the introduction of an IMD hub for managing extra-personal communications and security.

However, it is important to remember that these devices are implemented within a human body. Adding resources or hardware to improve security requires invasive surgery. Adding complexity and embedded software increases the risk of device failure and human injury.The trade off and tension between solutions means that the optimal choice is not certain. What is clear is that the design of security for IMDs requires careful consideration of the patient. The computer security industry has to be ready to provide robust solutions at the design phase and avoid the current develop-then-patch approach to security.

IMD security is hard and we don't seem to be ready to implement meaningful security.

Camara, C., Peris-Lopeza, P., & Tapiadora, J. E. (2015) Security and Privacy Issues in Implantable Medical Devices: A Comprehensive Survey.

Lessons from the Strategic Corporal - Implications of Cyber Incident Response

The current challenge of Advance Persistent Threats (APTs) requires cyber incident handlers to make decisions every day that can have real strategic impact on companies. Yet, they are poorly equipped to make such strategic decisions. The mismatch between the strategic decision-making and communication models of companies and the real-world needs of cyber incident handlers is not sustainable.

Lemay, Leblanc and De Jesus build up an argument that cyber incident response is undergoing a shift in operating environment that is similar to that experienced by modern militaries. They believe that the solutions put forward by the military could be transferred to the cyber-security context, to resolve the strategic incident responder problem.

Military forces have increasingly been called upon for operations besides combat such as peacekeeping and providing humanitarian aid. Because the nature of operations can change drastically, in a very short time and require different responses in a small area, troops need to be equipped for the entire spectrum of operations. Further, the quick decisions made at the front line can have a big impact on overall strategy and the organisation as a whole. A stiff decision-making hierarchy and strict delineation of roles would make it difficult to operate effectively in this environment. The new reality is a frontline "Strategic Corporal" making decisions that consider operational, tactical and strategic realities, a task usually distributed vertically through the organisations' structure.

Cyber security professionals also face dynamic and time critical decision-making scenarios securing company assets and operations. They are often operating within organizations that are vertically hierarchical and role restrictive, like a traditional military. The greater number of high impact incidents such as those involving APTs have increased the strategic impact of technical decisions. The extremely time sensitive nature of cyber security and the adversarial nature of the incident response process makes it impossible to wait for management input. Technical personnel also often have difficulties communicating the strategic implications of highly technical problems to management. In many ways, cyber incident handlers are thrust into the role of "Strategic Corporal" whether they are adequately prepared or not.

Cyber incident responders who make strategic decisions need to be well equipped to respond appropriately and in line with organizational strategy. Role specialization can hinder communication and consequently limit decision-making. The table below puts forward three solutions to counter the strategic incident responder problem.

Solutions for the Strategic Incident Responder Problem

Training	Mission Command	Decentralized Decision Making
Invest resources to train technical employees for them to gain real strategic understanding of the company's business environment	Improve methods used by managers to communicate Instructions must be clear and open-ended. Employees must be able to adapt for the realization of the job to the reality of the ground	Reorganize decision making to a decentralized process, but keep the unity of purpose obtained through centralized command and control.

Cyber incident handlers need to be provided with the tools to tackle the challenges introduced by this strategic reality. The solutions put forward for similarly dynamic management environments – training, communication skills awareness, decentralised vision and purpose achieved through decentralized decision making – provide suitable avenues to make cyber incident responders ready to meet current challenges.

Cyber Incident handlers are making strategic decisions for your firm. Training, improved communication and decentralized decision-making structures will help them do it right.

Lemay, A., Leblanc, S. P., & De Jesus, T. (2015). Lessons from the Strategic Corporal: Implications of Cyber Incident Response. In Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research (pp. 61-66). ACM.

Snooping Keystrokes with mm-level Audio Ranging on a Single Phone

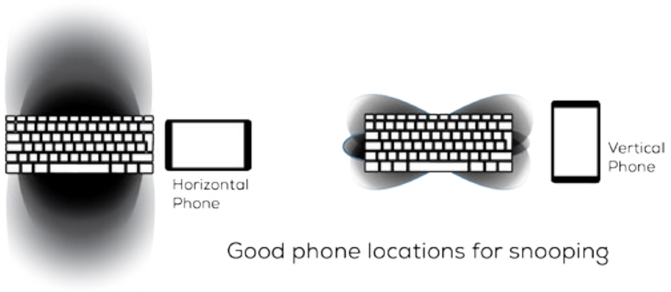
The capability of audio hardware in mobile devices is improving and supporting higher definition sound. In particular there has been a great improvement in recording and digitization hardware and the use of microphone arrays for stereo recording and noise cancellation. These advancements could have an impact on the feasibility of ranging and localization by mobile hardware, in particular for eavesdropping and keystroke detection. To listen in on and detect keystrokes an adversary could add malware into an app with microphone access and wait until the phone is placed near a keyboard, or leave a phone near a keyboard of the target. In the past, research has found limited possibility of keystroke snooping using mobile device microphones however the increasing use of multiple microphones on these devices creates new potential.

Liu et al. explored the question of keystroke snooping and show the feasibility of keystroke snooping with a technique that works without having trained the device or established context in advance. Prior techniques that relied on training the device to recognize the sound of typing required context specific data and so not needing this data is important because of the difficulty involved in obtaining this data. This was achieved by focusing on acoustic ranging techniques based on time-of-flight measurements, or the calculation of a source point based on the difference in time of sound detection at two fixed points.

They tested their method with a Samsung Galaxy Note 3 mobile device and a laptop with a pair of microphones; to simulate a potential future phone with improved audio sampling capability. Audio sampling capability, or the number of times per second that a device can collect and process sounds is of particular importance as it directly affects accuracy of keystroke detection. The method was tested with a Microsoft Surface keyboard, an Apple wireless Keyboard and a Razer Mechanical Keyboard to assess its effectiveness with keyboards of differing form factors and key noise levels.

A current model phone can discover passwords without training by exploiting mm-level acoustic ranging and fine-grained acoustic features. The researchers developed a method that exploits the geometry-based information and unique acoustic signatures of keystrokes to pinpoint their positions on a keyboard. The accuracy and precision of this system depends on several key factors notably the Sampling Rate, the Distance between the Microphones and the Placement of the Mobile Device.

At the 48kHz sampling rate commonly found in mobile devices at the moment it is possible to accurately identify keystrokes with over 85% accuracy or from 3 candidates at 97% accuracy. This increases to as high as 94% with a higher sampling rate of 192kHz, which is possible in future devices. This distance between microphones is important as greater distances between microphones allow greater accuracy, larger portable devices making this technique feasible. The placement of the device relative to the keyboard also is significant, with a relatively small range of locations being useful to an attacker.



Good phone locations for snooping

The attack is currently only possible with the few mobile devices that expose stereo recording and have large microphone separation. Even at future higher audio sampling rates there is still only a moderate chance of accurately capturing a long password on the first attempt. Even so it still does allow the discovery of a small set of password candidates that can then be brute-forced. The research does highlight the difficulties of security in a sensor dense environment and raises the point that limited access to multiple microphones and higher sampling rates be prioritized.

Improving mobile hardware makes acoustic password detection possible, but not practical. Sensor dense environments require extra awareness to ensure security against snooping.

Liu, J., Wang, Y., Kar, G., Chen, Y., Yang, J., & Gruteser, M. (2015). Snooping Keystrokes with mm-level Audio Ranging on a Single Phone. In Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (pp. 142-154). ACM.

Investigating the Computer Security Practices and Needs of Journalists

Information technologies have enhanced communications between individuals, but have also increased the risk of a violation of confidentiality. This has put professionals that require such confidentially for the performance of their trade, such as journalists, doctors, researchers and lawyers, and their sensitive clients at risk. The computer security community needs to have a better understanding of the practices, needs and constraints of these professionals. This will allow the development of security tools that can fully protect the sanctity of confidential practitioner to client communications.

McGregor et al., conducted interviews in both the United States and France to investigate computer security practices and needs of journalists from a computer security perspective. Security issues that are apparent in communications between journalists and their sources are likely to be applicable more widely. This would include communications between lawyers and their clients, doctors and their patients, government departments and members of the public, researchers and study participants and so on.

15 journalists from a range of well-respected institutions participated in the study. Working with a small group allowed the authors to conduct in-depth, semi-structured interviews. The interviews focused on the general practices, security concerns, defensive strategies and unfilled needs regarding security technology of the participants.

The study found that the professionals made use of non-technical defensive strategies, such as physically mailing digital data and ad-hoc defensive strategies, like code names or intermediaries. Those who did employed technical strategies, such as disk encryption, did so sporadically and reported requiring an extended amount of time before being comfortable with them. The professionals stated that anonymous security tools interfere with the process of authentication of sensitive clients. Alternatively, not using security tools puts them at risk, because of the recording and auditing inherent in modern communications; such as metadata trails. Also, clients often determine the communication method used by professionals. As they often do not have the technical knowledge or access to computer security technologies, especially if they are part of more vulnerable populations, a lower levels of security is required. The professionals also mentioned that they lack secure systematic management tools and secure technical support for transcription purposes. The organization employing these professionals also appeared to play an important role in influencing their security behavior.

Recommendations for the Computer Security Community

- Anonymous communication tools should address the issue of authentication of sensitive clients by professionals.
- Effective, usable and transparent solutions to overcome the tracking of metadata trails are needed.
- Security technologies that are accessible to populations with low technical skills or limited access to technology should be developed.
- Improved access to computer security technologies for low-income and vulnerable populations is needed.
- Professionals need a secure and systematic knowledge management system to support the storing, organizing, searching, and indexing story-related data.

The organization is able to play a crucial role in the understanding and competent implementation of communications security and related behaviours of professionals. However this is only part of the problem Professionals make decisions on how to communicate on the level of comfort their client has with securing technologies. Ensuring the confidentiality of these forms of communication requires that the awareness and competence of the greater public is required. Further, professionals are missing secure tools for the collection processing and storage of data. The computer security community could seize these opportunities and fill the voids.

Practical communications security is limited to the level of the least capable. Ensuring that the public can confidently confide in their professionals requires work at many levels.

McGregor, S. E., Charters, P., Holliday, T., & Roesner, F. (2015). Investigating the computer security practices and needs of journalists. In Proceedings of the 24th USENIX Conference on Security Symposium (pp. 399-414). USENIX Association.

Why phishing still works: User strategies for combating phishing attacks

Phishing is an ever-present threat. When users` ability to detect phishing was studied nearly a decade ago the results were worrying. Today, people are more familiar with phishing attacks. Improved web browsers help prevent phishing by providing security indicators such as the SSL lock, security certificates and warnings.

Alsharnouby, Alaca and Chiasson evaluated the effectiveness of recent modifications in browser design that assist users to identify fraudulent websites. They also investigated whether users have developed improved detection strategies and mental models of phishing. The researchers examined human behaviour, in particular what the user looked at and for how long, with a device that measures eye movements and infers the point on the screen that the user is looking at based on reflection from eyes. This was the first study that used eye-tracking data to identify the security indicators that captured attention of users determining the legitimacy of websites.

The 21 study participants were first emailed a pre-session questionnaire to collect information to tweak the test websites. They then took part in an in-lab session examining 24 websites. They had to judge whether each website was genuine, say why and how sure they were. The interactions of participants with each website, captured with eye-tracking data, along with the time taken to judge, were recorded. Finally, a semi-structured interview was held to understand the participants' mental models, knowledge and experiences. The findings were made more reliable by combining the data collection on the decision-making processes of users and their eye gaze on security cues. For example, one participant stated that they rely on the URL indicator to decide the safety of a website, while the eye tracking data showed otherwise. A decade of user education and browser security indicators enhancements has improved phishing detection rates by a mere 6%. Security is usually a secondary task for everyday users. Even in this best-case scenario where users were asked to identify fraudulent websites, making security their primary task, only 53% of participants were successful. Further, participants frequently identified forged websites with faulty reasoning. For example, a website was identified as fake based on outdated content, however it was an exact copy of the current website. Users` phishing detection strategies, in order of popularity can be categorised as: evaluating website content, brute-forcing website functionality by testing site for completeness, paying attention to the URL, using a search engine to verify, and relying exclusively on SSL.

The most efficient phishing detection strategy was a combination of using a search engine and brute forcing website functionality. But putting these strategies into practice requires users to prioritize security in real world use. Surprisingly, participants spent less than a minute glancing at the security indicators and the remaining time looking at the easily forgeable contents of the webpage. Furthermore, the presence of security hints grabbed attention but their absence went unnoticed. Even when the users observed the visual cues, they had interpreted them in different ways. This highlights some possible security improvements:

User-friendly URLs - Participants often glanced at the URL but didn't understand it. Confusion caused by URLs showing different domains for different sections of one website could be reduced.

Visual aids for browsing - Phishing websites can link to genuine websites making the determination of safety more complicated. A visual indicator could be created that notifies of a transition from an unsecure to a secure domain. The reverse is already addressed by many websites.

Moving authentication to the web browser - Web browsers should be responsible for essential tasks such as user authentication. This would require collaboration between browser and web developers.

Automate as much as possible - Security indicators are not reliable, which makes the user task of detecting phishing very complicated. Automate as much as possible to reduce complexity and ease the burden on users.

Reliably detecting phishing requires that users prioritize and put effort into security in the real world. Users currently make poor use of security indicators. Even when they are understood by users, these security indicators are a poor solution, as fake websites are able to satisfactorily imitate indicators of security. Under the same conditions, a genuine website displaying genuine security warnings was judged to be fake. Thus, in absence of reliable indicators and tools, users should not be entrusted with detecting phishing attacks and we should look toward more automated phishing detection.

Phishing still happens because users have ad-hoc strategies backed by poor tools. Better tools and more automation is required to make a difference to phishing.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: user strategies for combating phishing attacks. International Journal of Human-Computer Studies.

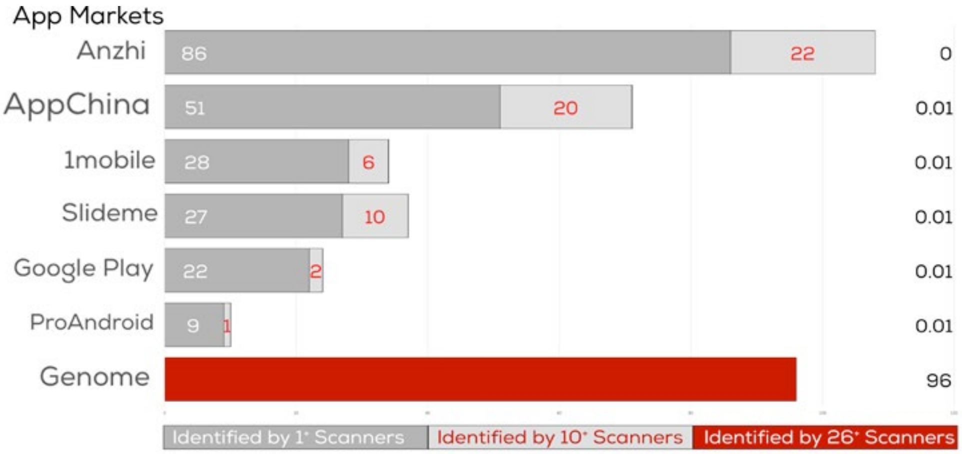
A Forensic Analysis of Android Malware: How is Malware Written and How it Could be Detected?

The growing use of the Android platform has been accompanied with an increase of mobile malware. Malware threats range from simple user tracking and disclosure of personal information to advanced fraud and premium-rate SMS services subscription, or even using the resources of the device for the benefit of an attacker as part of a network (or `botnet`) of infected smartphones. Anti-virus software forms part of the effort to overcome malware on mobile devices. However, the effectiveness of anti-virus programs is in question. Statistical investigation provides a first step to show the state of the art in anti-virus solutions for the mobile application ecosystem to identify the current gaps and issues.

Allix et al. analyzed a set of both benign applications (apps) and malware in the Android ecosystem that were developed over recent years and downloaded in 2014. They collected over 500,000 free Android applications from user markets including the official Google Play and some other unofficial app stores including AppChina, Anzhi, Slideme, FreewareLovers, ProAndroid, F-Droid, and 1mobile. In addition, they collected some apps through Bittorrent and malware from the Genome academic dataset.

These apps were scanned with the approximately 40 antivirus products hosted by VirusTotal, including those from market leaders such as McAfee and Symantec.

The results show that no single antivirus product can identify all existing malware. Only a small subset of widely known malware are recognized by a large number of antivirus software. As shown in the figure below, there is great variation in both the percentage of apps detected as malware and also the agreement between antivirus products on what is malware. From the Genome dataset of known malware, 96 percent of samples were detected as such by more than 25 anti-virus products. However, the scanning results show that only small subset of malware downloaded from active app markets was recognized by a majority of anti-virus software.



The study also examined information on app production, for clues into malware detection. The analysis of packaging dates of applications provides some insight into malware development. It shows that malware development is often a standardized process that aims to produce a large number of malware at once. Moreover, malware writers like other developers, follow a consistent work schedule, suggesting an industrial rather than hobbyist approach to building malware.

The research also studied the developer's digital certificate of each app, assigned before a product is uploaded to an app store. There is no distinct pattern between malware and benign applications, suggesting that studying only the application certificates will not contribute to the detection of malware. There is a clear need for more consistent and stronger anti-virus products, to improve on the low level of agreement in malware detection by existing anti-virus products in a real world environment. If malware is developed in mass produced batches from an industrial process, as this study suggests, the detection industry has to improve the general standard of detection.

Malware production is happening on an industrial scale and our current detection tools are inconsistent and a poor defensive solution to the problem.

Allix, K., Jerome, Q., Bissyande, T. F., Klein, J., State, R., & le Traon, Y. (2014, July). A Forensic Analysis of Android Malware-How is Malware Written and How it Could Be Detected?. In Computer Software and Applications Conference (COMPSAC), 2014 IEEE 38th Annual (pp. 384-393). IEEE.

Geopolitics and Cyber Power: Why Geography Still Matters

The myth of the borderless cyberspace is simply not true. The study of geopolitics allows geographic context to provide an understanding of international political power. However, the Internet appears to devalue this field, based on the assumptions that borders aren't important because conventional notions of time and space don't apply in cyberspace.

Using traditional geopolitical thought, where the domination of a relevant domain is the ultimate goal, Sheldon argues that geopolitical has meaning in cyberspace. He puts forward that virtual space has a geopolitical dimension just like any other strategic domain (i.e. land, sea, air, space). The omission of the geopolitical dimension of cyber power limits our understanding of the struggles and attacks in this space between countries around the world.

Cyberspace is inextricably linked to a geographic setting, because the underlying infrastructure is physically based somewhere (computers, cables, satellites, etc.). Laws, norms and governance structures shape physical territory; each action in cyberspace has a corresponding action in the physical realm. The system that supports online actions is owned and regulated by an existing international power.

Forensics rarely provide solid technical evidence to identity the actors involved in cyber attacks. Understanding the political dimensions of an attack can provide a context to inform investigators and identity the perpetrator. Using a geopolitical framework can help identify the motivations underlying cyber attacks between countries and enable decision-makers to respond more effectively.

Well Sam, Can you think of anyone who might want to steal your data ?

Geopolitics goes far beyond this physical attachment. The physical infrastructure of cyberspace is shaped and influenced by practical geographic imperatives and by powerful geopolitical forces.

The appearance of densely populated megacities like Karachi, Mumbai and Accra is reshaping cyberspace both technically and culturally. New centers of power are emerging from these highly connected, highly concentrated hubs of capacity, content and commentary generation. These centers may affect the relative strength of established powers or the megacities may result in gatherings of cyber activity with their own geopolitical narratives and imperatives.

In practice, geopolitics and cyber power are intimately related. The rise of cyber power isn't a change in the nature of things, but a subtle shift in the character of war and international strategy. For this reason ignoring geopolitics when assessing cyber power overlooks a key element. Assessments of the possession or application of power revolve around the questions of 'who', 'why' and 'how'. Establishing 'where' is still often the key to answering these questions for cyber security.

Cyberspace is full of real people that live in the real world. Geopolitics will provide useful insight into cyberspace for as as long as this is the case.

Sheldon, J. B. (2014). Geopolitics and Cyber Power: Why Geography Still Matters. American Foreign Policy Interests, 36(5), 286-293.Chicago

SERENE-RISC Six Key Activities

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 knowledge brokers' forum, quarterly knowledge digests, Konnect - online knowledge-sharing platform, a public website and a professional development program.

Workshops & Seminars

April 2016
Vancouver
October 2016
Ottawa

Knowledge Brokers

Expanded Access Program

Knowledge Digest

More than 50 Summaries.
Sponsorship Opportunities Available

Konnect

More than 500 hand-selected resources on Cybersecurity including exclusive content

Website

Cyber security tips section , news on the network and Digest Archive.

Professional Development

Ask us about the Graduate Development Sessions

The SERENE-RISC Quarterly Cybersecurity Knowledge Digest

2015 Autumn
Editor-in-Chief Michael Joyce; **Scientific Editor** Benoît Dupont
Editors: Emily Maddock, Masarah Paquet
Sheldon J.B summarised by Anne-Marie Côté sponsored by SERENE-RISC
Allix, K. et al., summarised by Kobra Khanmohammadi sponsored by SERENE-RISC
Alsharnouby, M. et al., summarasied by Kalpana Hundlani sponsored by SERENE-RISC
Ion, I. et al., Summarised by MichelleWong 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