Georgia Institute of Technology

EMERGING CYBER THREATS REPORT 2015

Presented by the Georgia Tech Information Security Center (GTISC) and the Georgia Tech Research Institute (GTRI)

Georgia Tech Cyber Security Summit 2014

Introduction

Over the last year, information and technology have become more tightly intertwined in our lives. The ubiquity of mobile devices has increased citizens' reliance on cloud services to store personal and business data, making them more productive but at the same time, more vulnerable. While phones and tablets have become the most common devices to connect to the Internet, interconnected devices—the so-called Internet of Things—promise to deliver greater control and understanding over our lives, but at the same time raise privacy concerns.

Our reliance on these technologies has left us open to a variety of threats. Cybercriminals continue to compromise users' computers and are increasingly turning their attention to mobile devices. In addition, online thieves have aimed their tools at larger prey, resulting in a string of large data breaches at well-known companies, such as Target, Home Depot, and JPMorgan Chase.

Meanwhile, more countries have made operations in cyberspace part of their intelligence and military strategies. Cyber espionage groups are targeting governments and businesses to steal sensitive information, intellectual property, and increasingly, money itself. The number of governments using the Internet as an easy way to gather information on rivals, allies, and citizens is quickly increasing. Leaks of classified documents describing the data collection by intelligence agencies worldwide have resulted in greater scrutiny of monitoring conducted both by government and private industry.

In light of these events, users of information technology need to be better educated. From malicious insiders to uninformed users, human decisions are often the source of breaches and represent a problem that neither training nor technology alone can solve.

The United States and other countries must continue to invest in research and pioneer technology, processes, and policies that help society deal with these developments. Researchers from academia, the private sector, and government must continue to work together and share information on emerging threats, make improvements to policy, and educate users.

The annual Georgia Tech Cyber Security Summit (GTCSS) on October 29, 2014, provides an opportunity for researchers and stakeholders from different spheres to come together and prepare for the challenges we face in securing cyberspace, critical data, and Internet-connected devices. By hosting the event, the Georgia Institute of Technology aims to support new efforts to develop new technologies and strategies that are effective against sophisticated cyber attacks and create the foundation for a better digital society.

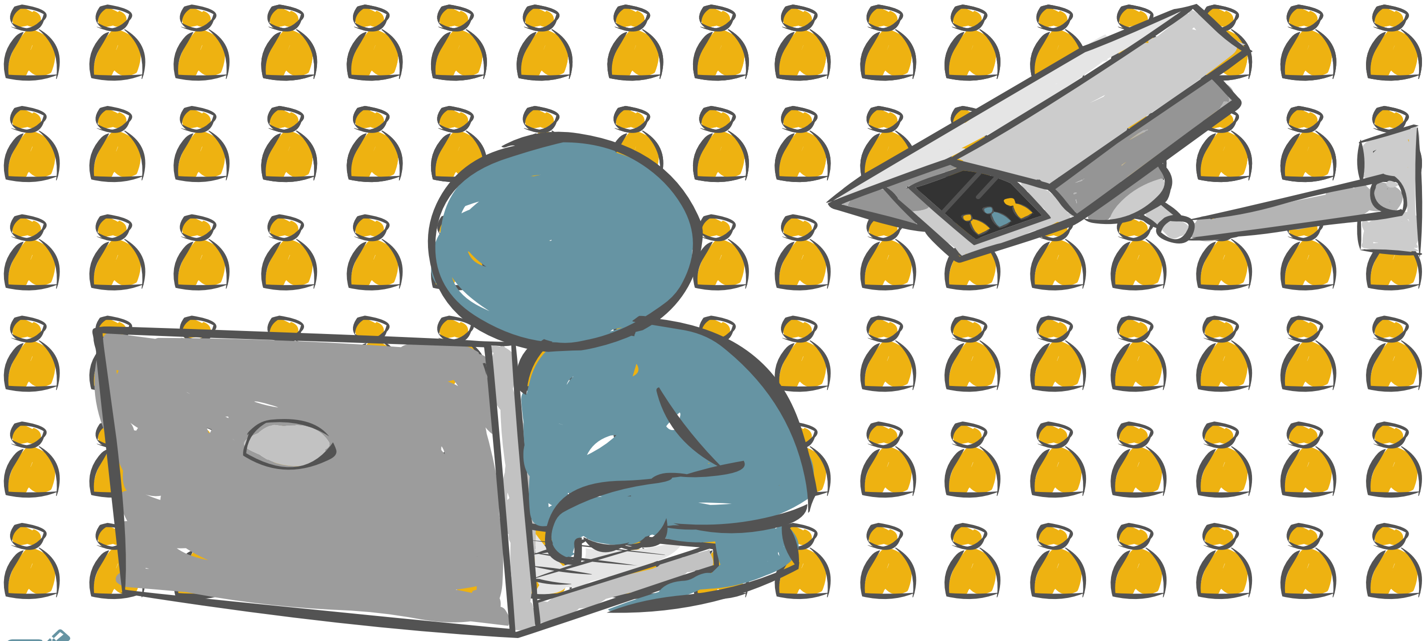
The discussion starts here. As key stakeholders, we all need to cooperate more effectively to combat the emerging threats we face and develop the necessary technologies and policies for a sustainable digital future. As part of fulfilling this need, we have compiled the following Emerging Cyber Threats Report, which includes insight and analysis from a variety of experts from the IT security industry, government, and academia. The Report and the Summit provide an open forum for discussion of emerging threats, their potential impact, and countermeasures for containing them. After the summit, we invite you to learn more about our work in cyber security and connect with our experts to understand and address the challenges we face.

— **Wenke Lee**
Director, GTISC

— **Bo Rotoloni**
Director, Information and Cyber Sciences Directorate, GTRI

Technology enables surveillance, while policy lags behind

Revelations about how nations are collecting data on their populations spurs a frank discussion of privacy, and while policy slowly develops, innovative technologies will fill the gaps



Highlights:

- Leaks about data collection by intelligence agencies, especially the National Security Agency, have created renewed interest in privacy not seen since the 1990s, but developing a comprehensive policy continues to be difficult

- Even without direct government surveillance, a variety of technologies – including social networks and behavioral advertising – allow large online companies to monitor their users

- Encryption could be a solution, but continues to be difficult to use effectively and governments continue to resist its deployment, fearing an inability to gather evidence

- The European Union will likely continue to set the privacy agenda for U.S.-based companies, in the same way that California's data breach notification act affected companies across the country

With the release of classified documents by former National Security Agency contractor Edward Snowden, government surveillance has been cast into the spotlight, turning privacy into a major concern for technology-savvy users and a significant business problem for Internet and communications companies. The exposure of the government surveillance programs has resulted in a growing backlash that will not settle for some time.

The scope and impact of the issues of government surveillance on national policy are difficult to forecast. While privacy-conscious users and technology companies worry over data collection, government officials and security-conscious citizens fear the loss of visibility into the activities of malicious actors. In December 2013, the President's Review Group on Intelligence and Communications Technologies released a 308-page report[RG1] demonstrating the complexity of the issues involved, the often conflicting priorities of the government to both secure its citizens and guarantee their privacy, and the lack of an easy policy that gives government tools to gather intelligence while protecting citizens' privacy.

The leak of classified documents has renewed the debate over privacy — businesses, policy makers, and citizens are now more focused on the relationship between privacy and technology. The list of privacy-impacting technologies is long, from the expansion of the Internet of Things to the collection of online consumer data, says Peter Swire, the Huang Professor of Law and Ethics at the Georgia Institute of Technology's Scheller College of Business, and one of the five members of the President's Review Group on Intelligence and Communications Technologies.

"Every era, a new technology poses a new privacy threat, but the list right now seems longer than usual," he says.

The tug-of-war between security and privacy will continue as government and corporate data-collection practices are scrutinized

The Snowden leaks have caused diplomatic problems for the U.S. government, from giving China ammunition against charges of economic espionage[ST1] to weakening ties with allies[SS1] such as Germany and Mexico. Other nations have been impacted as well, as claims that New Zealand collected data on its populace cast a shadow over recent elections.[RH1]

Greater insight into government monitoring activities has also made many citizens more suspicious of the information-collection practices of Internet and technology companies. In Europe, a number of lawsuits have targeted social media networks and search engines, from the class action lawsuit filed against Facebook[TG1] to a legal ruling against Google that upholds citizens' and businesses' right to be forgotten.[TJ1]

Expect more in the future. Europe's role in setting privacy standards means that U.S. companies are left deciding whether to create two sets of products—one for the United States and one for the rest of the world—or to adopt more stringent privacy protections. Much like how California's passage of a data breach reporting bill led to a trickle, and then a flood, of breach reports, Europe's update of its data privacy directive could result in worldwide changes, says Georgia Tech's Swire.

"U.S. companies can ignore the right-to-be-forgotten ruling about as much as they can ignore the California data breach law, which is to say, not at all," he says.

A lack of pro-privacy policy leaves Internet firms unreceptive to government requests, while technology firms aim to fix policy shortcomings with data security products

The National Security Agency's activities required the active participation of many U.S.-based companies. While some legally resisted government requests, the lack of a public forum for judicial oversight gave companies little recourse but to comply. Following the release of classified documents, Internet and technology firms faced a loss of their customers' trust, especially international clients.[RL1]

Some companies and civil rights groups have focused on policy and legal means to resist the post-9/11 rush to surveillance. Following the Snowden leaks, a number of Internet giants — including Google, Yahoo, and Microsoft — have lobbied for a greater ability to report on requests for information, hoping to gain increased transparency.[GS1] Such firms are more likely to resist government requests for information on users, especially in the form of National Security Letters, which legally prevent companies from informing users of the requests.

Capturing the frustration with the government's activity, Microsoft's General Counsel Brad Smith equated the monitoring activities of government agencies to the ongoing cyber espionage taking place between nations online. "Government snooping potentially now constitutes an 'advanced persistent threat,' alongside sophisticated malware and cyber attacks," he said in a December 2013 policy statement.[BS1]

However, technology excels at finding the gaps that policy leaves behind. A number of technology providers have taken steps to make surveillance harder.

Major Internet companies, for example, have begun encrypting the links between their data centers and e-mail servers, links that had been exploited by the NSA to collect information.[GS2] Apple and Google have improved the encryption of their mobile operating systems to make it more difficult for unauthorized users — whether they are criminals or law enforcement — to access stored data.[TM1]

Other companies are marketing to the privacy-conscious consumer. From secure messaging applications such as Silent Circle and Wickr, to more secure mobile devices such as the Blackphone, innovative technologies will likely continue to offer better ways to stay private.

Privacy policies continue to fail to serve consumers, but machine learning could help

Information-collection policies continue to be a poor way to guarantee consumer privacy. Policies are rarely read, and for good reason — the documents are complex and require the reading level of a junior in college to understand, according to a Georgia Tech and Ohio State University analysis of more than 2,000 privacy policies.[MA1]

Simpler policies would help, and while there are efforts for simplified privacy statements, few incentives exist for companies to clarify their data-collection efforts. Machine learning algorithms could help classify privacy policies and detect those policies that exceed acceptable standards. Initially such technologies will aim to help software engineers comply with regulations and help regulators find bad policies, says Aaron Massey, a postdoctoral fellow in Georgia Tech's College of Computing.

"Most engineers are not going to read hundreds of pages of text, and most regulators are not going to look at every privacy policy," Massey says.

Eventually, the same technology could help consumers gain a better grasp of what companies plan to do with their data.

Mining Privacy Policies to Understand Intent

A 2013 collaboration between Georgia Tech and Ohio State University conducted a large-scale analysis of 2,061 privacy-policy documents, including those from the Google top 1,000 sites and the Fortune 500, to determine what characteristics the documents had in common and what attributes stood out. The research used topic modeling, an artificial intelligence technique that is similar to clustering but does not require the knowledge of a "right" answer. Treating each document essentially as a bag of words, the researchers found what words were common — such as 'data' and 'privacy' — and what words were uncommon — such as 'opt-in'.

"The most common words are interesting in a way, and the more uncommon worlds are interesting in a totally different way," says Aaron Massey, a postdoctoral fellow in Georgia Tech's College of Computing.

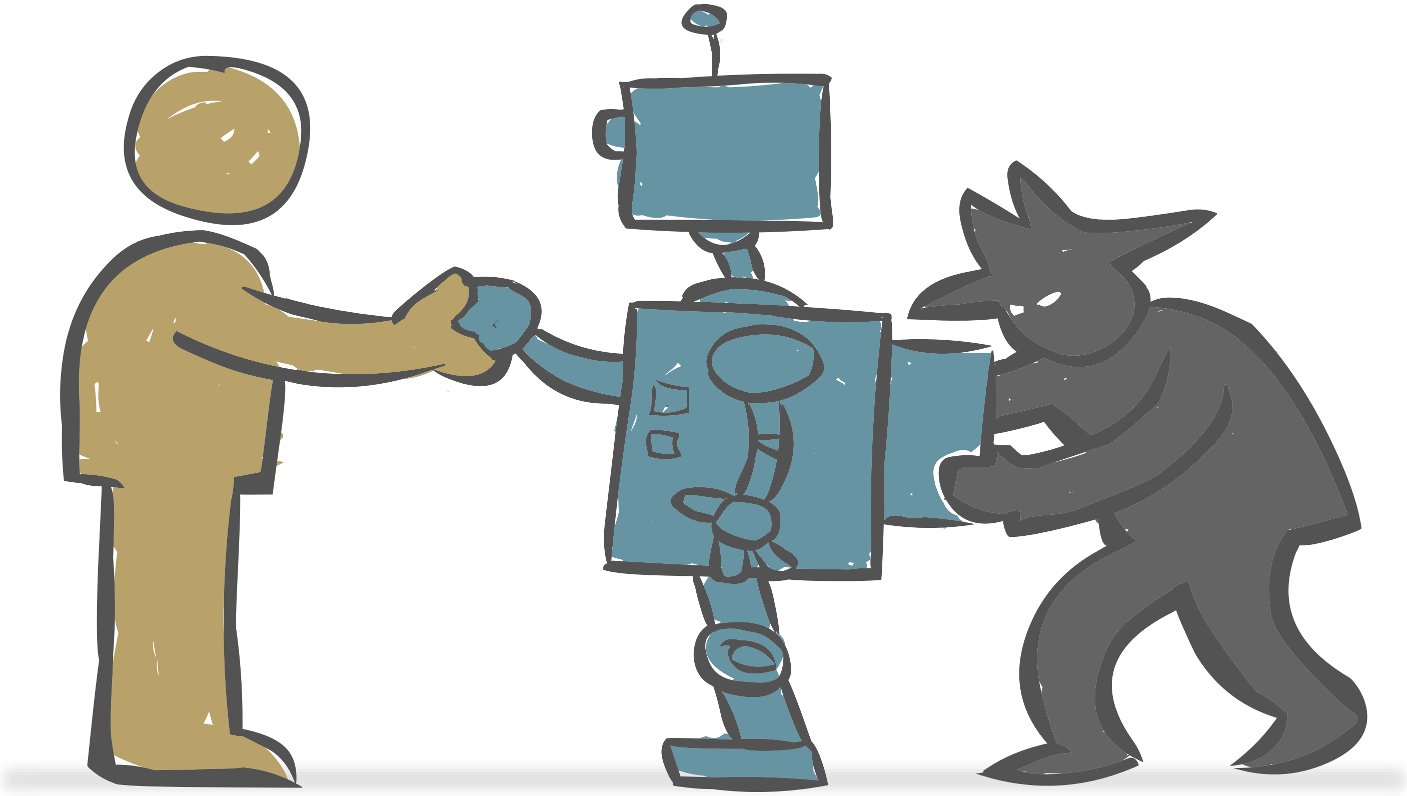
The study found the most common meaningful term 'access' in more than 900 documents, while only 76 documents included the term 'opt-out' and 32 included the term 'opt-in'.

Encrypting data from the phone to the cloud

In an attempt to overcome the barriers to using encryption, a group of researchers at Georgia Tech have created a prototype overlay for Android phones that intercepts input in popular applications and encrypts the data before it moves to the cloud. The system, known as Mimesis Aegis, uses secure overlays to preserve an application's experience while capturing input. Data from the cloud service is decrypted before being displayed to the user in another overlay.[BL1]

Attackers target the trust relationship between users and machines

Cybercriminals continue to successfully abuse the trust of users, while the Internet of Things poses problems for the current systems of trust between machines



Highlights:

- While software vulnerabilities continue to be exploited, the user is still the greatest weakness to information security
- The Internet of Things will stress the foundations of trust as a variety of machines share data with one another on their users' behalf
- Neither training nor technology alone can prevent the most targeted phishing attacks that have caused the most significant data breaches in the past few years
- New models for establishing trust between humans and machines, and between different machines, must be developed in the future

With compiler developers and major operating-system vendors integrating techniques that make exploitation more difficult, it has become more complex and costly for attackers to use vulnerabilities to compromise systems. In 2013, for example, only 10 percent of Microsoft's vulnerability bulletins were remotely exploitable, down from more than 40 percent in 2011.[MS1] Instead, attacks that leverage social engineering have become increasingly popular, with 67 percent of cyber espionage starting with a phishing e-mail, according to the Verizon 2014 Data Breach Investigations Report (DBIR).[VR1]

Attackers have increasingly focused on exploiting trust, whether through employing social engineering or compromising the certificate infrastructure of the Internet. In the future, as machines make more decisions on behalf of the user, attackers will aim to exploit the web of trust between these systems. With 50 billion “things” expected to be connected to the Internet, the web of trust between users, systems, and devices will become even more important, says Margaret Loper, principal research scientist at the Georgia Tech Research Institute (GTRI).

“In this emerging Internet of Things world, with however many billions of devices connected to the network, we will be relying much more on machines to make decisions for us, whether in healthcare, leisure, finance, or in smart homes,” she says.

Humans remain the link most often exploited in attacks

Humans are no longer the last line of defense against cyber attacks, but often represent an end run around security measures. Convince a user to open an attachment and dismiss a security warning, and an attacker’s job is mostly done.

When Georgia Tech first piloted phishing awareness training using the 300-member Office of Information Technology (OIT), one out of every four people clicked on the link in the phishing e-mail message and could have had their system compromised. The experiment showed that not only is social engineering common, but extremely effective. “That scared me,” says Jason Belford, associate director of cyber security for Georgia Tech’s OIT. “One out of every four people responded, and they were all technical. These are the people that had the keys to the kingdom.”

Georgia Tech’s experience is typical. The click-through rate on phishing e-mail messages typically starts at 20 percent or higher in most organizations, according to training companies[RL2]. Training can help reduce that to single digits but only very infrequently to zero, which means that combining training with exploit-mitigation technologies is necessary to keep out attackers.

The Internet of Things will exacerbate issues of trust

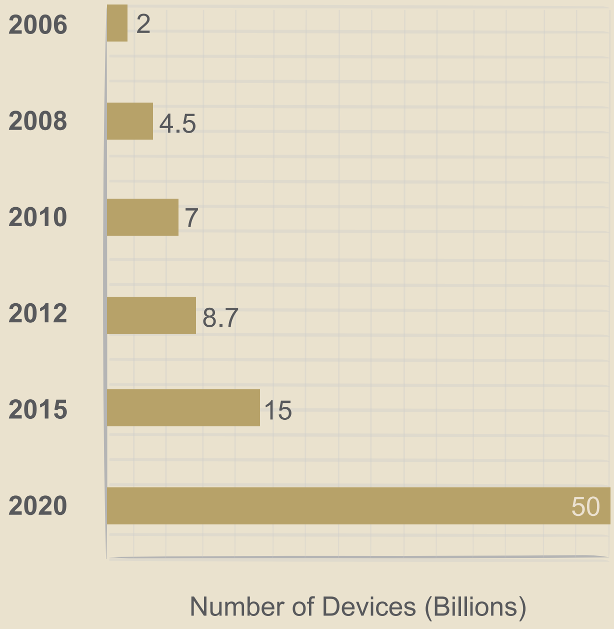
With the proliferation of mobile devices and the growth of the Internet of Things, developing policies and algorithms for trusting information and devices will become more difficult. The Internet of Things will encompass at least 50 billion objects by 2020, including mobile devices, a variety of applications for radio frequency identifiers (RFID), intelligent home automation, and medical devices.

Deciding how those devices will communicate with each other, which ones will pass information on to others, and how users will interact with them are complex issues. The issue of a human’s trust of digital information may end up being an easier problem to solve than developing a model for trust between machines, says GTRI’s Loper.

“In the Internet of Things world, there are machines coming and going, so it is going to be much more dynamic,” she says. “These devices are going to have to continuously assess each other to figure out what to trust, and like humans, they may start off with a level of trust that will change over time.”

The Internet of Things to Pose Privacy and Security Challenges

In 2008, the number of interconnected devices exceeded the number of human beings in the world. By 2020, there could be 50 billion devices. Securing these devices and the data passed between them will be a challenge.



SOURCES: Cisco, Intel, IDC

From sensor networks and smart grids to home automation and medical implants, the networkable objects of the future will require a robust framework of trust to securely operate.

Neither training nor technology are sufficient solutions to the problem of trust

The complex landscape of trust in the future will mean that training alone will not be enough to determine whether data or an object can be trusted. Just as humans increasingly rely on machines to tell them whom to trust, machines will likely require human guidance in determining what devices they should trust.

Today, training is an important piece of the security puzzle and one that companies do not employ often enough. While 49 percent of companies do not perform employee security-awareness training, they pay the price — their annual losses are four times greater than those that do have a training process in place, according to accounting firm PwC US.[PW1]

“Training is somewhat effective, but it does not come anywhere close to solving the problem because you only need one message to get through,” says Fred Wright, chief scientist of the Cyber Technology and Information Security Laboratory at GTRI. “On the other hand, any reduction in that rate saves money, because there are fewer incidents to respond to and clean up.”

Micro-grants for Security Training

The Georgia Tech Information Security Center (GTISC) has created a micro-grant program to help develop security content for courses and colleges that might not otherwise have the resources or expertise to develop such material on their own. The effort, sponsored by Intel Labs University Collaborations Office and the National Science Foundation, provides the resources to create a broader base of security knowledge in the community, says Paul Royal, associate director of GTISC.

“At a smaller university there may not be a dedicated information security faculty member, and thus sometimes the only way to get security content into the curriculum is through external content creation and training,” Royal says.

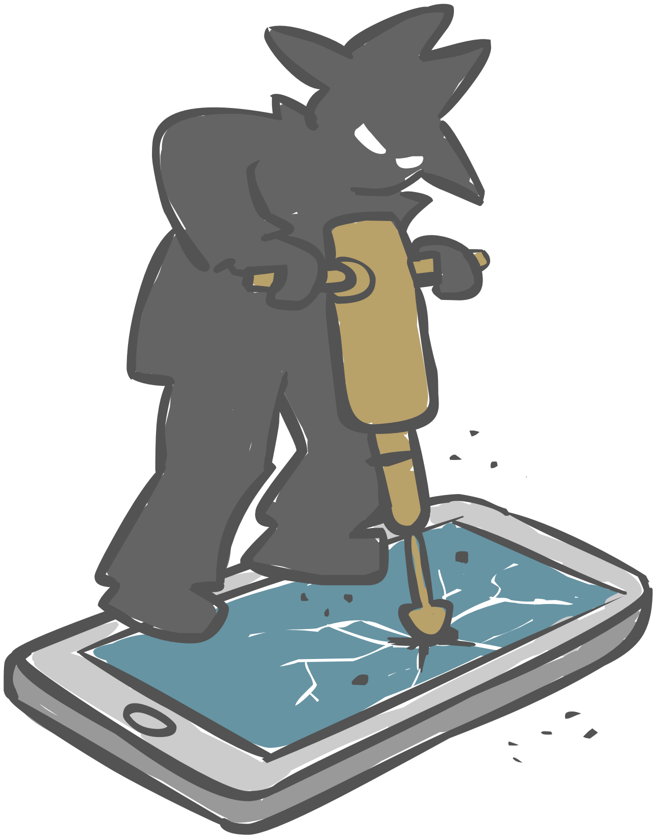
Defining trust among machines

The Georgia Tech Research Institute has embarked on a project to help machines evaluate their environment to decide what other devices can be trusted. The security of users and their data in a future of billions of interconnected devices will rely on having a firm foundation of trust. The Machine-to-Machine Trust Framework focuses on three dimensions of trust: the technical integrity of the devices, the devices’ ability to perform actions on behalf of others, and the trustworthiness of the result.[ML1]

“Many of the ways that we determine trust — such as body language —machines don’t have,” says GTRI’s Loper. “We are trying to look out at the harder scenarios in terms of things that have very dynamic memberships and may be deployed in very critical kinds of missions.”

Mobile devices fall under increasing attack, stressing the security of the ecosystem

While more controlled software ecosystems have protected mobile devices until now, attackers are increasingly targeting users as the value of devices grows



Highlights:

- Consumers and employees tightly bind their lives to their mobile devices, turning phones and their linked cloud repositories into treasure troves of information

- Android devices continue to bear the brunt of attackers' focus, requiring better security measures and communication of risk to users

- Apple's iOS is not free from risk, with studies showing that targeted attacks are practical and mass infection possible

- The future popularity of using mobile devices to pay at the counter will increase their value to attackers, spurring greater interest in attacks

Outside of unregulated third-party app stores and countries with anemic protections against criminal abuse of premium text messages, monetizing mobile compromises remains difficult. Unsurprisingly, the encounter rates of mobile malware — which should not be equated with infections — remains less than 6 percent in most countries tracked by mobile security firm Lookout.[LO1] While mobile malware continues to remain a nascent threat, software that uses aggressive advertising frameworks, known as adware, is more pervasive, with encounter rates of 20 to 30 percent for most countries' users.

These threats will continue to grow as attackers find ways to circumvent the protections of the mobile ecosystem. In June 2013, mobile devices saw attacks involving a program called Android Defender that displays fake alerts in an effort to trick the user into paying for a "full version" of the program.[TK1] In 2014, more attacks emerged, including Oleg Pliss, an attack on Apple’s iCloud that locked victims’ phones using the Find My iPhone functionality.[PD1]

“Five or six years ago, everything was targeting the laptop, but smartphones have more data, more features, and more capabilities,” says Yeongjin Jang, a Ph.D. candidate in Georgia Tech’s College of Computing. “So the attackers are trying to get access to these devices through various means.”

Android remains the focus of opportunistic attacks, while iOS is still vulnerable to persistent adversaries

Google and Apple have taken different approaches to the software ecosystems surrounding their mobile operating systems. While Google has opened its Android platform to spur adoption and kept access to its app store relatively unfettered, Apple has kept iOS closed source and strictly controls what is allowed in its store. The impact of these decisions is dramatic: 99 percent of mobile malware targets Android devices,[CS1] attempting to infect the systems by slipping into the Google Play app store or by convincing users to download and install applications from third-party stores and untrusted sites.

However, Apple’s ecosystem is not a safe haven and attackers have found ways around the security measures taken by the company. By focusing on iCloud, for example, vandals grabbed intimate photos taken by celebrities with their iPhones and uploaded to the cloud.[JL1]

Those attacks are just the start. Georgia Tech researchers demonstrated two attacks against the iPhone ecosystem that circumvented the security of Apple’s App Store model. The first attack, dubbed Mactans[BL2], used the key signing functionality given to developers and hardware disguised as a power adapter to install malicious apps on devices plugged into the adapter. In another attack, known as Jekyll[TW3], the attacker submits a seemingly benign app to the app store and then uses intentional vulnerabilities in the application to turn the software malicious.

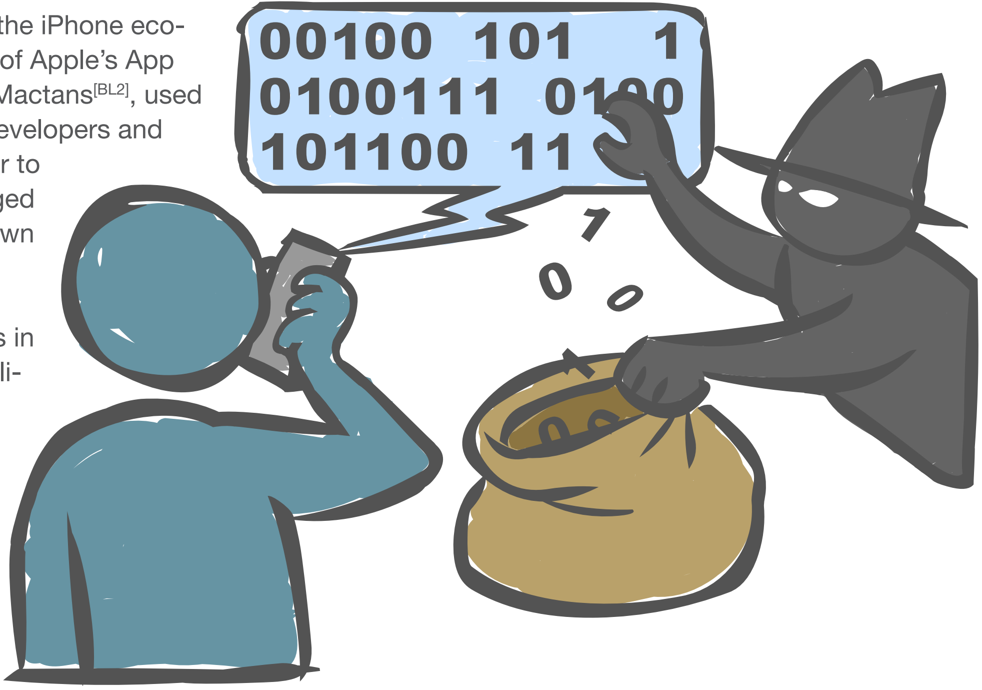
“The Jekyll research is an example of how these techniques are going to get serious,” says Chris Smoak, deputy chief for the Emerging Threats and Countermeasures Division at the Georgia Tech Research Institute. “A threat like Jekyll in the wild is going to be a big problem for the ecosystem as a whole.”

Application developers continue to focus on monetizing users and not enough on the security of their software

The explosion of mobile application popularity over the past five years has meant that many developers are relatively inexperienced, especially in creating secure code. In addition, the proliferation of free apps, monetized by the adoption of advertising frameworks, has driven many developers to use untrusted code libraries in their products.

The result is that many applications have vulnerabilities that can be exploited or have questionable privacy practices, collecting data on users in ways that may not be acceptable or fully disclosed. In 2014, 91 percent of the top 200 iOS apps and 83 percent of the top 200 Android apps had some risky behavior, according to data collected by mobile app reputation service Appthority.[AP1] Previous studies have found that development and advertising frameworks—used by programmers to quickly add features to their products—are responsible for much of the questionable behavior.

Mobile operating system makers are not exempt from these issues. In March 2014, Apple fixed a group of vulnerabilities that allowed attackers to bypass iOS’s code-signing security. Georgia Tech researchers, however, found that the company’s fix was not comprehensive and demonstrated an attack that reused several of the unpatched vulnerabilities to jailbreak iOS at Black Hat USA 2014.[YJ1]



Mobile payments will draw attackers' focus

While the ability to pay with a mobile phone at the point-of-sale has caught the imaginations of many technologists, slow adoption has hindered the growth of the market. In 2013, for example, while the transaction volume of mobile payments grew by 44 percent to $235 billion worldwide, the volume of payments using near-field communications (NFC) — the key to point-of-sale transactions — fell flat, according to Gartner estimates.[GT1] Yet, the announcement in September of Apple Pay could give NFC mobile payments a tremendous boost.[TW1]

Because attackers follow the money, mobile payments will be targeted by security researchers and opportunistic criminals, leading to more intense scrutiny of the devices' security. Apple's Touch ID — which protects Apple Pay transactions — and other biometric technologies may not be enough, says Billy Lau, a research scientist at GTISC.

"In other parts of the world, mobile payments have taken off," says Lau. "But the security technologies are not fully there yet."

!

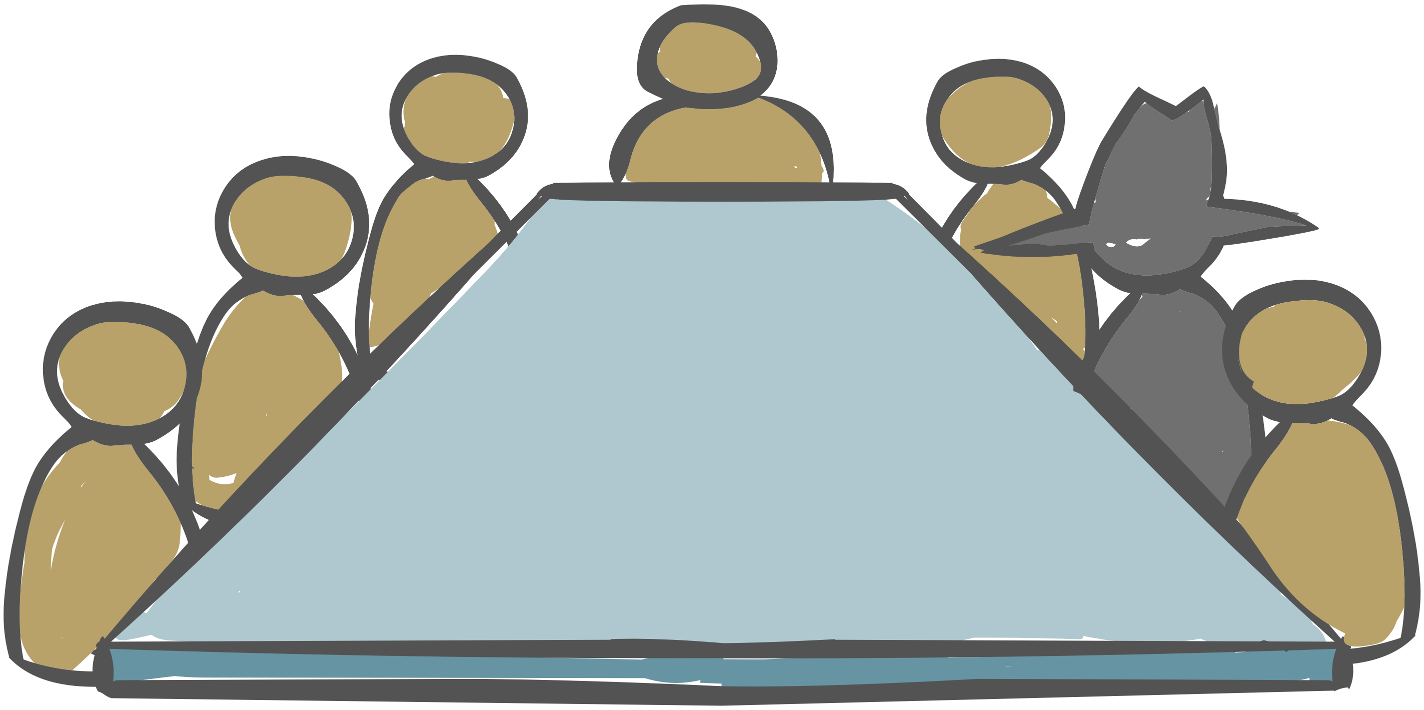
Investigating the possibility of a mobile outbreak

While digital worms, which spread automatically and quickly, have largely disappeared from the digital landscape, researchers at Georgia Tech looked into the feasibility of mass iOS device infection. The researchers posited that iOS devices such as the iPhone could be infected through the synchronization process with a system running iTunes. Using network traffic data, the researchers were able to discover that 23 percent of Windows systems with signs of botnet infection also showed purchase activity through the iTunes application, suggesting that the devices could be attacked through iTunes.[TW2]

"The personal computer is a new attack vector for mobile devices, but we believe it will be an important one," says Tielei Wang, a research scientist with GTISC and part of the team that conducted the research.

Rogue insiders can cause significant damage, but solutions are neither simple nor easy

Companies must trust their workers, leaving them open to damage when insiders go rogue



Highlights:

- While massive data breaches cause the most measurable damage to companies, the involvement of an insider causes costs to rise quickly
- Behavioral indicators continue to pose significant challenges as a method to detect the activities of a rogue insider
- Outreach to employees and access restrictions, such as splitting the keys to valuable data between two or more people, can make it much less likely that a single rogue insider will be successful
- Classification of data and monitoring access are time-consuming activities, so companies should focus on initially protecting their "crown jewels" before expanding any data-protection program

From former National Security Agency contractor Edward Snowden to a group of employees at high-end clothing store Saks Fifth Avenue, insiders who turn against their company can cause significant damage. Overall, companies require more time to detect and respond to insider attacks, nearly 260 days, compared to 170 days for other attacks, according to data from the Ponemon Institute's 2014 Cost of Cybercrime survey.[HP1] Incidents involving malicious insiders also cost, on average, more than $210,000 to resolve, according to the study.[PI1]

Many executives are driven by media coverage of security topics, and the headlines over the last year have focused heavily on insider attacks. The result is predictable, says Andrew Howard, director of the Cyber Technology and Information Security Laboratory (CTISL) at the Georgia Tech Research Institute (GTRI). "Companies today are interested in military grade defenses of their data, which was not the case 18 months ago," he says. "The pendulum between usability and security is swinging, and when it comes to critical, crown-jewel data, it's swinging more towards security."

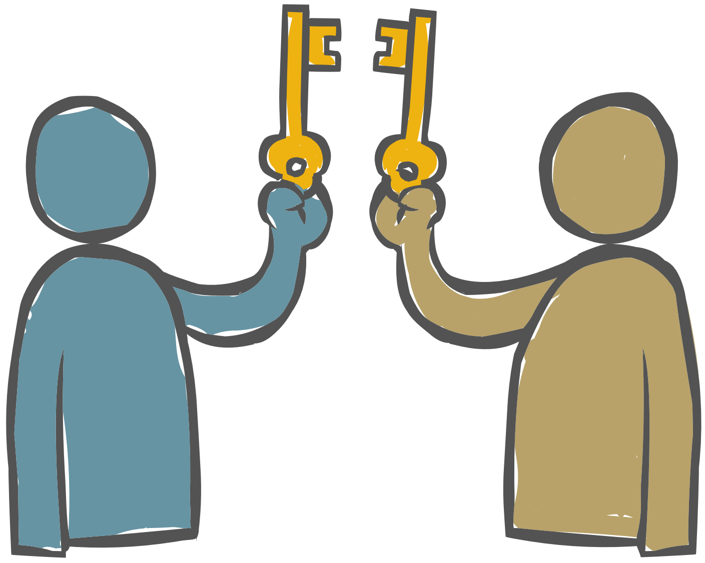
Anomaly detection continues to be difficult, because defining "normal" behavior is difficult

Many companies have attempted to detect internal threats by looking for employees whose activities seem to be out of the ordinary. While the concept is straightforward, implementation typically results in burgeoning false positives, overburdening IT security staff and desensitizing them to potential attacks.

Georgia Tech's internal efforts are illuminating. While the university has a number of insider threat initiatives, detecting anomalous network behavior is not among them, says Jimmy Lummis, information security policy and compliance manager for the Office of Information Technology. Due to the heterogeneous nature of a university's traffic, attempting to classify anomalous activity too often results in false positives, he says.

"We have never been successful in establishing a baseline, because everything shifts so quickly," Lummis says. "Everyone is constantly standing up new projects and new research."

A potential area to focus defenders' efforts is modeling user behavior and raising a red flag when people are acting outside of expectations. By determining behavioral profiles for employees and detecting changes in behavior — such as calling in sick, reduced productivity, or excessive spending — organizations could detect potential threats earlier. In addition, techniques combining such research with a variety of network and system events could result in alerts for potential malicious behavior.[DB1]



Overclassification of data can swamp current data-protection systems

In conjunction with detecting potential threats, most companies also attempt to add extra protections around their most sensitive data. A common tactic is to categorize data into asset classes, as a way to decide what data needs to be protected, and then focus on the most critical information. By guarding a smaller subset of data, companies should be able to better track who accesses the information and what they do with it.

Yet, determining what data is valuable to a company is a complicated problem, especially when employees — who may have a narrow view of the impact of data loss — make the decision on the fly, says GTRI's Howard. For example, when classifying a schematic for a motor, an engineer may not have a good reference from which to judge its criticality. "Most of the companies that I deal with, even the cream of the crop, don't know what their crown-jewel data is," Howard says. "They need to create guidelines that are actionable by employees."

A variety of factors — from the instinct to err on the side of caution to employees' overestimation of their value — could mean data is classified as more important than warranted, leading to a greater volume of work to protect the data.[RM1]

Neither prevention nor detection is enough, leaving companies to take a broader view of the problem

Rather than solely relying on technology, organizations should approach the problem of data protection and insider threats as a broad issue with many solutions. Technology, in combination with access control processes, can be a benefit. In addition, employee training can also help companies teach correct behavior, educate workers as to the potential damage from mistakes, and recruit them to help keep the company safe.

While insider attacks are a tough problem, security professionals have a tool to use against insiders that they do not have against other cyber attackers — deterrence. Companies have access to their insiders, and if found, can punish them, says Tom Cross, director of research at security firm Lancope.

"In most computer security areas, we have no ability to deter the attackers — the person who is breaking into your network is on the other side of the planet, and you are never going to find them. Even if you do, they are likely in a country from which they cannot be extradited," Cross says. "But you know the insider who creates the insider threat, you have a personal relationship with them, and you have access to them, so you can manage the problem in a different way."

Enforceable two-person security for popular operating systems

Given that rogue insiders often act alone, companies can defend against unapproved actions by requiring another person to sign off on risky activities. As part of its initiative on developing defenses to prevent data loss due to insiders, the Georgia Tech Research Institute is creating drivers for popular operating systems that will require two or more operators to sign off on actions, such as updating the operating system or copying data to removable media.

In many ways, the idea is similar to the two keys necessary to launch a nuclear missile, says GTRI's Howard. "Before a system administrator can go look at data, they might need a second systems administrator there with them to authorize the activity."

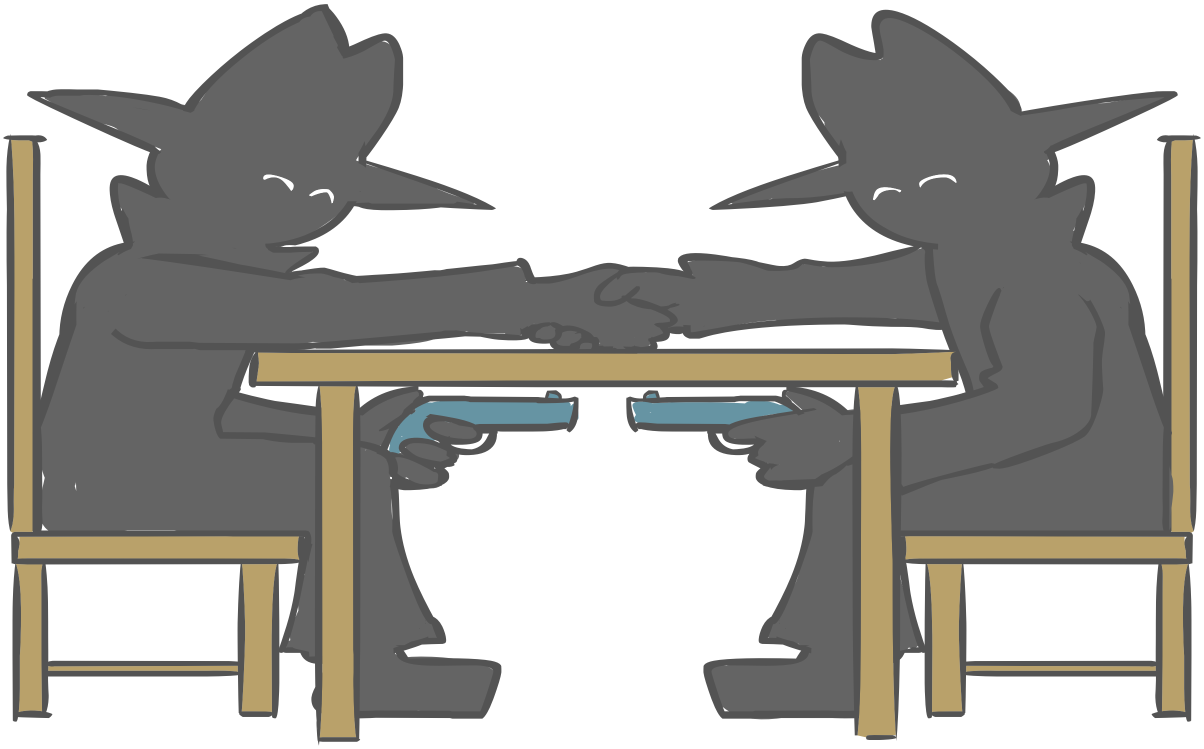
Modeling people to detect rogue behavior

Anomaly detection systems aim to identify actions that a potentially rogue user does that can harm a company. Research at Georgia Tech aims to gauge when a user may be preparing to go rogue. Called Layered Ensemble Anomaly Detection (LEAD), the research project models user behavior and then looks for users that may be acting in an unexpected way, says Erica Briscoe, senior research scientist at the Georgia Tech Research Institute.

"We don't want to catch insiders at the moment they do something bad; we want to catch them before they do it," says Briscoe.

Low-intensity online nation-state conflicts become the rule, not the exception

Major countries have conducted many online operations, dodging the diplomatic fallout of more overt actions



Highlights:

- The number of reports of online espionage and information operations, seemingly sponsored by nation-states, continues to grow
- Cyber conflict continues to be a complex problem because of the difficulty in attributing attacks and the potential for smaller, non-nation-states to asymmetrically impact larger countries
- As espionage activities continue to escalate, so will diplomatic actions, such as the recent indictment of five Chinese military personnel for their part in economic espionage
- While some experts espouse stronger countermeasures to punish attackers, diplomacy and policy will continue to be the most effective deterrent

When pro-democracy protests erupted in Hong Kong in September, cyber attacks aimed at compromising protesters' mobile phones soon followed[SG1]. Spread through links in pro-Hong Kong e-mail messages, the mobile remote access tool (mRAT) gave the group behind the attack—the most obvious suspect being the Chinese government[LC1]—almost total access to the device and its data. Two weeks later, similar espionage attacks were found hidden on compromised websites of organizations supporting the democratic movement.[SA1]

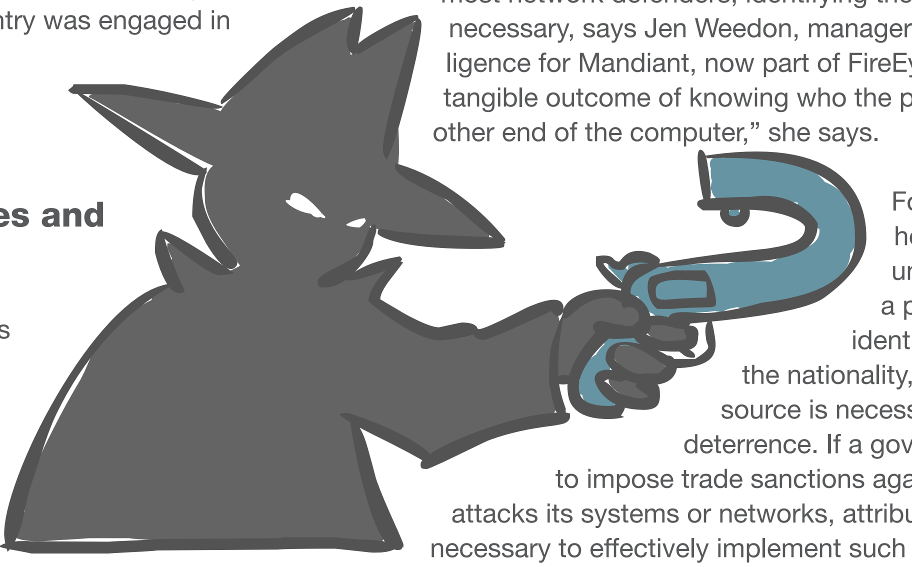
The attack on Hong Kong citizens underscores the degree to which governments have taken to programs typically associated with hackers and cybercriminals. From cyber conflict to industrial espionage to law enforcement monitoring, nation-states and government-sponsored groups have adopted online tactics to complement their real-world strategies. China's efforts at economic espionage have gained the most attention, along with the United States' presumed development of the Stuxnet worm used to slow Iran's nuclear ambitions.[EN1]

In 2014, however, Russia's cyber capabilities became increasingly clear with the outing of the Snake campaign targeting Ukraine's government[DS1] and the Sandworm campaign targeting the North Atlantic Treaty Organization (NATO) and European governments[RL3]. While attribution is never certain on the Internet, most experts placed suspicions for the attacks on Moscow.

While cyber espionage appears to be the new normal for stealing secrets from competitors in other nations, recent conflicts indicate that cyber attacks will play a tangible role in future military affairs. In an analysis of malicious Internet traffic based on data collected from security firm FireEye, Kenneth Geers, a researcher and ambassador from the NATO Cooperative Cyber Defense Center of Excellence, found that malware communications sent to servers in Russia, Ukraine, and Israel increased during the months in which each country was engaged in conflict.[KG1]

Choosing offense over defense will penalize businesses and citizens

One axiom of online attacks is that defenders need to be right every time, while attackers only need to be right once to gain access to the defenders' network. Moreover, attackers who do not succeed are typically not punished, allowing them to learn from their failures and to return to attack in the future.



Such asymmetry has convinced many that attacking back and creating a strong offense is a good strategy. Collecting information on other countries' strategies and plans, even during peace time, is the reason that intelligence agencies exist. Yet, just because defense is hard, governments should not default to offense, otherwise they will be essentially conducting a cyber war during peace time, argues Peter Swire, the Huang Professor of Law and Ethics at Georgia Institute of Technology's Scheller College of Business.

With the vast majority of Internet infrastructure in private hands, any attack against a nation's government will also be an attack on the private sector, causing enormous collateral damage, he says. In addition, offensive-minded governments will hoard vulnerability information rather than seeing security flaws patched, effectively leaving their own citizens and businesses vulnerable.

"A fundamental question for U.S. policy is how much to emphasize offense versus defense for cyber security," says Swire. "I think there are strong reasons to lean towards defense: The U.S. is more heavily dependent on networks and IT than other countries, so we have more to lose if the defense is weak."

Attribution continues to be a problem

Whenever security researchers discuss the likely provenance of an attack, they often couch any attribution with qualifications that any attacker could make themselves appear to be from China, Russia, or the United States. For most network defenders, identifying the attacker is not necessary, says Jen Weedon, manager of threat intelligence for Mandiant, now part of FireEye. "There is little tangible outcome of knowing who the person is on the other end of the computer," she says.

For policymakers, however, such uncertainty poses a problem — the identity, or at least the nationality, of an attack's source is necessary for effective deterrence. If a government decides to impose trade sanctions against whomever attacks its systems or networks, attribution becomes necessary to effectively implement such penalties.

In addition, the practice of attempting to pose as a different actor, a technique known as false flagging, may become more popular, especially if an attacker can elicit the victim to punish another country. Whether attribution techniques can detect such false flagging attacks remains uncertain.

Policy will remain the most effective way to remove attackers' incentives to conduct cyber operations

Even when a nation knows the identity of an attacker, the government is left with scant choices for deterring future attacks. The United States diplomatic trajectory with China is case in point. U.S. government officials have publicly blamed the country for supporting attacks against businesses and finally, in May, indicted five members of the Chinese military on charges of criminal hacking.[EN2]

The charges against the five men are part of a slow escalation of diplomatic consequences that will continue and eventually be effective, says Dmitri Alperovitch, chief technology officer and co-founder of security services firm CrowdStrike. “The question that no one knows the answer to is what will it take for the Chinese to get the message.”

Such policy works well against nations, but governments are not the only adversaries. Groups of hackers, such as dissidents aligning themselves with the Anonymous philosophy, or cyber militias — perhaps acting on behalf of a government — can easily mount effective attacks and have less fear of punishment, says NATO’s Geers.

“If and when you figure out who did it, you may also find that there is no real cyber infrastructure against which to retaliate,” he says. “ISIL does not fear retaliation from the U.S. — whether in traditional or cyber form — in the same way that, say, Mexico would.”

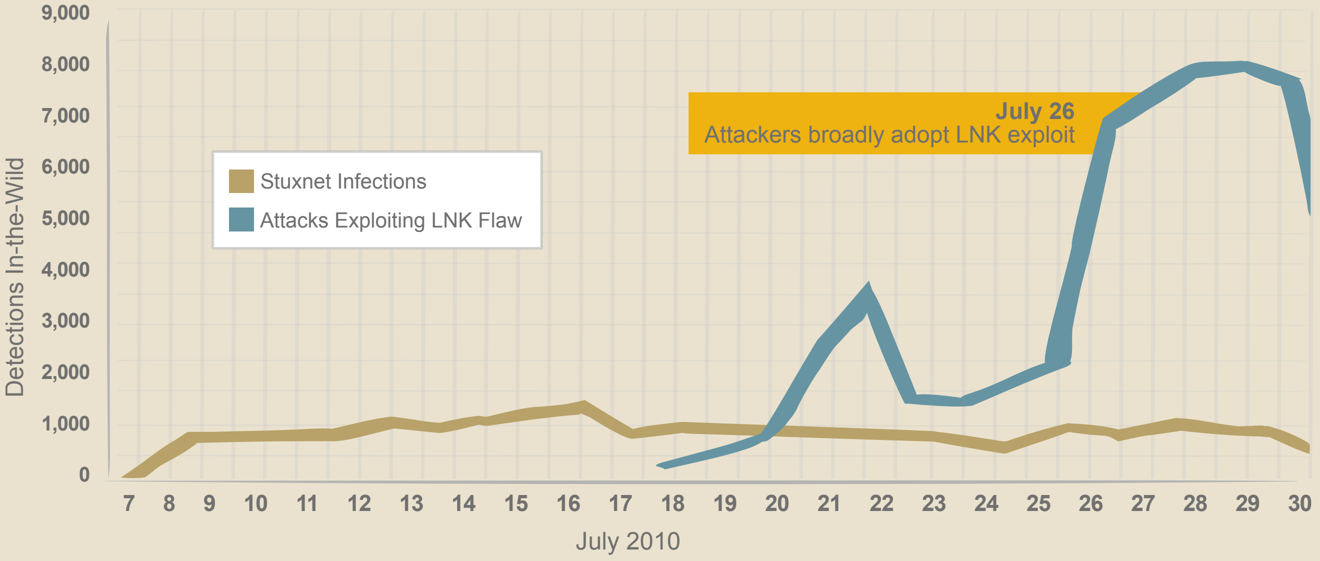
Creating a better game theory to evaluate adversaries

During the 1940s, John von Neumann and Oskar Morgenstern created Game Theory to provide a rational framework for making decisions based on expected outcomes. Given that Game Theory provides the theoretical framework for applications in diplomatic policy, such as nuclear deterrence, researchers have pondered whether it could equally apply to cyber conflict.

However, humans are not always rational and do not always make decisions based on the expected outcome. Fariborz Farahmand, a senior research engineer in the Electrical and Computer Engineering Department at Georgia Tech, is investigating ways to take human behavior into account. Cyber security policy could benefit from such research, he says.

Cyber Attacks Constitute a Transfer of Technology to the Adversary

The Stuxnet cyber attack exploited a vulnerability in how Windows processed icons (LNK files). The public disclosure of the flaw resulted in a variety of criminals incorporating the exploit into their malware, essentially giving adversaries a better weapon.



SOURCE: Stewart, Holly and Cross, Tom, “Lessons Learned: Can Alerting the Public about Exploitation do More Harm than Good?” Virus Bulletin, Oct. 2013.
(link to paper: https://www.virusbtn.com/files/StewartCross-VB2013.pdf)

References

Technology enables surveillance, while policy lags behind

[BL1] Lau, Billy et al., “Mimesis Aegis: A Mimicry Privacy Shield–A System’s Approach to Data Privacy on Public Cloud,” Proceedings of the 23rd USENIX Security Symposium, 23 August 2014, https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-lau.pdf

[BS1] Smith, Brad, “Protecting Customer Data from Government Snooping,” The Official Microsoft Blog, 4 December 2014, http://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/

[GS1] Gustin, Sam, “Tech Titans Reveal New Data About NSA Snooping,” Time, 3 February 2014, http://time.com/3902/tech-titans-reveal-new-data-about-nsa-snooping/

[GS2] Gellman, Barton and Soltani, Ashkan, “NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden documents say,” The Washington Post, 30 October 2013, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

[MA1] Massey, Aaron et al., “Automated Text Mining for Requirements Analysis of Policy Documents,” Proceedings of the 21st IEEE Requirements Engineering Conference, 15 July 2013, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6636700

[RG1] President’s Review Group on Intelligence and Communications Technologies, “Liberty and Security in a Changing World,” 12 December 2013, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[RH1] Howard, Rebecca, “Edward Snowden Accuses New Zealand of Deception Over Surveillance,” The Wall Street Journal, 15 September 2014, http://online.wsj.com/articles/snowden-makes-new-zealand-claims-1410766263

[RL1] Lemos, Robert, “NSA Snooping Likely to Damage U.S. Cloud Services Industry: Studies,” eWEEK, 28 August 2013, http://www.eweek.com/security/nsa-snooping-likely-to-damage-us-cloud-services-industry-studies.html

[SS1] Smale, Alison and Sanger, David, “Spying Scandal Alters U.S. Ties With Allies and Raises Talk of Policy Shift,” The New York Times, 11 November 2013, http://www.nytimes.com/2013/11/12/world/spying-scandal-alters-us-ties-with-allies-and-raises-talk-of-policy-shift.html

[ST1] Tiezzi, Shannon, “China’s Response to the U.S. Cyber Espionage Charges,” The Diplomat, 21 May 2014, http://thediplomat.com/2014/05/chinas-response-to-the-us-cyber-espionage-charges/

[TG1] “Lawyer Suing Facebook Overwhelmed with Support,” The Guardian, 6 August 2014, http://www.theguardian.com/technology/2014/aug/06/facebook-privacy-action-austria-max-schrems

[TJ1] Toobin, Jeffrey, “The Solace of Oblivion,” The New Yorker, 29 September 2014, http://www.newyorker.com/magazine/2014/09/29/solace-oblivion

[TM1] Timberg, Craig and Miller, Greg, “FBI Blasts Apple, Google for Locking Police Out of Phones,” The Washington Post, 25 September 2014, http://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html

Attackers target the trust relationship between users and machines

[ML1] Loper, Margaret and McCreary, JD, “Machine to Machine Trusted Behaviors,” Proceedings of UBICOMM 2014, 24 August 2014, http://www.cdait.gatech.edu/sites/default/files/trusted_m2m_behaviors_loper_mccreary_-_wip_v3_no_comments.pdf

[MS1] “Microsoft Security Intelligence Report, Volume 16,” Microsoft, 6 May 2014, http://www.microsoft.com/security/sir/default.aspx

[RL2] Lemos, Robert, “Phishing Messages Trick One in Five Employees Into Clicking: Survey,” eWEEK, 7 November 2013, http://www.eweek.com/security/phishing-messages-trick-one-in-five-employees-into-clicking-survey.html

[PW1] “The Global State of Information Security Survey 2015,” PwC US, 30 September 2014, http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml

[VR1] “2014 Data Breach Investigations Report,” Verizon, 22 April 2014, http://www.verizonenterprise.com/DBIR/2014/

Mobile devices fall under increasing attack, stressing the security of the ecosystem

[AP1] “App Reputation Report,” Appthority, Winter 2014, Pg. 4, https://www.appthority.com/app-reputation-report/report/AppReputation0214.pdf

[BL2] Lau, Billy et al., “Mactans: Injecting Malware Into iOS Devices via Malicious Chargers,” Black Hat USA 2013, August 2013, https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-WP.pdf

[CS1] “Cisco 2014 Annual Security Report,” Cisco, pg. 33, http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

[GT1] “Gartner Says Worldwide Mobile Payment Transaction Value to Surpass $235 Billion in 2013,” Gartner press release, 4 June 2013, http://www.gartner.com/newsroom/id/2504915

[JL1] Linshi, Jack, “What We Know About the Latest Nude Celebrity Photo Hack,” Time, 22 September 2014, http://time.com/3418330/kim-kardashian-jennifer-lawrence-nude-photos-hack/

[LO1] Gamble, John et al., “2013: Made-to-Measure Malware and the Battle Against Adware,” Lookout, 20 February 2014, https://blog.lookout.com/blog/2014/02/20/malware-made-to-measure/

References

[PD1] Ducklin, Paul, “Apple iOS Ransomware Mystery Deepens - ‘Oleg Pliss’ Pops Up in LA,” Naked Security Blog, 29 May 2014, http://nakedsecurity.sophos.com/2014/05/29/apple-ios-ransomware-mystery-deepens-oleg-pliss-pops-up-in-la/

[TK1] Katsuki, Takashi, “Android.Fakedefender Summary,” Symantec, 2 June 2013, http://www.symantec.com/security_response/writeup.jsp?docid=2013-060301-4418-99

[TW1] Warren, Tom, “Apple Pay Available on October 20th with 500 More Banks on Board,” The Verge, 16 October 2014, http://www.theverge.com/2014/10/16/6981117/apple-pay-release-date-available-october-20th

[TW2] Wang, Tielei et al., “On the Feasibility of Large-Scale Infections of iOS Devices,” Proceedings of the 23rd USENIX Security Symposium, August 2014, https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-wang-tielei.pdf

[TW3] Wang, Tielei et al., “Jekyll on iOS: When Benign Apps Become Evil,” Proceedings of the 22nd USENIX Security Symposium, August 2013, https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_wang-updated-8-23-13.pdf

[YJ1] Jang, Yeongjin et al., “Exploiting Unpatched iOS Vulnerabilities for Fun and Profit,” Black Hat USA 2014, August 2014, https://www.blackhat.com/us-14/briefings.html#exploiting-unpatched-ios-vulnerabilities-for-fun-and-profit

Rogue insiders can cause significant damage, but solutions are neither simple nor easy

[DB1] Bader, David et al., “Detecting Insider Threats in a Real Corporate Database of Computer Usage Activity,” Proceedings of the 9th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, August 2013, http://dl.acm.org/citation.cfm?id=2488213

[HP1] “Annual Study Reveals Average Cost of Cyber Crime Escalates 96 Percent to $12.7 Million per Organization,” Hewlett Packard, 15 October 2014, http://www8.hp.com/us/en/hp-news/press-release.html?id=1815969

[PI1] “2014 Cost of Cybercrime Study,” Ponemon Institute, 15 October 2014, http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/index.html

[RM1] Mogull, Rich, “The Five Problems with Data Classification, and Introduction to Practical Data Classification,” Securosis Blog, 10 October 2007, https://securosis.com/S=0/blog/the-five-problems-with-data-classification-and-introduction-to-practical-da

Low-intensity online nation-state conflicts become the rule, not the exception

[DS1] Sanger, David and Erlanger, Steven, “Suspicion Falls on Russia as ‘Snake’ Cyberattacks Target Ukraine’s Government,” The New York Times, 8 March 2014, http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html

[EN1] Nakashima, Ellen and Warrick, Joby, “Stuxnet Was Work of U.S. and Israeli Experts, Officials Say,” The Washington Post, 2 June 2012, http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

[EN2] Nakashima, Ellen and Wan, William, “U.S. Announces First Charges Against Foreign Country in Connection with Cyberspying,” The Washington Post, 19 May 2014, http://www.washingtonpost.com/world/national-security/us-to-announce-first-criminal-charges-against-foreign-country-for-cyberspying/2014/05/19/586c9992-df45-11e3-810f-764fe508b82d_story.html

[LC1] “Chinese Government Targets Hong Kong Protesters with Android mRAT Spyware,” Lacoon, 30 September 2014, https://www.lacoon.com/chinese-government-targets-hong-kong-protesters-android-mrat-spyware/

[KG1] Geers, Kenneth, “Strategic Analysis: As Russia-Ukraine Conflict Continues, Malware Activity Rises,” FireEye, 28 May 2014, http://www.fireeye.com/blog/technical/2014/05/strategic-analysis-as-russia-ukraine-conflict-continues-malware-activity-rises.html

[RL3] Lemos, Robert, “Suspected Russian ‘Sandworm’ Cyber Spies Targeted NATO, Ukraine,” Ars Technica, 14 October 2014, http://arstechnica.com/security/2014/10/suspected-russian-sandworm-cyber-spies-targeted-nato-ukraine/

[SA1] Adair, Steven, “Democracy in Hong Kong Under Attack,” Volexity, 9 October 2014, http://www.volexity.com/blog/?p=33

[SG1] Gallagher, Sean, “Year of the RAT: China’s Malware War on Activists Goes Mobile,” Ars Technica, 2 October 2014, http://arstechnica.com/security/2014/10/year-of-the-rat-chinas-malware-war-on-activists-goes-mobile/

Georgia Tech Information Security Center

www.gtisc.gatech.edu

Georgia Tech Research Institute

www.gtri.gatech.edu