Georgia Institute of Technology

EMERGING CYBER THREATS REPORT 2014

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

Georgia Tech Cyber Security Summit 2013

Introduction

With the Internet's pervasive reach into business, government, and private life, *it is unsurprising that cybercrime and espionage not only continue to evolve, but that new techniques are quickly adopted.*

Cybercriminals continue to develop new ways to monetize victims, while nation-state hackers compromise companies, government agencies, and non-governmental organizations to create espionage networks and steal information.

As we evolve as a society, changes to the way information technology supports business has caused fundamental changes to the threat landscape. For example, the vast majority of employees now bring mobile devices into the workplace and expect to be able to use their smartphones and tablets to work from anywhere. In addition, the adoption of cloud services has continued to accelerate. Companies are increasingly connecting to dozens, if not hundreds, of cloud services, and data is rapidly being exported outside the traditional security boundary of the firewall.

To better understand and combat threats associated with these changes, the United States and other countries must continue to support investigative and defensive research. Researchers from academia, the private sector, and government must continue to work together and share information on emerging threats and innovate ways to combat them.

The annual Georgia Tech Cyber Security Summit (GT CSS) on November 6, 2013, provides an opportunity for academia, private industry, and government to come together and prepare for the challenges we face in securing cyberspace and cyber-connected physical systems. By hosting the event, Georgia Tech aims to support efforts to develop new technologies and strategies that are effective against sophisticated cyber attacks.

The Georgia Institute of Technology is one of the nation's leading public research universities. As a multi-unit, campus-wide organization, the Georgia Tech Information Security Center (GTISC) works to drive the study of cyber security problems, issues, and solutions. The Georgia Tech Research Institute (GTRI) and dozens of labs across campus are engaged in research efforts focused on producing technology and driving innovation that will help secure business networks, government systems, and people's data. As a leader in cyber security research, Georgia Tech focuses on developing novel solutions to solve important problems. Atlanta is a major hub for cyber security and Georgia Tech has acted as an incubator for multiple companies that have succeeded internationally.

The discussion starts here. As key stakeholders, we all need to cooperate more effectively to combat the threats we face today and keep pace with their evolution.

At Georgia Tech, we understand this need and, leveraging in-house research and expertise, have compiled the following Emerging Cyber Threats Report, which includes insight and analysis from a variety of experts in cyber security. The Report and the Summit provide an open forum for discussion of emerging threats, their potential impact, and countermeasures for containing them.

In closing, 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 going forward.

— **Wenke Lee**
Director, GTISC

— **Bo Rotoloni**
Director, Cyber Technology and Information Security Laboratory, GTRI

Losing Control of Cloud Data

As companies move data to the cloud, trade-offs between security and usability hamper business

Highlights:

- Business data is regularly stored in the cloud without any security beyond that provided by the cloud storage firm
- While private-key encryption is an option, encrypting data in the cloud robs businesses of much of the cloud's utility
- Searchable encryption continues to have trade-offs between security, functionality, and efficiency

With the rapid shift from business-owned to employee-owned information technology (IT), companies increasingly have to face the challenges of protecting data dispersed among workers' devices and consumer-grade cloud services. The evolution of IT to a mobile, distributed ecosystem means that most companies have data seeping out into the cloud. Even though seven out of every ten IT managers have either confirmed or assumed that employees are saving business data to the cloud[1], few companies are doing anything about the issue.

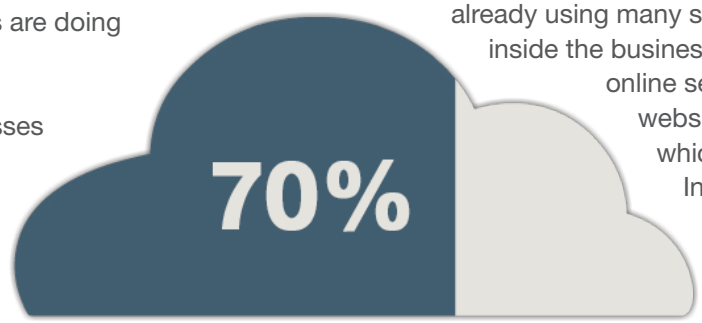
Yet, consumers and businesses are not the only ones using the cloud. The broad adoption of cloud services has allowed cybercriminals to use reputable services to bypass many of the digital defenses erected by companies. In addition, technically sophisticated cybercriminals have created their own cloud services, so that anyone intent on utilizing compromised systems can sign up and immediately lease a botnet or purchase other illicit services.

Against that backdrop, companies face a number of threats created by the ubiquity of the cloud.

File sharing and other cloud services still have questionable security

Companies continue to deal with the acceleration of so-called "shadow IT," the adoption of cloud services by employees who are seeking to make their work more efficient. With unknown and unmanaged services, productivity may improve, but important business data is left outside the protection of the corporate network, potentially placing the information at more risk. Dropbox, Box.com, and Google Drive are file-sharing services regularly used by employees that could allow outsiders to gain access to unencrypted data.

Companies first need to gain more visibility into the movement of business data. The average company's employees use more than 500 cloud services and most firms do not have a risk-based policy in place, according to data from Skyhigh Networks[2]. Cybercriminals are already using many services to exfiltrate data from inside the business or to gain access using trusted online services, such as reputable websites or file-sharing services from which malware can be downloaded. Inventorying a business's cloud use is a good first step.

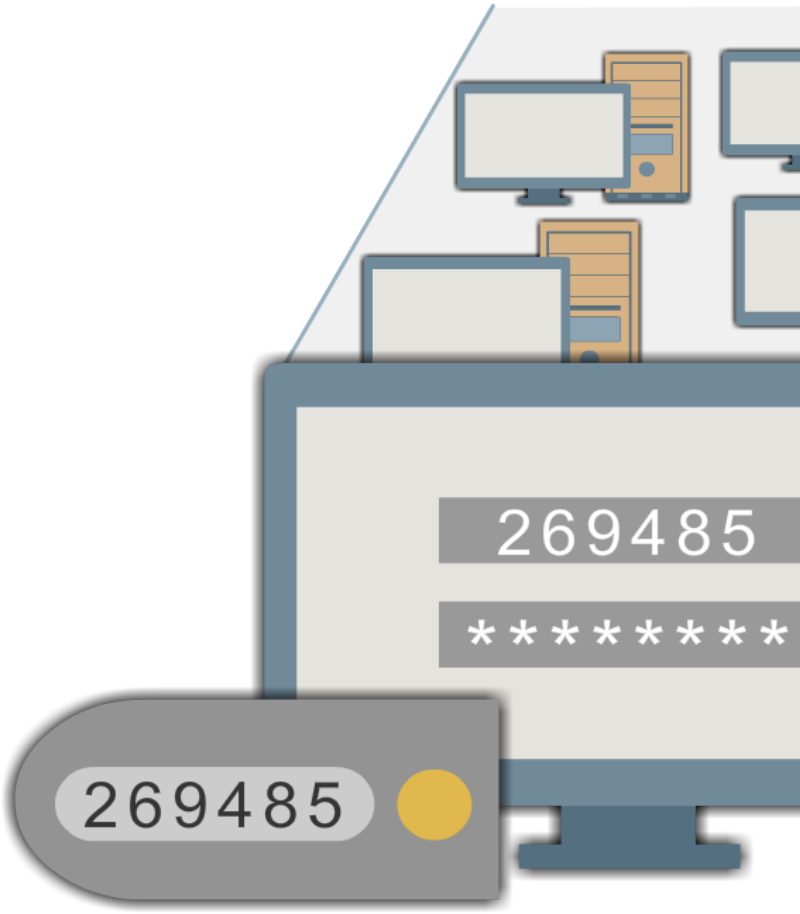


IT security professionals

[1] Marko, Kurt, "Backing Up Mobile Devices May Be A Nonissue," InformationWeek report, August 2013, http://reports.informationweek.com/abstract/2/11155/Business-Continuity/Research:-Backing-Up-Mobile-Devices-May-Be-A-Nonissue.html

[2] Skyhigh Networks, "2013 Cloud Adoption and Risk Report," company blog post, August 2013, http://info.skyhighnetworks.com/2013CloudAdoptionRiskReport_Registration_WS.html

should also look to secure access to sensitive data in the cloud by using two-factor authentication, making access to the data more difficult for attackers. Other threats exist as well: the cloud service can itself be compromised or become subject to a legal request by a sovereign government for data access. In those cases, companies need to implement encryption before the data is exported to the cloud, said Sasha Boldyreva, associate professor in the School of Computer Science at Georgia Tech.

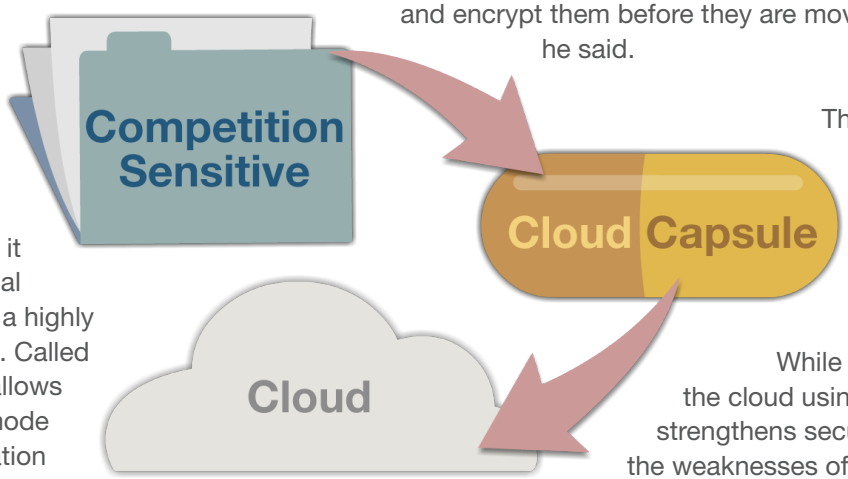


Protecting data against malware using the cloud

In 2009, a group of online hackers with links to China compromised Google and a number of other high-tech companies, stealing business information. Since then, nation-state-related attacks have only increased: From the Stuxnet attack on Iran's nuclear processing capability to the Syrian Electronic Army's hacktivism campaign to the ongoing collection of intellectual property by the Chinese[4].

In this environment, companies and government agencies need to protect information from data-stealing malware while still allowing employees to continue to do their jobs.

The cloud can actually help. Pairing the reliability of cloud storage with strong encryption can create a system that is both secure and reliable even when using the public Internet. Some companies have already created cloud proxies that encrypt information as it is moved to a file-sharing service, such as Dropbox.



Georgia Tech researchers have developed a system that can use the cloud for online storage, and by pairing it to a secure and separate virtual machine instance, can create a highly secure way of accessing data. Called "CloudCapsule," the project allows a user to switch into secure mode using the exact same workstation and access encrypted files stored in the cloud. To allow fast access to the stored files, each file is encrypted and stored separately, said Billy Lau, a research scientist with the Georgia Tech Information Security Center (GTISC).

"It allows the user to import sensitive files into this capsule and encrypt them before they are moved into the cloud," he said.

The system has transparent integration with Google Drive and Dropbox, but can be used with any cloud storage. While encrypting data in the cloud using CloudCapsule strengthens security, it retains the weaknesses of any encrypted file storage system: data is less accessible.

[4] Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017," Cisco Web site, Feb. 6, 2013, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html

Very Good Privacy

Encrypting information sent to, or through, a cloud provider has other applications as well. With increasing evidence that the National Security Agency and other nations' intelligence agencies have regularly accessed their citizens' e-mail and other data, encrypting messages before they are sent to the cloud should be a priority.

However, a popular option for data and e-mail encryption, Pretty Good Privacy (PGP), is not very useable. Georgia Tech researchers have created another, more user friendly option that can be used with popular cloud e-mail services. Dubbed "Very Good Privacy", the software overlays a transparent user interface layer, or secure overlay, allowing the user to interact with their e-mail service but quickly encrypt and decrypt data.

"Any plain text that the user types in is intercepted and encrypted before it goes to the e-mail service," said Lau. "The look and feel of the service is completely preserved and the workflow is unchanged."

Trade-offs between security, functionality and efficiency

While encryption can secure data stored in an online service, focusing on security alone can rob the company of much of the ability to use the data. Search, for example, is a key capability that companies want to continue to have even if their data is in the cloud. Yet, allowing an exact keyword search, a partial match, or the ability to order data by a specific field would require that data encrypted with regular encryption be reimported from the cloud and decrypted before performing any of these functions.

Searchable encryption is the right tool for the problem. However, most existing solutions are inefficient. The problem is that most researchers target very strong security at the loss of both functionality and efficiency. Yet, most businesses do not want to reduce the efficiency of accessing and processing their data and want secured data to approximate the utility of plain text.

Researchers at Georgia Tech have started with the functionality and efficiency desired for certain applications and found ways to achieve the best security under these constraints. "We proposed several efficient and provably secure searchable encryption schemes for various query types," Boldyreva said. "Most of the protocols do not require any change on the server side; the encrypted data is processed in the same way and with the same speed as the unencrypted data."

In particular, Boldyreva's research team proposed order-preserving encryption (OPE), which retains the order of the unencrypted information. Of course, to achieve efficient order-preserving functionality one has to sacrifice some security. The proposed scheme provides as much security as possible for such a protocol, according to Boldyreva.

Insecure But Connected Devices

The "Internet of Things" continues to expand, but security remains untested

Highlights:

- Detecting compromised and counterfeit devices continues to be resource intensive, though research on fingerprinting devices has advanced
- Companies need to evaluate the security of their suppliers as well as their own security
- Critical infrastructure companies must find better ways to secure their devices and prevent possible outages
- The Internet of Things will have an unprecedented view into people's lives, but will be difficult to secure after the fact, so security should be considered from the start

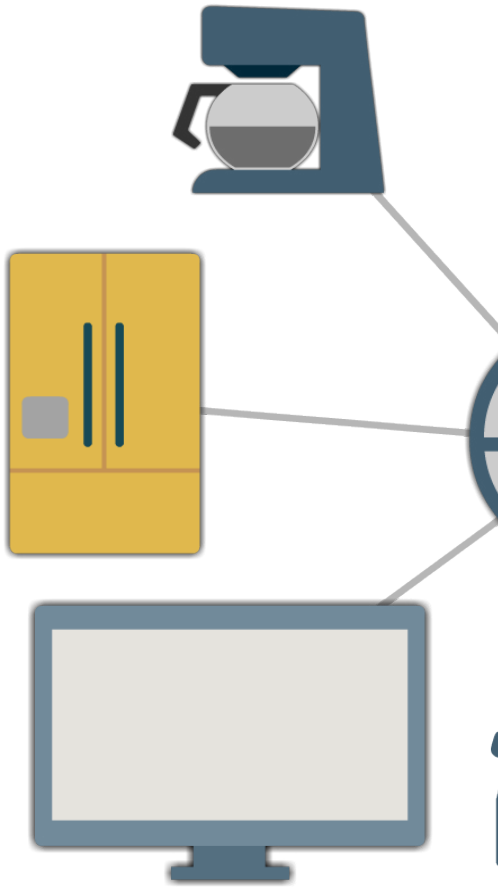
A plethora of devices now connect to the Internet. From embedded automotive systems to home automation to industrial control systems to consumer devices, the Internet of Things will only expand and become a more integral part of businesses and people's lives, making security and privacy important features of such systems.

Yet, security issues remain. Many device makers continue to make the same mistakes as the manufacturers of early operating systems. Industrial control systems, most of which were not intended to connect to the Internet, can frequently be found online and are vulnerable. Engineers designing the next generation of such devices do not typically think about advanced attacks, such as those using timing, power fluctuations, and other side channels.

"Over the next five years, you will see a plethora of devices connected to your home or business network," said Andrew Howard, a research scientist with the Georgia Tech Research Institute (GTRI). "And these can be used as avenues for attack."

Proliferation of insecure devices threatens the Internet of Things

Personal computers and servers, which dominated Internet-connected devices in the 1990s and early 2000s, have given way to smartphones and other mobile devices connected to the Internet. By the end of this year there will be more Internet-connected mobile devices—about 7 billion—than people on the planet, according to an annual prediction published by Cisco[4].



Yet, mobile devices are already being surpassed by sensors, consumer devices, industrial control systems, and other "things" that are quickly being connected to the network. Analysts estimate that in two years, between 15 billion and 25 billion devices will communicate across the Internet. This Internet of Things promises to allow companies to better monitor their business and for people to better monitor their life.

The security and privacy implications of such a pervasive network remains an open question, although this summer's revelations of the National Security Agency's data-collection efforts have revealed the extent to which routine data collection can be used to spy on people.

[4] Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017," Cisco Web site, Feb. 6, 2013, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html

"For most of these systems, you are taking some things that were never meant to be connected to a network and adding another channel that can be exploited or leak information," Howard said.

A significant problem for devices connected to the Internet will be in handling security updates without putting the devices at risk of compromise. Companies hesitate to upgrade critical infrastructure because of the potential repercussions if the update fails. Devices that are part of the Internet of Things, however, have to be managed remotely by the manufacturer. Moreover, the vast majority of devices will not be complex enough to run sophisticated security software, so companies will need to use network-level monitoring to detect compromises, said Raheem Beyah,

associate professor in the School of Electrical and Computer Engineering at Georgia Tech.

"It is likely that we will not have sophisticated software on these small systems to help us with security, so ways to determine the devices' identity on the network will be important," Beyah said.

Critical infrastructure in the crosshairs, but security still a question mark

Over the past three years a succession of security researchers have used Internet scans—or the easily accessible Shodan search engine—to find critical infrastructure systems that are connected to the Internet. In January, for example, two researchers from security consultancy InfraCritical used Shodan to hunt for dozens of industrial control system products, finding more than 7,000 servers and systems directly connected online including energy, water, and building-automation control systems[3].

The threat is not theoretical. In 2009, the Stuxnet attack used specialized knowledge of industrial control systems used by Iran for uranium processing to destroy much of that nation's refinement capability. The malware compromised the facility when contractors inadvertently carried in USB drives infected with Stuxnet. In another case, attackers attempted to access and compromise the network of one water utility more than 70 times in five months. Fortunately, the network was a honeynet set up for research purposes[13].

Georgia Tech researchers continue to study the security of embedded devices. While attacks on many consumer devices may not be critical, the knowledge of related classes of vulnerabilities can help attackers compromise more critical systems, said GTRI's Howard.

"What I'm worried about is someone taking one of these trivial attacks and escalating it to a more complex and critical system," he said.

Looking for Bad Devices in the Supply Chain

While waterhole attacks and social engineering are the latest techniques, worries still persist that attackers will compromise a device's hardware or software somewhere along the supply chain. Malware has already infected devices such as digital picture frames and network appliances, and detecting such compromises continues to be difficult.

[3] Boscovich, Richard, "Microsoft Disrupts the Emerging Nitol Botnet Being Spread through an Unsecure Supply Chain," http://blogs.technet.com/b/microsoft_blog/archive/2012/09/13/microsoft-disrupts-the-emerging-nitol-botnet-being-spread-through-an-unsecure-supply-chain.aspx, Sep. 13, 2012.

[13] Lemos, Robert, "Water-Utility Honeynet Illuminates Real-World SCADA Threats," Dark Reading, Aug. 2, 2013, http://www.darkreading.com/advanced-threats/water-utility-honeynet-illuminates-real-/240159393

Many current approaches are too expensive to scale to a widespread program of auditing devices. Physical hardware inspection and examination of electronic emissions of the devices require too much effort or time for a typical business. Another approach, using benchmarking software to profile the device, can be used for computers, laptops and some other devices, but requires the availability of such software for every device. With the proliferation of devices, creating benchmarking software for each platform is difficult, said Georgia Tech's Beyah.

At Georgia Tech, researchers are working on fingerprinting and profiling devices on the network using the traffic that moves to and from the device. The researchers boot the system, listen to the traffic it generates, and use network probes to determine if the architecture is compromised, and not what it is purported to be, said Beyah. By using a statistical approach, the researchers are able to determine if the device fits its profile.

The idea is to detect traffic that indicates that the device is counterfeit or malicious and then block future communications, he said.

"Instead of installing agent software, you can pick up the internal composition of these devices through the network traffic," Beyah said. "Is it a thermostat or a laptop that is trying to look like a thermostat?"

Attackers Adapt to Mobile Ecosystems

While mobile platforms have largely been safe for consumers and businesses, researchers and attackers are finding ways around the ecosystems' security

Highlights:

- As sensors—and not just computing platforms—mobile devices bring a new set of threats, including allowing malicious software an unparalleled look into victims' lives
- Employee-owned devices make platform-specific security difficult, suggesting that focusing on protecting data may be more effective
- Researchers and attackers have found ways to bypass the inherent security of the "gated community" of app stores
- The implications to society of tracking ubiquitous mobile devices is not well understood, and U.S. courts have not yet come to a consensus on government access to the data

By the end of this year, there will be more Internet-connected mobile devices than people on the planet, with four out of five workers using their personal mobile devices to do work[5]. While personal computers defined how people worked in the last decade, this post-PC decade will be defined by mobile devices and on-the-go productivity.

Even though malware is still much less a problem for mobile devices than it is for PCs, the threats are quickly following workers onto mobile platforms. In addition, man-in-the-middle attacks are increasingly common because mobile users are typically less leery of connecting to untrusted networks[16].

[4] Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017," Cisco Web site, Feb. 6, 2013, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html

[14] Lemos, Robert, "4 Mobile Device Dangers That Are More Of A Threat Than Malware," Dark Reading, Sept. 11, 2013, http://www.darkreading.com/mobile/4-mobile-device-dangers-that-are-more-of/240161141

Employee-owned devices change the security model

Mobile devices have changed the dynamics of IT security in the workplace. The bring-your-own-device (BYOD) trend introduces two different threats to companies: relatively insecure devices are entering the network and data is increasingly stored on personal devices. First, because the platforms are owned by the employees, assuring that the device is secure is more difficult, as such malware can use smartphones and tablets as a launchpad for attacks into the corporate network. Second, because employees are using their devices for work, corporate data will be stored in these relatively insecure environments.

"If you get an infected device or phone coming into your business, your intellectual property could be stolen," said

Chuck Bokath, senior research engineer at the Georgia Tech Research Institute (GTRI). "It is hard for IT professionals, the CIO, or the CTO to get their arms around it at this point."

BYOD is not going away, however, because the productivity gains and cost savings are too alluring for most companies. Companies will have to take a variety of approaches to locking down—or locking out—devices, from compartmentalizing trusted apps and sensitive data using secure containers to using network access controls to bar untrusted devices from accessing parts of the network.

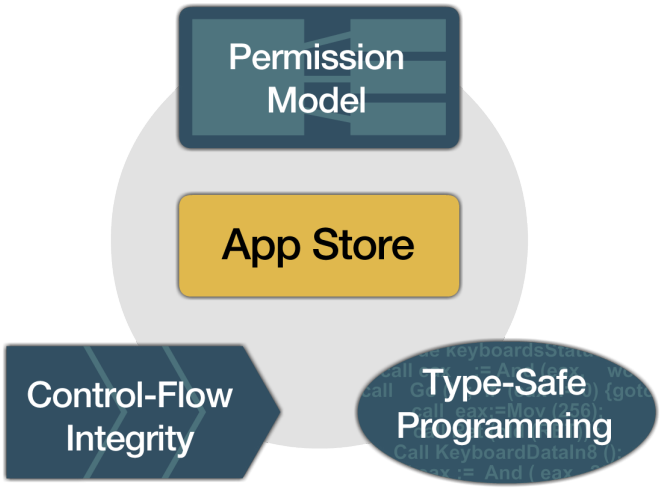
Gated app stores not a perfect defense

The creators of mobile devices have attempted to learn from the mistakes of computer operating system manufacturers. Google added a permission-based security model, a variety of security controls, the ability to revoke applications, and eventually an automated system of vetting applications submitted to its application marketplace, Google Play. Apple adopted a much stricter approach to the gated community, keeping tight control over certain system functions and checking applications for potential malicious behavior from the start.

Users that refrain from jailbreaking their phones and only use a major application marketplace have generally been safe. Current rates of mobile malware infections in North America run less than one percent of all devices, with jailbroken smartphones representing the most at-risk group of devices[12].

Yet, researchers and attackers have found ways of getting around the defenses provided by both Android and iOS ecosystems. At the USENIX Security Conference in August 2013, four researchers from Georgia Tech showed that intentional vulnerabilities could be added to an application without being detected by Apple's vetting process. By exploiting the vulnerabilities at a later date, an attacker could gain access to the device.

"We have shown that the regular app store review process is not able to prevent the introduction of a malicious app," said Tielei Wang, research scientist with GTISC and one of the authors of the USENIX paper.



[4] Lemos, Robert, "Companies Need Defenses Against Mobile Malware," Dark Reading, Nov. 8, 2012, http://www.darkreading.com/advanced-threats/companies-need-defenses-against-mobile-m/240062687

A number of countermeasures could help restore the security of the application marketplace model, including a more fine-grained permission system, control-flow integrity checking, or mandating that developers use a type-safe programming language. How likely these security measures are to be adopted remains an open question.

Mobile devices leak user data without controls

Malware and technical hacks represent a significant threat to the users of mobile devices, but a far more pervasive threat is the legal use of data collected from smartphones and tablets. When former National Security Agency contractor Edward Snowden revealed in June 2013 details of the data collection practices of the intelligence agency, the extent of the NSA's PRISM program for gathering data on persons of interest surprised most watchers. However, the program only scraped the surface of the data available for potential analysis.

Given that mobile devices double as sensors and tracking platforms that consumers voluntarily carry with them, the wireless carrier, manufacturer, and a plethora of application developers regularly collect data about the user from the device. Much of that data can be used to track the user, although U.S. courts have split on whether law enforcement can request such information without a warrant[11].

"In short, in human history, people have never carried tracking devices and now they do," said Peter Swire, the Nancy J. and Lawrence P. Huang Professor in the Law and Ethics at Georgia Tech. "So as a society, and as a creator of the technology, we have to decide when that location information goes to different holders and when that information can be used for other purposes."

Yet, even if the courts require that law enforcement agencies obtain a warrant to gain access to the historical location of the phone, such a ruling will be unlikely to rein in the amount of information extracted from the phone by application developers.

Malicious USB charger allows hacking

Another way that attackers can circumvent the gated mobile ecosystem is by leveraging security vulnerabilities in everyday activities, such as charging a device. At the Black Hat Security Briefings in July 2013, three Georgia Tech researchers demonstrated how attackers could create a hardware device that appears to be a USB charger, but in reality compromises any iPhone that is connected to the hardware.

Such devices could be placed in airports or hotels to automatically compromise phones, which would then connect back to command-and-control servers, said Billy Lau, a research scientist with GTISC.

"There is no question that someone could create a charger that looks like the real thing," he said.

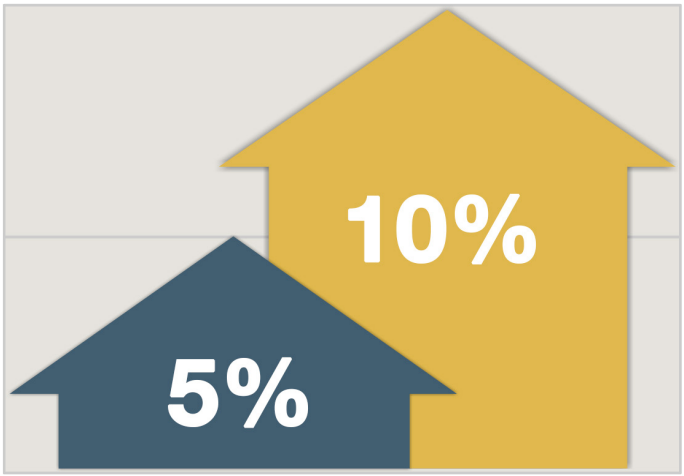
[11] Sengupta, Somini, "Warrantless Cellphone Tracking Is Upheld," New York Times, July 30, 2013, http://www.nytimes.com/2013/07/31/technology/warrantless-cellphone tracking-is-upheld.html

Costs of Defending Against Cyber Attacks Remain High

Mitigating the risk of cyber attacks continues to be uncertain and costly, but gaining better visibility into threats and mitigating specific risks can help

Highlights:

- Chasing technology and creating multiple layers of static defenses has driven up security costs
- Companies need to focus on gaining visibility into their networks and the external threats targeting their business
- Shifting focus from devices to data can simplify defensive concepts and better cope with the bring-your-own-device (BYOD) trend, but usability continues to be a problem
- While the market for cyber insurance is growing, fundamental problems continue to prevent broad acquisition of policies to mitigate risk



Over the past decade, companies have moved from deploying a simple firewall, antivirus software, and patch deployment system to adopting a variety of other technologies: security information and event management (SIEM), data loss prevention, identity and access management (IAM), application firewalls, and more recently, mobile device management (MDM). Following the mantra of defense-in-depth, the more layers of technology placed between the attackers and the business, the better.

Yet, a technology-oriented focus has driven the cost of security higher for companies. Despite slow economic growth, IT security budgets will climb five to ten percent higher in 2013. Surveys in the past year have found half[9] to two-thirds[8] of IT security professional expect budgets to increase in the coming year.

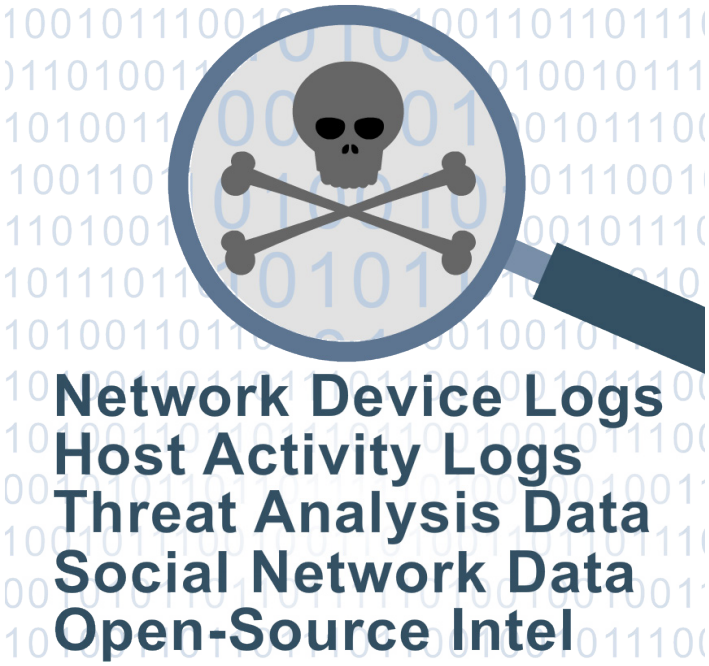
Reducing cost while protecting the business will require a more data-driven approach to security. Researchers and businesses that focus on gathering more information on their security state and their current threats can better protect their networks and data while holding down costs. In addition, moving the focus of security from the device to a business's data can simplify defenses. Finally, cyber insurance can act as a safety net for companies, although questions remain over the efficacy of policies and coverage.

Threat intelligence is necessary, but still in early stages

Finding information on attackers is not difficult: blacklists, open-source intelligence, logs from a variety of network devices, malware analysis, social networks and other sources can all give defenders some insight into attackers' techniques, identities and motivations. However, making sense of that data and turning it into intelligence relevant to a specific company or target is difficult. In addition, unless the information can be delivered to the right people in a short amount of time, it may lose value quickly.

[8] SC Magazine Poll, "Security Budgets in 2013," SC Magazine, http://www.scmagazine.com/security-budgets-in-2013/slideshow/1157/#1

[9] Presti, Ken, "Report: Security Budgets Trending Upwards For 2013," CRN, Dec. 7, 2012, http://www.crn.com/news/security/240144099/report-security-budgets-trending-upwards-for-2013.htm



There are different ways to address attack vectors. Companies can discover and map their networks and assets, then prioritize defenses by value, vulnerability, and criticality. They can also focus on the attacker, using kill-chain analysis to determine the steps necessary to target the company's valuable intellectual property. Rather than simply attempting to keep the attacker out, such an approach gives the company multiple opportunities to mitigate an attack.

The goal is to quickly determine the current state of the network and assets, what the attacker may be targeting, and the pre-determined business impact if the attack succeeds. The process should help defenders prioritize incident response, said George "Fred" Wright, a principal research engineer at the Georgia Tech Research Institute (GTRI).

"We should do better than just a gut feeling," he said.

While there has been some interest on creating a single metric of risk, essentially a "threat barometer" for cyber security, such an oversimplification can remove any actionable content and cause apathy, rather than focus a defender's efforts, says Wright. The most well-known indicator of threat, the U.S. Department of Homeland Security advisory system for terrorism risk, was eventually scrapped; more attacks happened while it was yellow than while it was orange, and no attack occurred while it was red, a representation of the highest threat level[10].

Data loss prevention shows promise, but security context remains a problem

With a menagerie of employee-owned devices connecting to business networks, securing every device is no longer practical or desirable: the proliferation of devices is difficult to support and managing a worker's device raises sticky privacy issues. For those reasons, many companies are focusing on controlling where their data is sent and stored. Data loss prevention technologies promise to focus on the data and protect sensitive information from being leaked or stolen.

Determining the context of the data remains a challenge, leading to a high incidence of false alarms. A nine-digit number, for example, could be a social security number, or it could be just a nine-digit number. Add to that the difficulty posed by encrypted or obfuscated data, and data loss prevention systems need to evolve if they are to help reduce the cost of security, said Andrew Howard, research scientist with GTRI.

"If I'm trying to steal data, data loss prevention is not going to keep me from stealing it," he said. "But currently, data loss prevention is effective at keeping good users from making a mistake."

More companies are taking the first step and creating data-classification policies and estimating the costs associated with the loss of data. Researchers are focusing on aiding the classification of data and making data tagging easier.

"Companies are becoming more aware of how sensitive their data is," said Howard. "Five years ago, most companies had no idea of what they had. It is a much bigger corpus of data than most realize."

With risk hard to quantify, insurance remains problematic

Insurance has always been a way for companies to offset the risk of a catastrophic event. Due diligence and requirements mandated by insurance firms are credited with increasing the safety and security of many industries, but a lack of actuarial data on cyber attacks, the difficulty in quantifying damages, and disagreement on which se-

[10] Schneier, Bruce, "Why terror alert codes never made sense," CNN, Jan. 28, 2011, http://www.cnn.com/2011/OPINION/01/28/schneier.terror.threat.level/index.html

Companies buying cyber security insurance

curity measures actually reduce the risk of a breach all make cyber insurance hard for many companies to justify insurance as an expense. In 2012, the number of companies buying cyber insurance policies increased by a third compared to the previous year, with educational institutions and professional service organizations accounting for much of the increase, according to risk management firm and insurance broker Marsh[5].

However, a great deal of confusion remains as to what is and is not covered. In August 2013, insurance company Liberty Mutual sued the Schnuck supermarket chain after hackers stole up to 2.4 million credit card numbers from the retailer resulting in eight class-action lawsuits and fines from banks and credit card companies. The supermarket claims that the lawsuits and fines should be covered, but Liberty Mutual argues that the costs are "intangibles," which are not covered[7].

"When you pick up the paper every day and read about a breach—not at a mom-and-pop shop, but at a major company—you understand that no one is immune to attack," said David Norfleet, senior vice president of professional liability at Starr Indemnity and Liability Co. "We frequently walk away feeling like we still don't have the solution."

GTRI is working with Starr and other insurance companies to clarify damages, define good security practices, and set standards around coverage options.

Supporting information sharing

Worries over giving rivals an advantage as well as the legal and business implications of admitting to being successfully compromised have limited companies from sharing information on attacks. A threat intelligence effort by GTRI, dubbed "Apiary," allows participants to submit evidence of potential attack, exchange indicators of compromise (IOCs), and get automated analysis of any malware used in the attack—all through an anonymous system.

"We found that most people would be unwilling to work with us if we were not Georgia Tech," said Chris Smoak, a research scientist at GTRI.

The Apiary system analyzes the malicious software, or malware, used by attackers to compromise and control systems, giving companies fast information on the capabilities of the attack and linking the programs to previous attacks. Apiary can already detect malicious attacks before security companies and public intelligence sources, said Howard.

[5] Marsh, "Number of Companies Buying Cyber Insurance Up by One-Third in 2012: Marsh," press release, March 14, 2013, http://usa.marsh.com/NewsInsights/MarshPressReleases/ID/29878/Number-of-Companies-Buying-Cyber-Insurance-Up-by-One-Third-in-2012-Marsh.aspx

[7] Walker, Danielle, "Insurer to Schnucks: We won't pay for lawsuits related to your breach," SC Magazine, August 20, 2013, http://www.scmagazine.com/insurer-to schnucks-we-wont-pay-for-lawsuits-related-to-your-breach/article/307960/

Information Manipulation Advances

Online recommendation and reputation systems increase in importance while threats to them mature

Highlights:

- As companies and governments rely more on data and intelligence to operate efficiently, information manipulation will become an increasingly important attack
- With reputation increasingly being used to make security decisions, attackers will continue attempts to poison or whitewash reputation
- Using cross-site request forgery, unscrupulous website owners can inject higher-value content to poison the profile of visitors and profit by fooling advertising networks
- Techniques for using information pollution and manipulation could be used to hide or camouflage attacks

Businesses and governments have increasingly focused on collecting and analyzing a wide variety of data to make better decisions. Retailers and financial houses, for example, use big data analytics to make better business decisions and be more responsive to demand. Google and other search engines use information on users' browsing habits to inform search query results and determine what advertisements are displayed. Government agencies, such as the National Security Agency, collect and process information to look for threats to national security.

With this information driving business and security decisions, attackers will increasingly attempt to game these analysis systems in their favor. Google has already faced such attacks in the form of black hat search engine optimization (SEO). Other attacks could attempt to manipulate different aspects of the information economy, such as influencing the personalization algorithms used by many services. The designers of such analysis and correlation systems must account for attackers' efforts to poison data.

With reputation becoming increasingly important, attackers will focus on gaming the system

Companies are increasingly focusing on reputation as a way to keep out many security threats. Firms use blacklists generated from the monitoring of a variety of malicious activities to block potentially hostile websites. More fine-grained reputation systems are also being developed, from rating the trustworthiness of an application or service to grading the security of a partner.

Information manipulation and pollution attacks can be used to undermine such reputation-based defenses. At the broadest applications, fraudsters have already gamed review services by using reputation whitewashing to bury bad reviews and SEO techniques to make sites seem more popular. Website blacklists can also be evaded by quickly changing domains or, as is increasingly the case, using legitimate but compromised sites.

While information service providers can fight such techniques by checking their sources for pollution or manipulation, everyday users need an increasingly suspicious attitude, said Wenke Lee, professor of Computer Science and director of the Georgia Tech Information Security Center (GTISC).

"Consumers who are not savvy about the quality of information online can be easily misled," Lee said. Greater transparency in how information and intelligence providers create their reputation systems could help users be more savvy, he said.

Poisoning personalized services can profit attackers

From news to advertising to book recommendations, online services are increasingly personalized. Misrepresenting the user's interest can be profitable. Researchers from GTISC demonstrated a technique using cross-site request forgery (XSRF) to manipulate the data collected by third party services, such as advertising networks, online bookstores, and search engines. Using this technique attackers can influence the personalized results returned by a service provider. In a paper presented at the USENIX Security Conference in August 2013, GTISC researchers showed that they could manipulate the personalized results presented by Amazon, Google, and YouTube. By using XSRF, the researchers injected HTML code to make it appear that the users had clicked on and showed interest in certain content.

This technique could be used by rogue publishers to fool advertising networks into delivering more expensive ads directed to high-value customers, said Wei Meng, a researcher at GTISC and one of the authors of the USENIX paper.

"The publisher could utilize this technique to inject some of the most expensive content into the webpage, essentially changing the interests of the user," he said.

Defending against the attacks is difficult, because effective defenses would also hamper personalization, Meng said.

Manipulating information can be an attack on Big Data analytics

Over the next decade, companies and government agencies will analyze an increasing amount of data to derive intelligence that can be used to streamline operations, make more informed decisions and detect anomalies that indicate a threat. As the use of such big data analytics spreads, attackers will have to find ways to hide from statistical analysis and anomaly detection.

Information manipulation will likely be the attackers' strategy, said GTISC's Lee. By polluting data in certain ways, such as slowly creating a wider variance in some metrics, a knowledgeable attacker could modify an analysis platform's threat model and cause it to consider anomalous behavior as normal. Or, an attacker could create a lot of fake attacks, causing false alarms and wasting the time of human analysts.

"How do we know that the data used for analytics has not been polluted?" Lee asked. "This threat represents a battle that we will have to fight in the next five to ten years."

Defending against such attacks requires that defenders be able to detect very slow changes in the data and be able to flag such changes as suspicious.

Georgia Tech Information Security Center

www.gtisc.gatech.edu

Georgia Tech Research Institute

www.gtri.gatech.edu