Georgia Institute of Technology

EMERGING CYBER THREATS REPORT 2013

Georgia Tech Cyber Security Summit 2012

Presented by the Georgia Tech Information Security Center
and the Georgia Tech Research Institute

Introduction

Innovative research *can help illuminate the security problems facing people, businesses, and governments online as well as propose and evaluate new defenses.*

In the past year, much has changed in cybersecurity. Attackers aligned with national agendas have focused on targeting businesses and governments in attacks that have resulted in the leakage of sensitive and critical data. Employees bringing consumer technology into the workplace—most notably, smartphones and tablets—have led to increased productivity, but at the same time have undermined the security practices at companies which had, in the past, focused on securing their perimeter. The movement of business and consumer data to the cloud has often led to the increase of the overall security of such information but created large stores of important data that will lure attackers.

If we are going to prevent motivated adversaries from attacking our systems, stealing our data and harming our critical infrastructure, the broader community of security researchers—including academia, the private sector, and government—must work together to understand emerging threats and to develop proactive security solutions to safeguard the Internet and physical infrastructure that relies on it.

The annual Georgia Tech Cyber Security Summit (GTCSS) on November 14, 2012, provides an opportunity for these stakeholders to come together and prepare for the challenges we face in securing cyberspace and cyber-connected physical systems. By seeking to engage a broader audience, Georgia Tech remains at the center of 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. The Georgia Tech Information Security Center (GTISC), 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, industrial controls, 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 cybersecurity, and Georgia Tech has acted as an incubator for many companies that have succeeded internationally.

The discussion starts here. As key stakeholders, we all need to cooperate more effectively to combat the large-scale threats we face today and keep pace with constantly evolving attacks.

At Georgia Tech, we understand this 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 from the IT security industry and academia. The Report and the Summit provide an open forum for discussion of emerging threats, their potential impact, and countermeasures for containing them. We invite you to learn more about our work in cyber security and to connect with our experts to understand and address the challenges we face in securing cyberspace.

— **Wenke Lee**
Director, GTISC

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

Information Manipulation

Understanding How Automated Information Systems Can Increase the Threat

Highlights:

- Information manipulation gives attackers the ability to influence what a victim sees on the Web in a way that survives cleaning the client machine.
- The act of personalizing search results and news feeds leads to a narrowing of viewpoints, a form of automated censorship.
- Attempts to increase the uptake of a given viewpoint can be detected based on certain characteristics.

Large parts of the modern Internet rely on algorithms that sift through information and deliver to the user what the system thinks the user wants. Increasingly, a variety of attackers are looking for ways to manipulate these search results and other forms of automated filtering to influence what the end-user sees. From cybercriminals focused on black-hat search engine optimization to authoritarian regimes focused on censorship, controlling the content filtered by these programs allows attackers to control what information reaches a user.

By understanding the automated mechanisms that control what information is presented to users and how these mechanisms affect user privacy and security, researchers can find ways to harden these mechanisms against manipulation. "We cannot just blindly believe that the algorithms are foolproof," said Wenke Lee, professor at Georgia Tech's College of Computing and director of GTISC.

Beyond Vanilla Search-Engine Poisoning

Search-engine poisoning attempts to manipulate the results of queries by creating malicious networks of pages that link to one another to boost the ranking of the target page—typically, a page that attempts to install malware. While information intermediaries, such as search engines, use a number of inputs, two attributes that matter most are the reputation of the sites that link to the result and the user's search history.

Attackers are already manipulating reputation. Rather than using their own botnets to create fly-by-night web sites—which typically have a low reputation—cybercriminals are compromising legitimate sites with code to present links to malicious destinations, increasing those targeted sites' page ranking. A more common attack in the future will use cross-site scripting to inject links from legitimate sites to malicious destinations, without the need for total compromise.

Manipulating a victim's search history may be next. Using cross-site request forgery, researchers have been able to enumerate and even modify a user's search history. The benefit to the attacker is that such manipulations, when stored as part of an online profile indexed by a cookie, can survive many defensive measures. Such attacks can significantly change input to a search engine's filtering algorithm, changing which sites a person sees.

"If you compromise a computer, the victim can always switch to a clean machine and your attack is over," Lee said. "If you compromise a user's search history and hence his online profile, the victim gets the malicious search results no matter where he logs in from."

Characteristics of Bad Behavior

Users can impact the behavior of the algorithms used to identify popular content in other ways as well. On Twitter, Facebook, and other social networks, legitimate and malicious users can skew the popularity of search results by liking or retweeting certain posts.

These sorts of behaviors can arise from the natural relationships between a source of information and a follower, whether between a celebrity and a fan, a company and its PR firm, or a politician and a loyal supporter. However, these behaviors could also be fabricated as a way to manipulate social networks and unnaturally amplify a certain message, said Nick Feamster, associate professor at the Georgia Tech School of Computer Science.

"We determine whether a sequence of messages constitutes manipulation based on the patterns of how these messages are disseminated," he said. "Often, multiple social network accounts can be used to falsely create the impression of multiple independent viewpoints, when in fact one 'ringleader' may be behind a set of messages."

Research at Georgia Tech has shown that such attacks on social networks, whether by propagandists or others, have certain characteristics.[1] A high volume of messages over a short period, quickly reposting content with few changes, and colluding with others to send the same message, all tend to differentiate a propagandist from more neutral users. This research could help social networks control accounts that try to abuse algorithms that determine popularity and decide which posts, tweets, or news items are forwarded to a wider audience.

Personalization Leads to "Filter Bubbles"

Other research at Georgia Tech has investigated the impact of personalization on the type of information that users receive. Search engines and other information intermediaries filter results based on dozens of attributes, some of which include search history and geography. The winnowing down of results, known as filter bubbles, can deliver desired content more quickly, but can also block the user from receiving a more diverse range of results. RSS feeds and searches can create filter bubbles dependent on geography. While such personalization can deliver the most relevant local news to a user, it also results in a lack of diversity and a local bias. Depending on the country, for example, 20 to 30 percent of news sources accounted for 70 to 80 percent of the articles, GTISC researchers have found.

One way to deal with these emergent characteristics of personalization is to educate users and reveal information that they are missing, said Georgia Tech's Feamster. "This type of personalization can be acceptable or even beneficial, as long the user is aware that it's happening."

Filter Bobble De-Personalizes the Filtered Internet

To demonstrate the impact of filtering techniques, a research team at GTISC created Bobble,[2] a browser plugin that distributes a user's searches to hundreds of nodes across the Internet with the intent of depersonalizing their search results. A user will no longer see just the results that the algorithm determines are best suited to their individual interests, but a set of results created by combining the outcomes of searches across hundreds of nodes.

[1] Palis, Courteney, "How To Spot Twitter Propaganda: Study," http://www.huffingtonpost.com/2012/06/01/how-to-spot-twitter-propa_n_1563325.html, June 3, 2012.

[2] http://bobble.gtisc.gatech.edu/

Insecurity of the Supply Chain

Hard to Detect, Expensive to Fix, and a Policy Nightmare

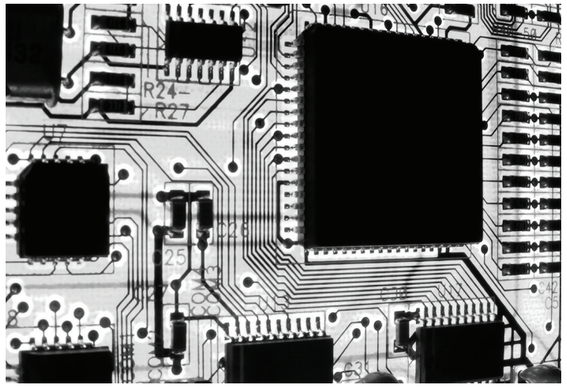
Highlights:

- Supply chain insecurity is both hard to detect and expensive to defend against.
- Detecting firmware changes will continue to remain difficult.
- On an international policy level, supply chain issues will continue to be an intractable problem.

Since 2005, the United States has ramped up its seizures of counterfeit networking hardware and other information technology from China, concerned with both the impact on major U.S. companies and the possibility of having such technology become part of the critical infrastructure. In 2010, law enforcement and homeland security officials seized $143 million worth of technology assets in an international operation that resulted in 30 arrests.

In 2012, the security of the supply chain has become a major worry. In an October report[3] on the danger posed by products of Chinese telecommunications firms Huawei and ZTE, the House Select Committee on Intelligence made a number of recommendations, including a strongly worded missive to U.S. companies to avoid Chinese networking hardware.

"Private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services," the report stated. "U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects."



Combating Counterfeit and Compromised Products Is Expensive

For U.S. companies, there are few good solutions to the problem of supply-chain insecurities. "I would say that we are in trouble," said Andrew Howard, research scientist with the Georgia Tech Research Institute. "This is a problem that is extremely expensive and difficult to solve. 'Solve' may not even be the right word." Currently companies take one of three strategies, said Howard.

The majority do nothing at all besides limit their purchases to trusted vendors. These companies may do some network monitoring to make sure that the devices are not acting maliciously, but the strategy will most likely fail to catch any attack through the supply chain.

A much smaller set of companies may do random tests on devices, selecting appliances during distribution and installation to test for indications that they may contain extra components or serious vulnerabilities. Such methods are better than doing nothing at all, but are still woefully inadequate, Howard said. While counterfeit hardware or hardware attacks are potentially detectable in spot checks, finding changes is a difficult, time-consuming process. Moreover, only a single device needs to escape detection to compromise an entire network, Howard said.

A handful of companies are taking a far more paranoid approach and not trusting the supply chain at all. Any device that comes in through the front door is assumed to have already been compromised, and the companies continuously monitor the devices for any behavior that could indicate that the product has been tampered with. This strategy, however, is not a realistic solution for the vast majority of companies due to the cost, technology, and time required to implement the necessary processes.

The Supply Chain Problem is a Global Problem

While the United States likes to point the finger at China for its attempts to steal intellectual property, China has major supply-chain issues of its own. In 2011, as part of Microsoft's investigation into the Nitol botnet,[4] its employees bought 20 computers in the local markets in China. None of the buyers were given a choice between a legal or counterfeit version of Windows, but all ten laptops and ten desktop systems had a counterfeit version of the operating system installed.

The problems did not stop there: Every system had been configured in such a way as to reduce security, and four of the systems already had malware installed, said Richard Boscovich, senior attorney with Microsoft's Digital Crimes Unit.

These are not isolated incidents but a pervasive problem that will hinder China's ability to grow its information technology market and could cause increasingly sensitive Western companies to question the security of the supply chain in that country.

"The supply chain clearly is broken," Boscovich said. "It's totally insecure, and it is very easy for criminals to inject what they want into that supply chain."

Detecting in Software Versus Hardware

Strategies to detect attacks through the supply chain tend to focus on analyzing the device or analyzing its behavior. Georgia Tech researchers are looking at more proactive strategies, finding ways to attest to the foundational components of an information-technology system so that modifications—even if made at the factory—can be detected.

Similar to the creation of the coming Secure Boot technology in Windows 8—which will prevent the modification of the firmware on PC systems—such security technology could allow a company to know that the software on a system remains trustworthy.

"The question is whether we can put hidden functionality into a device to know that it is our device," Howard said. Other methods under investigation include using non-destructive screening to identify the signatures of components and detect components that do not match known profiles or match the profiles of known counterfeit components.

Yet, progress remains slow because of the size of the problem and the lack of easy solutions, according to Howard. "It is going to take a bad event to have the momentum necessary to fully tackle the problem," he said.

U.S.-China Policy Impasse

Informal discussions on cybersecurity between the U.S. and China highlighted supply chain problems and underscored the difficulties in making progress. While the talks—organized by the China Institute of Contemporary International Relations (CICIR) and the Center for Strategic and International Studies (CSIS)—offered the hope of better communications between the two nations on cyber issues, they failed to even discuss cyber espionage—currently a major issue.[5]

"Both CICIR and CSIS note a 'mirror imaging' of supply chain concerns between the two governments," a summary prepared by the two groups stated. "Both believe that the other will seek to exploit the supply chain to introduce vulnerabilities into networks and infrastructures."

[3] "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf, Oct. 8, 2012.

[4] 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.

[5] CICIR & CSIS, "Bilateral Discussions on Cooperation in Cybersecurity China Institute of Contemporary International Relations, "http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf, June 2012.

Mobile Security Reanalyzed

Mobile Malware Continues to Be Developed for Android, but the Ecosystem Works Well to Keep Devices Secure

Highlights:

- Malicious and privacy-undermining applications for Android will continue to grow quickly, as cybercriminals use toll fraud and other mechanisms to turn compromised devices into cash sources.
- Well-vetted app stores will continue to be a good first defense against malware and have kept infection rates in the U.S. low.
- Infrequent patching by carriers and manufacturers continue to leave mobile devices vulnerable.
- Mobile wallets will face further scrutiny and slow adoption until their security is proven.

Mobile-device security continues to be a large question mark. While the operating systems on mobile devices are not necessarily more secure than Windows or Mac OS X, the ecosystems surrounding phones—with managed app stores and the ability to remove malicious apps from devices—has made it more difficult to exploit a large number of devices. Moreover, monetizing compromised mobile devices has been difficult in the U.S., if not abroad.

Nevertheless, the large population of smartphones and tablets is an opportunity that attackers cannot afford to ignore. Last year, shipments of smartphones surpassed PCs, and in 2012, mobile devices became the most popular way to access the Internet. The devices have also become a gateway into corporate networks as employees bring their own devices into work.

The ubiquity of mobile devices means that security researchers and cybercriminals alike will continue to test the security of the platforms. We expect novel attacks and new ways to monetize mobile devices to emerge.

iPhone and Android: Both Equally Safe (or Insecure) in Reality

Malware writers have moved from taking a casual interest in mobile platforms to trying to create a viable business model, especially focusing on devices based on the Android operating system. The number of malicious and suspicious apps grew to 175,000 at the end of September 2012, up from 30,000 in June, according to security firm Trend Micro.[6]

Yet the exponential growth of malicious Android apps has not translated to increased risks for most users. By analyzing three weeks of DNS traffic from a large cellular provider, GTISC researchers have found that only a very small number of devices—about 0.002%—are showing signs of infection in the United States. The research also showed that the detections of malicious applications occur well after their peak activity, suggesting that reactive security measures—such as removing the program from storefronts and publishing antivirus signatures—had little initial impact. Nonetheless, such measures likely prevent the software from spreading widely.

"Largely, it appears that the mechanisms in place appear to be working," said Patrick Traynor, assistant professor with Georgia Tech's School of Computer Science. "Even though malware does get into the market, people don't seem to be downloading those apps."

This research focused on users in the United States, however. Security firms have found a much higher rate of infection in other geographies, particularly China and Russia, where infection rates are as high as 40 percent,[7] according to Lookout, a mobile security firm. Like the GTISC researchers, Lookout found less than 1 percent of U.S. devices infected by malware.

[6] Lemos, Robert, "Android Malware Takes off, Mostly Outside the U.S.," http://www.eweek.com/security/android-malware-takes-off-mostly-outside-the-u.s./, Oct. 22, 2012.

[7] Higgins, Kelly Jackson, "Toll Fraud Tops Mobile Malware Threats," http://www.darkreading.com/mobile-security/167901113/security/attacks-breaches/240006901/toll-fraud-tops-mobile-malware-threats.html, Sep 6, 2012.

Browser Interface Still Lacks Security Indicators

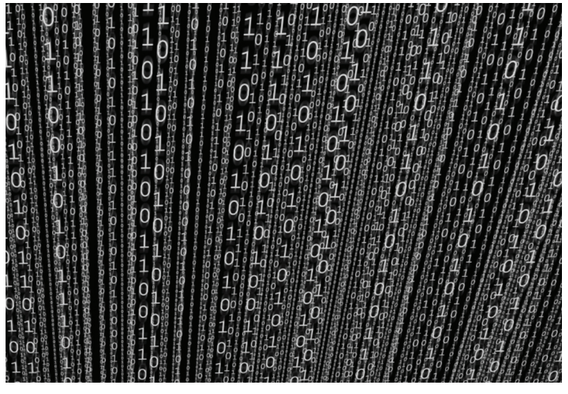
The tension between usability and security has led browser developers to sacrifice most security indicators on smartphones, where screen real estate is at a premium. The result is that mobile users are three times more likely to visit a phishing site than desktop browser users.[8]

Building on last year's Emerging Cyber Threats Report, researchers at GTISC studied the degree to which mobile browsers conformed to W3C guidelines, finding that many security indicators are missing, including extended certificate validation, undermining any value of the technology for mobile users. Popular mobile browsers, including iPhone Safari, Opera Mini and Mobile, Windows IE, and Safari on the iPad 2 do not allow users to see information identifying a Web site, such as certificate data.[9]

"Each of the browsers have decided in different ways which factors to include, and virtually all of them are susceptible to attacks which not even an expert could detect because subtle information is missing," Traynor said.

Browsers are not alone. Researchers from Leibniz University of Hannover, Germany, and Philipps University of Marburg, Germany, found that 8 percent of free applications improperly implemented SSL and TLS connections, leaving users open to a man-in-the-middle attack.

Mobile browser makers will have to find ways to communicate security information rather than sacrifice it for cleaner designs.



Mobile Wallets Still Need to Prove Themselves

U.S. consumers are still wary of paying for real-world transactions using their mobile phone. Despite a major push by Google for its digital wallet app and the existence of options from Isis and cellular carriers, pay-by-phone apps have only slowly taken root. Consumers are still leery of putting their financial information, even if it's replaceable credit-card account data, in a single place on their mobile device.

Moreover, there are still questions concerning security for the technology. Google and other wallet vendors use near-field communications (NFC) to transmit payment information to a terminal in the store. The protocol needs further research to head off the possibility of using it as a point of attack. At CanSecWest's Pwn2Own competition in September, for example, researchers compromised a Samsung Galaxy S3 phone using a vulnerability in NFC.[10] Last year, researchers had already discovered an attack—known as Ghost and Leech—that could siphon details from an NFC-enabled wallet.

Perhaps the biggest flaw in such payment technologies, however, is that smartphones are frequently lost and many are not secured with even a passcode. More than a third of consumers have either lost a cell phone or had one stolen, according to a report published by Symantec in 2011.

Given the uncertainties in the market, Apple may have taken a more prudent approach. In iOS 6, the consumer technology giant added Passbook, an app that focuses on collecting important documents—such as airline tickets, store cards, and movie tickets—in one place, but has skipped credit cards and automated payments.

While Europe and Asia are regularly using mobile payments, the U.S. will continue to adopt the technology slowly, said John Marshall, founder and CEO of AirWatch. "We are still in a race as to what the right platform might be," Marshall said.

[8] Boodaei, Mickey, "Mobile Users Three Times More Vulnerable to Phishing Attacks," http://www.trusteer.com/blog/mobile-users-three-times-more-vulnerable-to-phishing-attacks, Jan. 4, 2011.

[9] Amrutkar, Chaitrali, "An Empirical Evaluation of Security Indicators in Mobile Web Browsers," http://smartech.gatech.edu/jspui/bitstream/1853/43376/3/GT-CS-11-10_final_tech_report.pdf, May 2, 2012.

[10] Mills, Elinor, "iPhone 4S, Samsung Galaxy S3 hacked in contest," http://news.cnet.com/8301-1009_3-57516966-83/iphone-4s-samsung-galaxy-s3-hacked-in-contest/, Sep. 20, 2012.

Cloud Security Enters Its Teenage Years

Data in the Cloud Will Have Better Overall Security, but Failures Will Be Severe

Highlights:

- The accretion of data in the cloud will provide better-than-average information security, while at the same time offering attackers more attractive targets.
- Authorization will continue to be the weakest point for cloud data stores.
- The responsibilities and liabilities of cloud service providers will be resolved in the near future.
- Companies will need stronger guarantees of security to more widely move their data and business processes to the cloud.

The efficiencies of moving data and applications to the cloud continue to attract consumers, who store their data in DropBox and iCloud, use Gmail and Live mail to handle e-mail, and track their lives using services such as Evernote and Mint.com. While startups regularly use the cloud to avoid large capital costs, most established companies have held back from moving critical data and applications online.

Yet, cost savings and productivity gains will convince companies to move many business processes to online services. As more processes and components of businesses move to the cloud, security researchers need to work harder to understand the implications to industries and the economy as a whole.

Data in the Cloud: Safer, but More Attractive to Attackers

Consider data storage in the cloud. As security expertise is increasingly being located within cloud service providers, companies and their customers typically improve the overall security posture of their data. However, while improved virtualization infrastructure means that mass compromises are unlikely, the growing trove of data concentrated in these cloud storage services will attract attackers.

"Most of the time, we are not going to see many security issues because the large cloud services do a good job, but once they fail, the impact will be much, much higher, and that is the problem," said Engin Kirda, associate professor in computer science at Northeastern University.

Authorization, including account recovery, is a key weakness in cloud services. Allowing only authorized users to have access to the data continues to be a difficult and challenging problem.

In June, attackers compromised DDoS mitigation service CloudFlare by using flaws in AT&T's voicemail service for its mobile users and in Google's account-recovery service for its Gmail users.[11] The attack—which aimed to get control over the site of one of CloudFlare's customers—failed, but only because the company moved quickly when it discovered the incident.

"We will see more of these types of attacks, because a lot of interesting data is being hosted on [these] sites," Kirda said.

Google's latest approach to two-factor authentication is a good hybrid method, he said. Using a recognized device and a password, a user logs in and authorizes applications on other devices. By providing a different password for each application-device combination, the service provides stronger, yet usable, security.

[11] Prince, Matthew, "Post Mortem: Today's Attack; Apparent Google Apps/Gmail Vulnerability; and How to Protect Yourself," http://blog.cloudflare.com/post-mortem-todays-attack-apparent-google-app, June 1, 2012.

Attackers Exploit Compute Clouds for Quick-To-Create Botnets

Cloud infrastructure is not just about data, however. The ability to stand up virtualized computers, if successfully exploited by attackers, can be used to quickly create botnets. Just as large collections of data in the cloud become a siren call to attackers, the ability to create vast computing resources will continue to convince cybercriminals to look for ways to co-opt the infrastructure to their own ends, said Yousef Khalidi, distinguished engineer with Microsoft's Windows Azure group.

"If I'm a bad guy, and I have a zero-day exploit and the cloud provider is not up on their toes in terms of patching, the ability to exploit such a big capacity means I can do all sorts of things," Khalidi said.

The most obvious exploit that could lead to the creation of malicious compute clouds is simple credit-card fraud. Most cybercriminals have access to thousands, if not millions, of stolen credit card numbers. Using the stolen accounts to buy cloud computing resources can be a quick way for attackers to create dangerous clusters of virtual systems.

New Security Thinking for the Cloud

In addition, cloud service providers will have to be clearer about what their responsibilities are toward user data. A study by the Ponemon Institute found that 69 percent of cloud providers thought that the customer was responsible for the data kept in the cloud, while only 35 percent of cloud users agreed.[12] This disconnect will continue to cause security problems for companies that do not clarify the roles and responsibilities for protecting their cloud data.

Many companies are building private or hybrid clouds to increase confidence in the security of their data, said Kirda. "In the companies I've been talking to, people don't think the security guarantees are there, so they are building private clouds," he said.

Researchers will need to develop better ways of making data secure when it is nearly always accessible. Companies are already offering ways to encrypt data before its gets stored in a cloud service, but the problems of efficiently searching through encrypted data remain.

"Encrypted search and better performing encryption will be more important because there is a push to private clouds," Kirda said.

Of course, keeping data encrypted is difficult, especially when businesses want to search on the data or use it in algorithms running inside virtualized computing instances in the cloud. Companies concerned with security currently attempt to keep data encrypted as long as possible, decrypting it only for necessary operations. However, in many cases, that means that the keys have to be exposed to the cloud as well.

"You minimize the period in which the data is unencrypted, but ultimately a solution to work with encrypted data, or even search on encrypted data, is a long way off," said Microsoft's Khalidi.

[12] "Ponemon Releases Cloud Service Provider Study ," http://www.ponemon.org/blog/post/ponemon-releases-cloud-server-provider-study, May 2, 2011.

Malware Counteroffensive

Attackers Stymie Defenses and Add New Platforms

Highlights:

- The ability of automated systems to handle malware analysis will be compromised by the increasing use of DRM-like techniques for locking malware to infected systems.
- Attackers are honing their ability to compromise Mac OS X and mobile-device platforms.
- Domain generation algorithms will increasingly be used to harden botnets but at the cost of stealth.

The developers of malicious software continue to refine their techniques for avoiding defenses and hardening their software against easy removal. While polymorphism—the automatic generation of code variants that can fool signature recognition—has become commonplace, malware developers are experimenting with new ways to attack specific defensive activities, from preventing easy malware analysis to foiling botnet takedown efforts.

Software Licensing Techniques Will Stymie Malware Analysis

Digital rights management techniques are used to prevent widespread piracy of digital code. Software licensing can make it difficult for a pirate to mass-produce illicit programs by locking a program's execution to a specific device or locale.

Attackers are refining similar techniques to tie malware to a specific system, preventing the program from being run on another computer, such as the virtual machines widely used to analyze and create signatures for malicious software. By encrypting portions of the malware binary using specific attributes of the infected system and localizing the instruction set to certain geographies, attackers can make automated analysis much more difficult.[13]

The Flashback trojan, which started spreading in late 2011 and through the early part of 2012, used basic encryption to bind downloaded modules to the infected system. The Gauss espionage trojan, whose discovery was announced in August 2012, used a similar idea: The authors encrypted the payload of the attack using a key derived from a 10,000-iteration hash on two attributes of the infected system.

"Gauss's use of DRM is the most onerous we've seen so far," said Paul Royal, a research scientist with Georgia Tech's School of Computer Science and associate director of GTISC. "It highlights the often sophisticated and forward-looking nature of nation-state threats."

Malware Will Be Cross Platform, Making Use of Novel Smartphone Features

The Flashback trojan not only demonstrated new techniques for hardening malware against analysis, but also underscored that Mac OS X is now in the crosshairs of attackers. While government-sanctioned monitoring software has had the ability to infect Mac OS X, cybercriminals have mostly ignored the platform. With Flashback, however, cybercriminals exploited both the operating system and Mac users' false sense of security, ultimately infecting more than 600,000 systems using multiple Java runtime vulnerabilities.[14]

Apple's platform is not alone: Mobile devices, particularly those running the Android operating system, will be increasingly targeted by attackers. While Macintosh and Windows systems hold similar value to an attacker, smartphones and tablets pose different challenges and opportunities. Monetizing smartphones, especially in the United States, is not easy: Most attacks have focused on toll fraud, a scam that is mainly successful in China and Eastern Europe. However, smartphones have very interesting capabilities as sensor platforms.

While many people understand the implications of carrying a small computer in their pocket, most do not understand that they are also carrying a portable sensor suite. This year, researchers from the University of Indiana demonstrated a program—dubbed PlaceRaider—which could take opportunistic photos of a user's surroundings and build a 3-D representation of the room.[15] In 2011, Georgia Tech researchers demonstrated another capability of the platform, using a phone lying on a desk to recognize words typed on a nearby keyboard.

Attackers will find other novel ways to use the sensor capabilities of smartphones. "Our past work demonstrated the ability to capture keystrokes from nearby keyboards using only the accelerometers on a mobile phone." stated Patrick Traynor, assistant professor in the School of Computer Science at Georgia Tech's College of Computing. "While we don't expect the majority of malicious applications to use such channels, clever malware writers will continue to find ways to take advantage of the wealth of new interfaces provided by mobile devices."

Defending by Determining Intent

Attackers have already foiled many of the defenses designed to block malware and protect end users: Polymorphism has made circumventing antivirus software trivial, infecting legitimate Web servers with malicious Javascript stymies Internet blocklists based on reputation, and domain generation algorithms are designed to foil takedown efforts.

Rather than focus on defeating these countermeasures, researchers at Georgia Tech are considering ways to mitigate the damage from a successful malware infection by developing techniques to determine a user's intent. By narrowing the number of valid actions that a user can take, such a system could prevent malware from taking unwanted actions, such as logging into a victim's bank account or sending spam e-mail. By ignoring the specific malware and determining ways to mitigate the impact, such defenses will be more robust, said Wenke Lee, professor in the School of Computer Science at Georgia Tech's College of Computing and director of GTISC.

"Current security strategy is focused on the malware—such systems are fundamentally malware aware," Lee said. "We'd rather them instead be malware 'oblivious' and understand the intent of the user."

While the techniques are difficult to apply broadly, by focusing on developing rules for commonly used systems—such as e-mail clients and browsers—researchers may be able to add another layer of defense to further harden computer systems.

Domain Generation Algorithms More Reliable, but More Detectable

Domain generation algorithms (DGAs) make it difficult to take down whole botnets by sinkholing the command-and-control servers. However, the creation of a large number of nonexistent domains also makes the malware easier to detect within networks. In a paper presented at the USENIX Security Symposium in August 2012,[16] researchers from Damballa, Georgia Tech, and the University of Georgia described a system called Pleiades, which uses a combination of clustering and classification algorithms to find computers infected with DGA malware.

[13] Lemos, Robert, "Malware 'Licensing' Could Stymie Automated Analysis," http://www.darkreading.com/advanced-threats/167901091/security/encryption/240000843/malware-licensing-could-stymie-automated-analysis.html, May 22, 2012.

[14] Kaspersky Lab, "The anatomy of Flashfake. Part 1," http://www.securelist.com/en/analysis/204792227/The_anatomy_of_Flashfake_Part_1, April 19, 2012.

[15] The Physics arXiv Blog, "PlaceRaider: The Military Smartphone Malware Designed to Steal Your Life," http://www.technologyreview.com/view/429394/placeraider-the-military-smartphone-malware-designed-to-steal-your-life/, Sept. 28. 2012.

[16] Antonakakis, Manos, et al., "From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware," https://www.usenix.org/conference/usenixsecurity12/throw-away-traffic-bots-detecting-rise-dga-based-malware, Aug. 8, 2012.

Healthcare Security

Locking Down Sensitive Data in a Chaotic Environment

Highlights:

- With the move to electronic medical records, the healthcare industry will become more open to threats.
- Medical staff needs to be educated to better understand how security threats can impact their patients.
- Allowing patients to retain control of their records, while giving access in emergency situations, is a key challenge.
- Technology providers need to work with medical staff to provide solutions that do not impact efficiency.

Healthcare is a challenging industry to secure. On one hand, doctors and nurses have a low tolerance for any technology that hinders, rather than helps, their primary job. In addition, any security technology has to be ready to handle frequent exceptions—medical emergencies—when security controls need to step out of the way and allow access. With vitally important medical data being placed online, healthcare will increasingly find itself in attackers' crosshairs.

"The challenge with how well something works in this domain may be asking how well it works with exceptions rather than rules," said Mustaque Ahamad, a professor of computer science at Georgia Tech's School of Computer Science.

Patient Data Goes Online and Faces Greater Risks

Not even ten years ago, a paper record would follow a patient through the healthcare system. Now, healthcare systems use digital records, allowing hospitals and health authorities to analyze data on the health of Americans. Those records are also starting to make their way online into electronic medical record (EMR)—or electronic health record (EHR)—networks, which allow hospitals, doctors, and patients to access a single store of information.

While these records allow hospitals to better serve their patients by providing 24-hour access to doctors and electronic prescriptions, they also make the data accessible to attackers.

"Emerging threats in healthcare are not about new threats but about the way that healthcare is changing," said Praveen Chopra, chief information officer for Children's Healthcare of Atlanta. "We are more exposed now because of the expansion and changes in healthcare."

Companies are developing technology that allows consumers to control access to their information in these data stores. Similar to the encryption technology that secures corporate data in the cloud, services like Social Fortress allow people to replace plain text data stored in cloud services with encrypted data that requires access privileges. Consumers and patients can define policies around specific users, groups, or systems and grant and revoke access to the encrypted data.

"System-level access no longer means data-layer access," said Adam Ghetti, founder and CEO of Social Fortress, which started out securing data on social networks. "Even if a doctor has your data on 18 different systems and you've been going to his practice for 10 years, if a patient decides that he no longer gets access, then he won't be able to read any of that encrypted information."

Researchers at Georgia Tech are looking into ways of detecting anomalous use of patient data. With greater access to data comes a greater chance of fraud, said GTISC's Ahamad. Insurance companies, who typically bear the burden of such fraud, could use anomaly detection systems to find when a person is impersonating a patient. "Strong accountability measures and monitoring are needed, so that even in a break-the-glass sort of emergency, you still have accountability," he said. "If the information gets somewhere that it shouldn't be, you still have an idea of how it got there."

Securing Doctors' Offices

The top threat to hospitals is attackers that use it as a launching point for further attacks, according to Chopra of Children's Healthcare of Atlanta. In addition, disgruntled employees or patients can pose an insider threat to healthcare networks and facilities. Yet security in hospitals, clinics, and doctor's offices is problematic.

Part of the issue is healthcare workers' intransigence when faced with changes that improve security but require changes to the way they work. "As soon as you say, 'I'm the director of information security,' people start crossing their arms," said Chopra. "The doctors and nurses need to know that you are protecting them and not trying to get in the way."

Security firms need to make sure they are only requiring necessary changes. By choosing technology that works with the way that doctors and nurses perform their duties, security management can increase adoption. Social Fortress's Ghetti, for example, has encountered medical staff that has sent information over a phone's texting service because the approved file transfer method was too onerous.

"Encryption (for example) is way too complicated for the average user to use," Ghetti said. "They choose not to use it, so they start collaborating and communicating in other, insecure ways."

www.gtcybersecuritysummit.com

Georgia Tech Information Security Center

www.gtisc.gatech.edu

Georgia Tech Research Institute

www.gtri.gatech.edu