2017

EMERGING CYBER THREATS, TRENDS & TECHNOLOGIES REPORT

Georgia Tech Institute for Information Security & Privacy

Presented by the Institute for Information Security & Privacy

Privacy, Democracy & Security Square Off

As society becomes more connected and technology more ubiquitous, securing the systems, networks and data on which we rely becomes increasingly important – for individual safety, economic security, and national defense. Digital attacks can now affect critical infrastructure[1], turn smartphones into monitoring devices[2], and put the safety of healthcare patients at risk[3].

Since last year's report, we've seen a number of important trends — driven by the interconnectedness between the Internet and technology's impact on interpersonal relations — to force privacy, democracy and security into deeper conflict. Ransomware has steeply risen, costing U.S. businesses and consumers approximately $209 million during the first quarter of 2016[4] alone. Debates about privacy surged with the legal and very public battle between Apple and the FBI. The strike down of the Safe Harbor Act by a European High Court and its replacement with the EU-U.S. Privacy Shield framework, has focused businesses to re-examine the impact of privacy going forward.

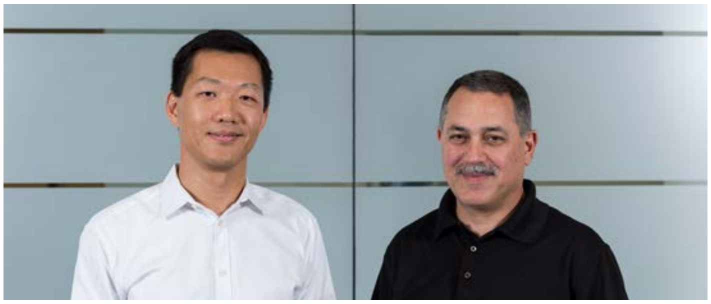
Underpinning much of the escalation in the importance of cybersecurity is the increasing number of connection points between the physical and the digital worlds. Unfortunately, companies and government agencies continue to lack steady guidelines, clear standards, or enough workers — leaving everyone vulnerable.

On September 28, the Georgia Institute of Technology held the 14th Annual Georgia Tech Cyber Security Summit. For the past 14 years, faculty from the Georgia Institute of Technology and research scientists from the Georgia Tech Research Institute (GTRI) have convened private industry, academia and government to work toward solving the greatest cybersecurity challenges. Between the dynamism of local startups and the innovative approaches of research scientists and the policy leadership of elected officials, we believe that together we can identify bold, new technologies and strategies to ensure the safety and security of government, industry and each other.

Georgia Tech is one of the nation's top-ranked engineering, computer science and research universities, and it has addressed cybersecurity with growing intensity and depth for more than 20 years. The Georgia Tech Research Institute, a long-time applied research partner of military and non-military government partners, makes us one of just 14 schools nationwide to hold accreditation from the U.S. Department of Defense as a "University Accredited Research Center" (UARC). Our academic labs also hold honors such as National Security Agency Center of Excellence in Information Assurance. These assets afford us opportunities to work with a wide range of external partners under the unified goal of making technology more secure, more profitable, and more enjoyable for all of us. Using the insights of our vast network of academic researchers, government partners and private-sector professionals, the *2017 Emerging Cyber Threats, Trends & Technologies Report* highlights the most urgent, trends and possible solutions.

We want to continue the conversation. After the summit and throughout the year, we invite anyone who wants to study or develop cybersecurity solutions to connect with us.

Thank you,



Wenke Lee
Co-Director, Institute for Information Security & Privacy
John P. Imlay, Jr. Professor of Computer Science, College of Computing

Bo Rotoloni
Co-Director, Institute for Information Security & Privacy
Director, Information & Cyber Sciences Directorate, Georgia Tech Research Institute

Privacy and technology on a collision course with no clear solution

Privacy in the United States is approaching uncertain crossroads and businesses are stuck at the intersection. While companies typically see consumer data as a competitive advantage, and so try to collect whatever may yield profit potential, consumers are becoming more hesitant to give up information — especially for free services. In fact, nearly half of all consumers now report declining an online service — for conducting finances, buying goods, posting on social networks or expressing opinions online — because of privacy concerns, according to the National Telecommunications and Information Administration[5].

In this environment, information technology companies will either choose to become champions of consumer privacy by voluntarily offering encryption and default do-not-collect policies, or will buckle as government authorities force one of two paradoxical solutions: don't collect customer data or give us unfettered access to what you have.

In February 2016, the FBI obtained a court order requiring Apple to engineer new access to iPhone data left by one of the massacre shooters in San Bernardino, Calif. Apple refused, stating that doing so would undermine consumer privacy for the short-term benefit of government access to communications by just two suspected criminals[6]. The incident underscored that privacy-enhancing technologies in devices or services help bad actors hide. Yet, encryption is an important defense against hackers, competitors and unwarranted government intrusion.

"The basic question is whether effective encryption will remain legal and in what settings," says Peter Swire, associate director of policy for the Institute for Information Security & Privacy, and the Huang Professor of Law and Ethics at Georgia Tech's Scheller College of Business. "Government agencies face new challenges because the rate of encryption has climbed sharply after the Snowden revelations."

The United States is not alone in debating the relative benefits of privacy and monitoring. A proposed law in England would require messaging providers to decrypt communications[7]; governments in Brazil and Pakistan have targeted the encryption of technology companies' products[8], and China requires that data be decrypted at the border[9].

Law enforcement will continue to drive backdoor requests

These laws are driven by government fears that, without unencrypted access, they will lose valuable intelligence tools. To make data more secure likely

Research in Focus

Privacy Leakage in Personalized, Mobile In-App Ads

While free mobile apps may seem innocuous, those who download them may be sending unintended personal details back to the developer, according to a Georgia Tech study published in February. It happens when developers include in-app advertising from ad networks, such as Google Ad Networks. Because of a lack of isolation between ad networks and the application, mobile app developers are able to learn sensitive details, such as political preference, by requesting which customized ads were shown to users of their app[14].

"Free smart phone apps are not really free," says Wei Meng, lead researcher and a Georgia Tech graduate student studying computer science. "Apps — especially malicious apps — can be used to collect potentially sensitive information about someone simply by hosting ads inside the app and observing what is received by a user. Mobile, personalized in-app ads absolutely present a new privacy threat."

The work was presented at the 2016 Network and Distributed System Security Symposium (NDSS '16) in San Diego, Calif., by researchers Wei Meng, Ren Ding, Simon Chung, and Steven Han under the direction of Professor Wenke Lee.

makes it less accessible during a criminal investigation — an end result that FBI Director James B. Comey and others call "going dark."[10]

Yet, circumventing encryption relies on trust in law enforcement. The leak of National Security Agency documents by former contractor Edward Snowden showed that online monitoring of U.S. citizens by intelligence agencies happened far more often than people realized. In its wake, online businesses and technology firms expedited efforts to encrypt communications and data. Some companies voluntarily moved to encrypt customer web traffic to their sites by default and approximately 50 percent of web traffic is now encrypted[11]. International companies asked their providers to boost encryption among and between service providers.

Whether through technology or policy, backdoors will weaken valid reasons for encryption — free expression, physical safety, financial safety — for the sake of a limited number of cases. The loss of agency access to information due to encryption is more than offset by a "golden age of surveillance" through other means, Swire says. Moreover, the ability is a capability that evolved from recent technology, not a historical right of government, says Bruce Schneier, chief technology officer for security firm Resilient Systems and a cryptographer. In the past, digital conversations could not be stored or wiretapped, so authorities could not gain after-the-fact access.

"The conversations you had would never be written down to be later read," he said. "Today, every correspondence, every note to yourself, exists in online storage that could be accessed in the future."

Privacy continues to stumble U.S. businesses in Europe

The privacy entanglement for businesses only worsens abroad as foreign governments debate how corporations should be ordered to protect or encrypt customer data. Following the Snowden revelations, European privacy advocates, business groups and governments grew more concerned that regulations under the Safe Harbor agreement did not protect European citizen data from American sensors once transferred across the Atlantic or to another country.

In October, 2015, Europe's top court agreed, declaring the Safe Harbor Act invalid[12]. A new legal agreement — the EU-U.S. Privacy Shield — has been ratified and presents privacy protections mutually deemed as "adequate." Yet, litigants continue to challenge it as incomplete[13]. Swire believes those litigants should lose in that challenge.

Cultural and legal differences in unresolved approaches to privacy continue to mire U.S. businesses with uncertainty and risk. Challenges to the legal movement of data — not only involving Privacy Shield, but also under two other legal approaches known as model contracts and binding corporate rules — will continue to pose risks to data flows between the United States and the EU, leaving the marketplace to develop (or not) standards in the absence of clear law.

"If model contracts and binding corporate rules go down, then a large section of trans-Atlantic business would be deemed illegal," Swire says. "The technique supported by some privacy advocates in Europe is to keep data inside Europe in the name of protecting individual rights."

Contributors: Policy

Peter Swire

Associate Director – Policy,
Institute for Information
Security & Privacy; and Huang Professor of
Law & Ethics, Scheller College of Business

Hans Klein

Associate Professor,
School of Public Policy
Ivan Allen College of Liberal Arts

Milton Mueller

Professor,
School of Public Policy
Ivan Allen College of Liberal Arts

Year in Review: Policy Milestones

October 6, 2015
European Court of Justice invalidates E.U.-U.S. Safe Harbor agreement in the case of *Schrems v. Data Protection Commissioner*.
Precipitating event: Max Schrems, an Austrian Facebook user, lodged a complaint with the Irish supervisory authority, arguing that the United States does not offer sufficient protection against surveillance of data transferred overseas.

February 1, 2016
Negotiations begin for U.K.-U.S. Agreement on Data Sharing for Law Enforcement Purposes.
Precipitating event: U.K. nationals use social media services by American companies to engage in criminal or terrorist acts, but U.S. law bars American firms from providing intercepts to anyone but the U.S. government with a court order. American companies are caught in an international tangle of conflicting law enforcement requests.

February 9, 2016
President Obama establishes the Federal Privacy Council and the Commission on Enhancing National Cybersecurity, with Professor Antón as one of the twelve commissioners.
Precipitating event: Paris terrorist attack (November 13, 2015) and San Bernardino shootings (December 2, 2015).

February 24, 2016
The U.S. Judicial Redress Act is signed into law by President Barack Obama, ensuring that citizens of EU member states have the same privacy protections and remedies as are available to U.S. citizens under the Privacy Act.
Precipitating event: The Judicial Redress Act of 2015 authorizes the Department of Justice (DOJ) to designate foreign countries or regional economic integration organizations whose natural citizens may bring civil actions under the Privacy Act of 1974 against certain U.S. government agencies.

March 10, 2016
Federal Communications Commission releases proposed rules on Broadband Consumer Privacy to ensure consumers have protection over how their data is used and shared by broadband providers.
Precipitating event: When broadband providers were placed under the FCC's net neutrality rules, they also became subject to new FCC privacy regulation. Increasing data breaches of large amounts of consumer data.

April 13, 2016
Senators Richard Burr (R-N.C.) and Dianne Feinstein (D-Calif.) introduce a discussion draft of *Compliance with Court Orders Act of 2016* to redefine encryption and its role within the rule of law. The bill is dubbed as being part of the "New Crypto Wars."
Precipitating event: *Apple v. FBI* (2015-16).

June 2, 2016
European Union and the United States sign "umbrella agreement" to protect personal data transferred across the Atlantic in a bid to fight crime and terrorism.
Precipitating event: Edward Snowden leaked evidence in 2013 of a massive network of U.S. and allied spy operations on friends and foes, including EU countries.

July 12, 2016
European Commission formally adopts EU-U.S. Privacy Shield law to replace the Safe Harbor privacy framework.
Precipitating event: *Max Schrems vs. Irish Data Protection Commissioner* decision by the European Court of Justice (October 6, 2015).

July 14, 2016
The Second Circuit Court of Appeals of the United States rules in *Microsoft v. United States* that the *Stored Communications Act* did not require a company that received a search warrant to seize the contents of an email account to provide electronic evidence that was stored outside of the United States.

July 14, 2016
An overturned court ruling renewed interest in *Law Enforcement Access to Data Stored Abroad (LEADS) Act* and whether the *Electronic Communications Privacy Act of 1986* allows U.S. law enforcement to search and seize private emails in a foreign country.
Precipitating event: *Microsoft v. United States* (evidence in Ireland) appeals court ruling of July 14, 2016.

Insecure e-voting systems emerge, but crowdsourcing and open source may hold promise

The security threats to electronic voting rose quickly when states adopted direct-recording electronic (DRE) voting machines in the 1990s and early 2000s. Poor design choices in early electronic voting systems — along with the lack of a verifiable paper ballot for some DRE systems — caused computer scientists and some election officials to question results from the machines.

Now those machines are aging, and whatever security vulnerabilities were present before only intensify. While newer electronic voting systems may have more secure features and a verifiable voting record, maintaining the security of older machines will be critical in the U.S. – especially as voter turn-out rises during a presidential election year. The majority of states need to replace their voting machines within the next five years, but election officials in 71 percent of states do not know where they will get the money[15]. Unlike older machines, such as lever-recorded machines, electronic systems need to be replaced every decade or so, and the National Conference of State Legislatures estimates that to cost $2,500 to 3,000 per machine.

"A lot of the equipment that was bought in 2000, 2001, 2002, is over a decade old, and electronic voting machines have a much shorter lifecycle than previous voting machines," says Pamela Smith, president of Verified Voting, a watchdog group of scientists and government experts focused on election technology.

Hacks of political IT systems put election safety in crosshairs

Voting security is critical because a variety of attackers already have targeted election information. One political hacker, allegedly linked to Russia[16], compromised the Democratic National Convention, publicly leaking donor lists and the Democrats' opposition research[17], perhaps as an attempt to sway American sentiment. In another incident, a political advisor and self-styled cybersecurity researcher was charged with criminal hacking after he found flaws in Florida's election website, giving him to access county voter names, passwords, and records[18].

Shady political operations have moved online to influence elections in other countries. One political operative, for example, claiming to have influenced many of the elections in Latin America, hacked smart phones, created fake Web sites and sent political propaganda in support of the highest bidder for his services[19].

Voting in Georgia

Voting methods vary across the United States. Georgia uses direct-recording electronic (DRE) machines without a verifiable voting paper-evidence trail (DREs without V.V. PATs). This category is not well-favored by computer scientists because it never produces a physical record of the vote or a way to verify what the voter intended to cast.

To fight issues like these, Georgia Tech professors Ellen Zegura and Michael Best developed a crowd-sourced election reporting tool known as "Aggie." The tool scrapes social media and other public sources for patterns of discussion that may indicate an election problem — focusing on issues such as long lines, voters being turned away, and the security of the voting machines. The software has been used in Nigeria (2011, 2014, and 2015), Liberia (2011), Ghana (2012), Argentina (2015), and informally in Mexico in 2016. It continues to be developed by Best at the United Nations University Computing and Society Lab.

“Election accuracy is a huge issue. The idea behind crowdsourcing is to give you more eyes on what’s actually happening at the polls,” Zegura says. “Aggie is meant to compliment formal election monitoring, which is very important in developing democracies.”

Open-source development offers promise

Because free and fair elections are at the core of democratic self-government, election officials have – perhaps appropriately – turned to the public domain to create open-source voting systems. Two large counties in California and Texas are developing their own technology for electronic voting because of the problems with current voting machines.

The largest election district in the United States, Los Angeles County, is using fast prototyping practices known as agile development, where designs are improved over time, to architect, code, and build a new generation of e-voting machines[20]. The software and design will be published as open source so other counties can use the same technology.

“In the event that this is successful, that could be really good for other jurisdictions,” says Verified Voting’s Smith. “Not everyone has the resources available for R&D, so this allows others to benefit from Los Angeles County’s development.”

To get away from the insecure DRE systems, election officials in Travis County, Texas also have created their own system based on open-sourced components[21]. The project is forecast to cost $8.5 million but will replace $4,000-voting machines, along with the licensing and maintenance costs of $250,000, with a year with a tablet-based system that provides printed voter receipts and cost only $1,000 each[22].

Research in Focus

Aggie and ‘Eye on the Vote’

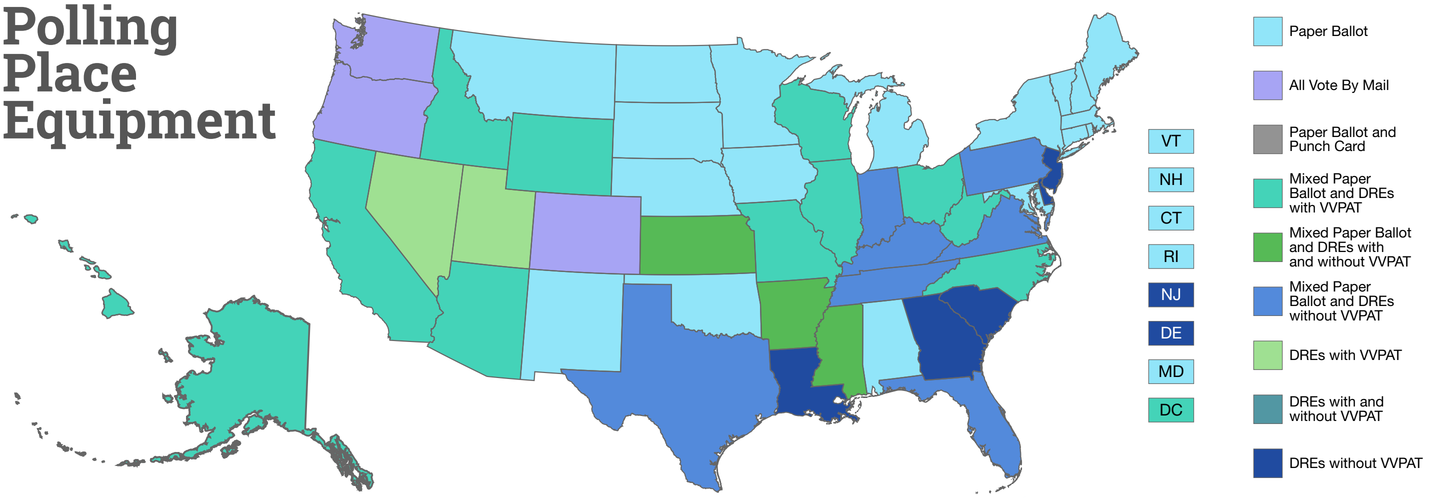
Election integrity matters for confidence in new leadership and future democratic participation. College of Computing Professors Ellen Zegura and Michael Best (with Ph.D. student Tom Smyth) developed a software system called “Aggie” to help combat intimidation at the polls and keep elections honest.

How long were lines? Were people turned away? Were voting machines in a secure place? Are false reports of problems at the polls being circulated to intimidate the public? Leads are anonymized day-of, in real-time and tagged as an “event;” then Aggie watches for more examples of similar reports to build a case before forwarding it to local law enforcement or an election commission.

In Argentina in 2015, it was paired with an app by Pol-IT called “Ojo con el Voto” (Eye on the Vote). The system allowed citizens to provide feedback about their voting experience via five, brief questions. According to study organizers, 43 percent of the app users said they had some type of problem at the polls – the most common complaint being a lack of ballots.

What are the lessons for the U.S.? Zegura personally believes there are enough checks and balances here to prevent what she has seen in other countries. However, there is interest in using Aggie in U.S. elections, and Georgia Tech “is starting conversations with pro-democracy groups here,” she says.

Polling Place Equipment


VT
NH
CT
RI
NJ
DE
MD
DC
Paper Ballot
All Vote By Mail
Paper Ballot and Punch Card
Mixed Paper Ballot and DREs with VVPAT
Mixed Paper Ballot and DREs with and without VVPAT
Mixed Paper Ballot and DREs without VVPAT
DREs with VVPAT
DREs with and without VVPAT
DREs without VVPAT

Ransomware on the Rise: It's Just Malware, People

The FBI estimates that criminals using software to encrypt data and then demand a ransom — *ransomware* — cost companies $209 million in the first five months of 2016 alone, or eight times more than all of 2015[23]. Based on those numbers, to say ransomware took off in 2016 would be an understatement. What changed, exactly? Did media outlets start reporting more, or did the technology become more accessible to less-sophisticated criminals?

Ransomware operators use a variety of means to infect users — initially focusing on phishing attacks and drive-by downloads, but increasingly use bespoke hacks to target potentially well-paying targets, such as hospitals where locked data literally can mean the loss of life. Once they get in, malware encrypts important files using a key only known to the operator. Unless the user has made frequent backups, their only choice may be to lose data or pay the ransom.

It's no longer just about extorting money, either. Ransomware has evolved from locking up just one machine to steal data, wiping it from company machines, to sometimes destroying servers and networks in the process. Wiper malware, which has the destructive potential of ransomware but not the financial motive, has been used in numerous incidents, including attacks on oil-and-gas giant Saudi Aramco, Sony Pictures, and South Korea's media companies[24]. With such devastating effects, and high profile victims, it's easy to see how ransomware gets more and more attention. In spite of this, businesses need not panic.

New tools, with very basic code, have proliferated like never before, making it easier to obtain and use. Ranscam is an example of how sloppy but effective low-rent hacking can be. Once the computer is infected with simple malicious code, files are deleted, but it demands a payment after the fact, with no hope for the victim of actual data recovery. Even though it's cheap and easy to obtain on the dark web, there's little incentive for hackers to suddenly shift to widespread use of ransomware: If victims catch on that paying a ransom for their files is futile (knowing data is already destroyed), they won't bother paying. This type of short-lived window of exploitation shapes the trends of tactics used in cybercrime.

It's just malware

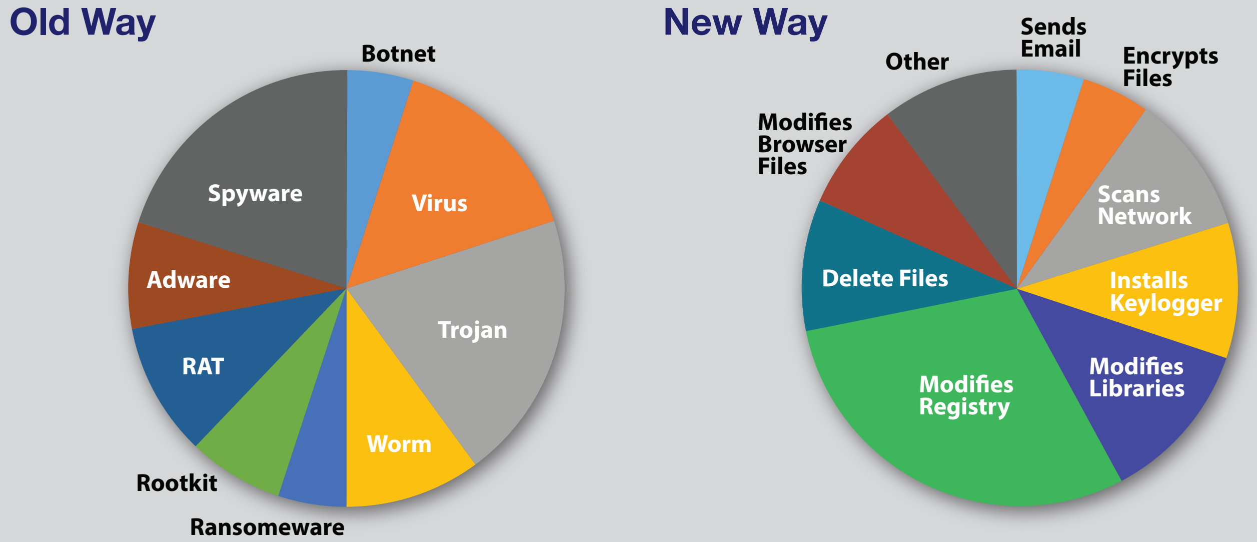
The problem with ransomware is that it can get by a lot of off-the-shelf defenses. Yet, ransomware is not very different from other malware, explains Evan Downing, a Ph.D. student in the School of Computer Science at Georgia Tech who is studying the evolution of more than 90 million malware samples. "Ransomware functions are extremely simple; it tells you what it has done. The majority of malware is doing far scarier things – it's more dangerous and craftier than ransomware — because it is silent."

Like any malware, ransomware has behaviors, trace signatures, develops over time, but it can be monitored and prevented…with proper vigilance and planning. "Technical malware analysis is not necessarily a solution because of the asymmetry between the attacker and defender — the attacker has to do very little to create a lot more work for the defenders," says Chris Smoak, a research scientist with the Georgia Tech Research Institute's Cyber Technologies & Information Security Lab (CTISL).

The Evolution of Malware ❯❯❯

Georgia Tech Ph.D. Student Evan Downing is attempting to define malware once and for all, not by type but by the damage it does and how it has changed over time. Historically, malware has been classified into various categories with relatively strict definitions: viruses, trojans, rootkits, spyware, botnets, worms, ransomware, etc. Downing's project will re-categorize them by specific behaviors because most forms of malware today are some mix of all of the categories, he says. "In the '90s and early 2000s, it was pretty easy to segregate malware into these strict categories but over time they've all adopted various combinations of each others' behaviors."

Downing has access to roughly 90 million samples spanning 10 years that will be continuously running on a carefully controlled and monitored network at the Institute for Information Security & Privacy. After categorizing all samples, he will attempt to locate the first known case of that sample, and then plot how it behaved or adapted as the threat was publicized and patches were introduced. The result will be an evolutionary timeline of the malware around us. Coupled with the 250,000 samples of malware that are collected daily by Georgia Tech Research Institute's Cyber Technologies & Information Security Laboratory, Downing has a dirty world as his oyster.



For demonstration purposes only. Not actual results.

"Treat this as a data loss problem, which means that you need to figure out what you really, really care about and protect that."

The typical advice for companies is to constantly have current backup servers, stored offline, ready to test restoration capability, which is paramount. Policies about external devices connecting to proprietary networks should be formalized, and port security implemented. Companies should consider having net flow logs that go back a minimum of 30 days; this may not prevent a ransomware attack, but it will assist in any law enforcement investigation. To address the ever-changing nature of malware, companies need to have visibility into anomalies on their networks and should implement a multi-layered defense.

Don't be a victim

More than half of all Internet users believe they would pay a ransom, according to a survey conducted by security firm BitDefender. Half of all victims in the U.S. and 44 percent of victims in the U.K. actually did pay the ransom after being infected. When asked if they thought they would pay in a hypothetical future attack, 40 percent of all Americans and 31 percent of British users said they would[25].

Victims may be naive about what happens when they pay; many assume that, if they have the money, they will get their data back. Yet, the compact between attacker and victims is shifting. In May 2016, Kansas Heart Hospital paid a ransom to an offshore ransomware group, only to have the group partially decrypt their files, demanding a second ransom to decrypt the remaining files. The hospital had to restore their data manually, after determining a second payment would be unwise[26]. Kansas Heart had a plan in place to deal with ransomware, making recovery possible, albeit painful.

Downing says he supports an idea first proposed in 2010 by Microsoft's Scott Charney, corporate vice president of trustworthy computing: create a standalone government agency akin to a “Cyber CDC.” The idea has yet to come to fruition.

“We need a central location where only the best, most competent people are employed, and it needs to be an educational outlet that widely shares information about how threats spread, just like we monitor the flu,” Downing says. “It can’t be part of any other agency.”

The ransomware threat is real, but with training, planning, and partnering for effective intelligence sharing, ransomware will hopefully wind down to become an outdated cybersecurity problem.

Contributors: Information Assurance

Taesoo Kim

Assistant Professor,
School of Computer Science
College of Computing

Manos Antonakakis

Assistant Professor,
School of Electrical & Computer Engineering
College of Engineering

Milos Prvulovic

Professor,
School of Computer Science
College of Computing

Chris Smoak

Division Chief,
Cyber Technologies & Information Security Laboratory
GTRI

Wenke Lee

Co-director,
Institute for Information Security and Privacy

Research in Focus

Mitigating ‘Social Engineering’ Attacks

To study the impact of web-based social engineering attacks, a team of four academic researchers collected signs of successful attacks against university students from live network traffic. In total, 2,004 attacks that successfully lured users into downloading malicious and unwanted software were collected and reconstructed from the data.

The researchers Terry Nelms, Roberto Perdisci, Manos Antonakakis, and Mustaque Ahamad categorized the tactics used by attackers to deceive or persuade; reconstructed the web path followed, and measured characteristics of how they were delivered.

More than 80 percent of attacks were delivered through advertising, another 7 percent through a combination of manipulated search results, and 6 percent used posts on websites to get the victim’s attention[27]. Fake updates for Adobe Flash and Oracle’s Java were among the most popular types of attacks, while fake antivirus has become much less effective and only represents 1 percent of all successful attacks.

By purchasing legitimate online ads on trusted sites, attackers easily “published” their malware while hiding the attack infrastructure from users and security researchers. Less than 75 percent of all attacks were successfully caught by commercial antivirus products and labeled as either malware, adware or potentially unwanted programs (PUPs).

The study, titled. “Towards Measuring and Mitigating Social Engineering Software Download Attacks,” was presented at the 25th USENIX Security Symposium and led to the identification of a pattern set for a statistical classifier that can recognize 91 percent of all attacks with just a 0.5 percent rate of false alerts.

Global information manipulation by nation-states now widespread

Censorship and information attacks have become more impactful and pernicious as digital devices have evolved. Governments and companies have greater control over people's perceptions of the world — not just through intentionally false propaganda or malicious information modification, but through subtle societal pressures as well.

While it's easy to point out internet restrictions in China, Russia, Cuba and the Middle East, many Western countries have added increasingly subtle limits and filters, as well, argues Milton Mueller, professor in the School of Public Policy at Georgia Tech. A code of conduct for Internet providers developed at the European Union Internet Forum in June pressures Internet intermediaries to censor accounts that could be contributing to recruitment of extremist organizations and the radicalization of citizens[28].

The code of conduct represents a significant change in policy for Western nations — a recognition that pervasive information content can be a cybersecurity issue, an opinion long argued by Russia, China and other nations, he says.

"So in effect, the West is kind of backing into the same view that we have roundly criticized during peacetime in other venues, but now we are starting to treat information in that way," says Mueller. "There is a debate to be had."

Doing so wouldn't be the first time Western nations have curtailed communication during wartime. Letters home were heavily censored during World War II if they contained too much detail about troop movements. Letters were destroyed and never delivered if they contained foreign or sexually suggestive language[29].

Nation-states are experimenting with information modification

The control of data flows – and the content of that information – continues to be a major area of research and development for most nations, whether using blunt tools such as censorship or more refined and subtle modifications, such as filtering search results or social media campaigns.

Social media and search-based information flows have made information manipulation and disinformation much easier. In March 2016, in the middle of a heated race for the Democratic nomination for president, *The New York Times* seemingly reported a bombshell: Senator Elizabeth Warren of Massachusetts endorsed Bernie Sanders. Although the news story matched the style of the *Times* and was distributed widely on Twitter, it was fake[30].

> *"...the West is kind of backing into the same view that we have roundly criticized during peacetime..."*
>
> **— Milton Mueller**
> School of Public Policy

Nation-states have used this type of attack in the past. As reported in the 2015 edition of this report, Louisiana residents started receiving text messages that an explosion had occurred at a local chemical plant that was leaking dangerous fumes. The tag for a collection of tweets seemingly supported the warnings, with eyewitness accounts and even video[31]. Yet, the entire incident appeared to be a disinformation campaign, reportedly run by Russian group known as the Internet Research Agency.

In May, former workers at Facebook claimed that the company had regularly censored conservative viewpoints out of the service's Trending section[32]. The company also regularly changes its news feed algorithm and display in ways that impact what type of news users regularly see[33].

Subtle forces are censoring information on the Internet

Controlling data flows across international borders has become an everyday activity for many countries, including China, Russia, and some Middle Eastern nations. In Cuba, for example, censorship is accomplished by offering only low-bandwidth connectivity and high-cost access. Citizens pay $4.50 (USD) an hour and the average Cuban earns the U.S. equivalent of $20 per month[34], says Michaelanne Dye, a Georgia Tech Ph.D. candidate in the Human-Centered Computing program, who is studying state-run attempts to stifle information in Cuba.

"At the same time it has liberating effects, the Internet can serve to reinforce structures that already exist and subjugate certain groups of people," Dye says.

The Russian news outlet, RT.com, poses a similar quandary, says Hans Klein, associate professor in the school of public policy at Georgia Tech.

"The Russians created RT.com, which is their Voice of America," he says. "Is this a cyber threat, is this information warfare, or is it just another more diverse form of media? Many see it as just another digital printing press, but we see a country with serious resources, Russia, using the Internet to publish their viewpoint."

Terrorism has meant closed societies are no longer the only ones to censor. Anti-terrorism policy acts as a subtle gag of information, allowing law enforcement to convince service providers to pull down potentially valid speech. Lawsuit-adverse services will be sensitive to cease-and-desist orders.

Research in Focus

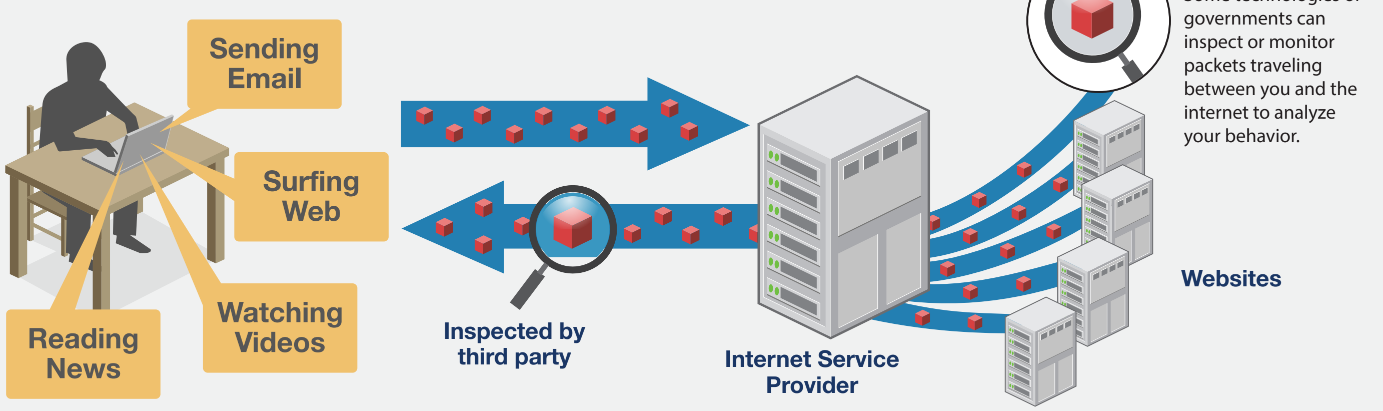
Detecting Promotional Attacks Using SEISE

Web sites with well-known brand names are often used by aggressive marketers, the Internet underground, and outright criminals to promote their own products or fool users into following a link to a malicious download. They also offer a way for nation states to inject "information pollution" into an enemy's citizen psyche.

"The basic idea behind 'promotional infection' is to attack websites that are highly-ranked and to leverage their importance to promote various things, most of them illegal," says Raheem Beyah, a professor in the school of electrical and computer engineering at Georgia Tech. "The bad content is nested into the prominent site to leverage the traffic of that domain. That gives the attackers a doorway to whatever they are promoting."

Georgia Tech and the Tsinghua University in China worked together to create a new technique, Semantic Inconsistency Search (SEISE), to find content that departs from the expected norm on a website[35]. The work was supported by the U.S. National Science Foundation and Natural Science Foundation of China, and presented in May 2016 at the IEEE Symposium on Security and Privacy in San Jose, Calif.

Nation states can profile your online behavior



Some technologies or governments can inspect or monitor packets traveling between you and the internet to analyze your behavior.

Healthcare fraud takes off in the absence of good defenses

In June, officials at the U.S. Department of Justice (DOJ) announced prosecutors had charged 301 people with fraudulently filing $900 million in Medicare claims, easily exceeding the $712 million lost to Medicare fraud in 2015. The bogus patients involved in the fraud were often poor drug addicts, who agreed to have services charged under their name in exchange for narcotics, according to the U.S. DOJ[36].

As hospitals and insurers move to electronic medical records, fraud has become the next plague for healthcare. Insurers are a major target of criminals, who often sell stolen patient records to fraudsters who use them to illegally bill insurance companies. Patients, however, are targeted as well. While electronic health records (EHRs) are making it easier for various doctors to broadly access one's medical history, EHR systems also make it easier for data thieves to steal personally identifiable information — data that is more difficult to correct than a stolen credit card number.

"There is an overwhelming argument in favor of the digitization of medical records, both in terms of patient safety, cost of care and quality of care," says Mark Braunstein, professor of the practice at Georgia Tech's College of Computing. "But we really need to protect the data, at rest and in transit. We are not there yet."

Healthcare data is 'the whale' for hackers

Electronic medical records hold out the promise of better and cheaper healthcare, an important goal considering that the U.S. healthcare system is the world's most expensive — by a large margin — but fails to make the top 10 in terms of successful outcomes[37]. Currently, nearly 20 percent of the U.S. economy, as measured in gross domestic product, is tied to healthcare[38].

No wonder, then, that health services was the most commonly sector breached in 2015[39]. In the first three months of 2016, more than 30 organizations already saw data leaked or lost to hackers[40]. Here's why: healthcare data sells for more money than most on the black market — as much as 10 times the price of stolen credit-card data[41].

"Just seeing a person's healthcare data opens up an avenue for many other types of fraud," says Musheer Ahmed, a computer-science Ph.D. graduate of the College of Computing at Georgia Tech. "In addition, if you do find someone using your healthcare identity, your medical history could become corrupted, which could pose health risks if misapplied or misinterpreted, and literally could kill you."

Contributors: Health IT

Jon Duke, M.D.

Director,
Center for Health Analytics & Informatics
Georgia Tech Research Institute

Musheer Ahmed

Co-Founder,
FraudScope

Gregory Abowd

Associate director –
Consumer-facing Privacy,
Institute for Information Security & Privacy;
Regents' Professor, School of Interactive Computing

Mark Braunstein

Professor of practice,
School of Interactive Computing

Complexity of the system invites fraud

Yet, securing electronic patient records is complex: Providers need fast, convenient access to the information in moments of emergency, but the data needs to be protected against illicit use. The U.S. healthcare IT marketplace adds more complexities as well, with three predominant health care platforms — none of which can talk to each other — and 50 to 60 other smaller offerings in the market, says Jeff Evans, director of the Georgia Tech Research Institute's Information Communications Lab (ICL).

In addition, the healthcare ecosystem results in medical information being distributed among dozens of providers, insurance companies and other firms, and the patient has little control, says Dr. Deborah Peel, president of Patient Privacy Rights.

"The thing that people don't understand is that we need technologies that serve us, and right now we are in a situation of maximal harm," she says.

This complexity is one reason why fraud has been so successful. Before healthcare officials catch on, fraudsters quickly shut down operations and move on, says computer science Ph.D. graduate Musheer Ahmed.

"By the time the government or anyone else realizes what is going on, they have stolen $10 million to $20 million between when they start up and when they shut down," he says.

Worse, the fraudulent use of identities can have a dramatically adverse impact. Patients whose identities have been unwittingly misused may have erroneous information in their medical records, possibly putting their future health at risk, depending upon what an emergency provider accesses and determines about that individual. With medical mistakes already the third leading cause of death for Americans[42], assuring the integrity of medical data in patient records is paramount.

U.S. Healthcare Fraud Takes Off

Year Announced*	Medicare Fraud ($ millions)	Persons Charged
2010	251	94
2011	225	111
2012	430	91
2013	223	89
2014	260	90
2015	712	243
2016	900	301

Source: U.S. Department of Justice data

*The year announced is not necessarily the year for which the fraud is tabulated. The U.S. DoJ announces the results of its Medicare Fraud Strike Force operations, which may not include prosecutions in a single calendar year.

Research in Focus

FraudScope

Recent Georgia Tech graduate Musheer Ahmed (Ph.D. CS '16) and his advisor, Prof. Mustaque Ahamad, identified a computer algorithm that can accurately predict who is most likely to commit healthcare fraud. Ahmed examined two-years-worth of Medicare claims data and found that the algorithm identified the same providers who were caught and indicted for healthcare fraud — validating the technique as a risk predictor without the need for whistleblowers.

"What I figured out was, to successfully find abuse, you need to look at the noise, not the signal," Ahmed says. "But if you find a pattern within the noise itself, that means that someone is trying to game the system."

The pair are continuing translational research as "FraudScope" to develop a solution that will address the growing healthcare fraud problem and ensure that more healthcare dollars go to actual patient care. In addition to keen interest from businesses and entrepreneurs across Atlanta, FraudScope has received $400,000 in funding from the prestigious Wallace H. Coulter Foundation and Georgia Research Alliance, won the Institute for Information Security & Privacy's inaugural "Demo Day Finale," and was one of four finalists among 80 competitors in the Technology Association of Georgia's Biz Launch competition.

When trust is lost, 'smarts' are too: Why smart devices and cities need cybersecurity

The future will be automated. Anywhere from 25 billion[43] to 50 billion[44] devices will go online by 2020 — from driverless cars and industrial control systems to health monitoring devices and more home automation.

Yet, danger looms when engineers of smart devices — and the societies who use them — ignore cybersecurity. Because connected devices will act as a proxy for human operators or users, trust needs to be built into initial system design. The rapid growth and scale of the problem means that humans will have to trust devices to operate securely and already be programmed to take the right course of action.

"There needs to be a recognition that when you have the scale that we see with the Internet of Things — with billions of devices — it is not going to be possible for humans to manage all that, so we have to delegate some decision-making to machines under some circumstances and conditions," says Margaret Loper, principal research scientist at Georgia Tech Research Institute (GTRI) and associate director of trust for the Institute for Information Security & Privacy.

Because machines will be required to make decisions based on data from other machines, the systems must have some basis for establishing trust with each other and detecting when an attacker may be infiltrating the system[45].

Users must be able to trust both machines and their operators

Making cities smarter and more easily managed is a popular area of research for the Internet of Things. Devices and technologies used to manage smart cities will become much more commonplace, with the global smart city technology market estimated to be worth $27.5 billion annually by 2023[46].

Yet, with increasing devices comes dangers. A 2014 report by the National Security Telecommunications Advisory Committee (NSTAC) found that the pervasive interconnectivity of devices could pose implications for national security[47]. Devices — especially cyber-physical systems such as autonomous vehicles and medical appliances — will have to have significant built-in intelligence. While it's currently not a major criteria in the development and deployment of these technologies, everyone who develops and funds these projects and products should consider the impact of interconnectivity and security, say Georgia Tech researchers.

Contributors: Trust

Margaret Loper

Associate director –
Trust, Institute for Information Security & Privacy

Alenka Zajic

Assoc. Professor,
School of Electrical & Computer Engineering

Alain Louchez

Managing director,
Center for the Development and Application of Internet-of-Things Technologies (CDAIT)

John Wandelt

Division Chief,
Information Exchange and Architecture Division (IEAD)
Georgia Tech Research Institute

"In the past, things were isolated, and you had the security advantages of a natural firewall," says Alain Louchez, Managing Director of the Center for the Development and Application of Internet-of-Things Technologies (CDAIT) at Georgia Tech. "But as we become more interconnected and the Internet becomes more pervasive, you increase the risk for hacking or ill will or malevolent attack. You expose yourself to the possibility of a cascade of catastrophic failure."

The United States is still playing catch-up with smart-city and Internet of Things initiatives supported by other nations. At the time of publication, the U.S. Senate is seeking to pass the Developing Innovation and Growing the Internet of Things (DIGIT) Act, a law aimed at supporting the nation's development of Internet of Things[48]. In addition, bi-partisan members of the U.S. House of Representatives have formed a committee that aims to find ways to boost research into, and adoption of, the Internet of Things[49].

To help secure interconnected devices, Georgia Tech is taking part in the White House's Smart Cities Initiative, a collaboration by 20 universities and their local cities to research, develop, and deploy solutions for improving the management and services of civil infrastructure. Each city-university team will tackle three projects each year and share the results with other universities in the initiative.

Security must be added to communications to prevent hacking

Devices must also be able to manage themselves and verify the state of others nearby. Any system must also be able to manage itself and verify the state of any sensors and device to which it is connected. Tackling trust between autonomous cars sharing the road, within a naval fleet, or swarms of unmanned aircraft requires multiple layers of security. Machines need to prove they are trustworthy at the hardware level, at the network layer, and the application layer.

"Before, machines were invited to work by themselves. Now machines communicate with each other," says Ling Liu, computer science professor in the College of Computing at Georgia Tech. "As soon as you communicate, there is a risk of manipulation."

Research in Focus

CAMELIA: Monitoring Side-Channel Signals for IoT Trust

A $9.4 million grant from the Defense Advanced Research Projects Agency (DARPA) could lead to development of a new technique for wirelessly monitoring Internet of Things (IoT) devices for malicious software – without affecting the operation of the ubiquitous but low-power equipment.

The technique will rely on receiving and analyzing side-channel signals, electromagnetic emissions that are produced unintentionally by the electronic devices as they execute programs. These signals are produced by semiconductors, capacitors, power supplies and other components, and can currently be measured up to a half-meter away from operating IoT devices.

By comparing these unintended side-channel emissions to a database of what the devices should be doing when they are operating normally, researchers can tell if malicious software has been installed.

"We will be looking at how the program is changing its behavior," explained Alenka Zajic, the project's principal investigator and an assistant professor in the School of Electrical and Computer Engineering at the Georgia Institute of Technology. "If an Internet of Things device is attacked, the insertion of malware will affect the program that is running, and we can detect that remotely."

If society is moving toward driverless cars and hybrid ground-and-air vehicles, those machines need to know how to talk to each other, Ling says. Encryption does not work in these scenarios; instead the solution demands multiple sensors or multiple kinds of sensors to ensure the reliability of readings that direct devices to act on our behalf and guide us, she says. Right now, most engineers are still trying to prove the feasibility of autonomous vehicles or hybrid air-ground vehicles, she says, and aren't yet willing to budget for or think ahead to cybersecurity. "They're still trying to prove feasibility of the idea first."

Dual-use technologies — exploits and encryption — come under scrutiny

The communication of exploit code — a key way that security researchers prove a vulnerability can be used to attack software — could be under attack. Proposed changes to the *Wassenaar Arrangement*, an international arms control deal that seeks to limit the sale of surveillance and hacking software to other regimes, originally made even the sharing of information among employees at the same company illegal when such information crossed national boundaries[50].

Cybersecurity companies are rightfully worried over the *Wassenaar Arrangement* negotiations, ongoing as of publication of this report. In 2013, the U.S. Departments of State and Commerce agreed with 39 other nations who are signatories of *Wassenaar* to try to limit the access of repressive regimes to cyberweapons. Initial language, however, would have made the communication of exploit code illegal for security researchers as well as the targeted governments and groups.

After back-pedaling on original language, talks between treaty signatories in June focused on how to limit the access of repressive regimes to such technology, while allowing security researchers and cybersecurity companies to experiment and test code, systems or networks for vulnerabilities.

"The challenge for the delegation from the U.S. State Department won't be just convincing the 39 other signatories to the *Wassenaar Arrangement*, a voluntary export-control regime mostly focused on conventional arms, that they should reconsider how the deal applies to digital weapons," wrote Christopher Porter, manager of the strategic forecasting arm of FireEye iSIGHT Intelligence, in a June column[51]. "They will also try to convince the American tech sector that there's a way to impose restrictions on this kind of trade without blunting legitimate cybersecurity sales and research."

The debate highlights the problems in dealing with information about vulnerabilities and threats. Moreover, the points made by each side mirror the rhetoric in the battle over security backdoors and encryption, both of which are dual-use technologies *(see "Privacy and technology on a collision course with no clear solution" pg. 1-3).*

Different ways of disclosing have different impacts

Now and into 2017, information sharing will continue to be a major issue for both companies and governments. Security researchers who find vulnerabilities typically disclose the issues in one of two ways: Waiting for the company to fix the software flaw before releasing any information or releasing the information to force the company to quickly patch the issue.

Each approach has benefits and drawbacks. Fully disclosing the vulnerability, along with exploit code, generally results in an increase in attacks — up to six orders of magnitude more[52] — but also speeds the user community's response to the vulnerability. Privately disclosing the vulnerability results in slower

Contributors: Privacy, Risk & Governance

Annie Antón

Chair,
School of Interactive Computing
College of Computing

Jimmy Lummis

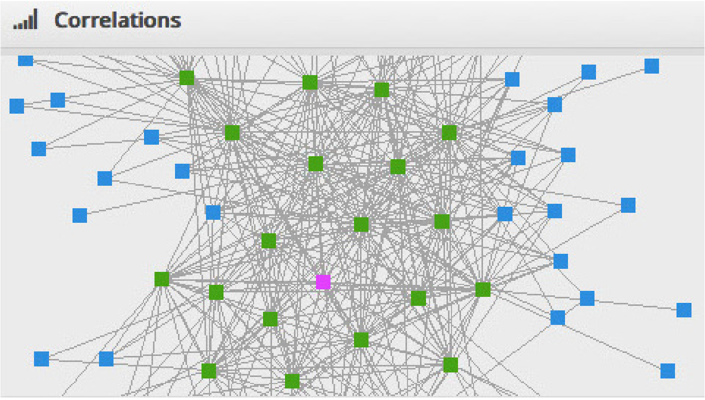
Associate Director,
Cyber Security
Georgia Institute of Technology

Saby Mitra

Associate director – Risk,
Institute for Information Security & Privacy

exploitation by online attackers, but also in slower patching and a longer lifetime for useful exploits, says Sabyasachi Mitra, a professor of information technology management at Georgia Tech's Scheller College of Business and associate director of risk for the Institute for Information Security & Privacy.

"With full disclosure, more clients saw vulnerabilities exploited," he says. "The lifecycle of the vulnerability is much shorter. With limited disclosure, the attacks start much later, but it extends for a longer period of time."



Both government and business see information sharing as a gamble

Despite an executive order and legislation, information sharing — especially between the government and private sectors — is weak. Numerous hurdles bar the way for most businesses to participate. While a large number of threat-intelligence services exist, the provided information frequently contains large number of false positives, making security professionals' jobs harder, says Jimmy Lummis, associate director at Georgia Tech Cyber Security.

"We are seeing more threat intelligence services, but the challenge is the fidelity of the information," he says. "That causes extra work and reduces my risk appetite for taking automated action on their recommendations."

The *Cybersecurity Information Sharing Act of 2015* offers hope that companies can benefit from their individual experiences in dealing with threats. Yet, progress is slow. While the Department of Homeland Security launched its Automated Indicator Sharing (AIS) platform in March 2016 with more than 100 participants, the effort unintentionally limits participants to large firms. Small businesses, for example, are not generally aware of CISA, do not know how information sharing can help them, and find cybersecurity too expensive in general[53].

"Groups have begun testing their ability to share and receive indicators, but there is not yet sharing on a massive scale," Matthew J. Eggers, executive director for cybersecurity policy at the U.S. Chamber of Commerce, told U.S. representatives at a subcommittee meeting on information sharing[54].

Worries over legal liabilities continue despite the fact that a core reason for the passage of the *Cybersecurity Information Sharing Act* was to develop liability protections for companies.

Research in Focus

RealFactor Protection

Password is still the de-facto, major component in authentication; yet, everybody hates passwords. Users are forced to create and remember multiple complex passwords; security administrators constantly worry about attackers stealing passwords from corporate servers. The RealFactor project led by Wenke Lee, professor of computer science at Georgia Tech, aims to move all of us beyond passwords.

RealFactor leverages audio, video, cryptography and blockchain technologies to provide a frictionless authentication platform and service. RealFactor provides the best blend of security and usability. A user downloads the RealFactor mobile app to generate a public-private key pair, and announces the public key in a selfie video, thus binding himself to the key pair. After this initial setup, anytime the user wants to login to a website or server configured to use RealFactor for password-less, secure authentication, he just needs to specify his name (without having to type a password), and click on his phone upon receiving a confirmation message. RealFactor also makes account recovery much easier and more secure than any existing methods (e.g. two-factor, biometrics); all the user has to do is to generate another key pair on the (new) phone and announce it as before, and the RealFactor server can confirm the announcement is from the same user and proceed to retire his old key and start using the new one.

Without open sources and evidence, attribution meets skepticism

Deterring cyberattacks requires attribution, and a proper case against the aggressors requires public evidence. But building a case to prove guilt by a particular party is hard: Anyone can emulate a Chinese, Russian or American attacker on the Internet.

When Sony Pictures lost gigabytes of sensitive data — including e-mails between executives and the script for the latest James Bond movie[55] — a U.S. government investigation eventually placed the blame at the feet of North Korea. Yet, because the evidence was not released, many in the security community doubted those assertions[56].

In June, three security companies — Crowdstrike, Mandiant (now FireEye) and Fidelis Cybersecurity — concluded that Russian intelligence services had hacked the Democratic National Committee[57]. Yet, a purported Romanian hacker Guccifer 2.0 claimed that he had hacked the DNC and leaked sensitive documents as proof. While many security professionals believed Guccifer 2.0 to be a fiction of Russian intelligence, others accepted his boasts[58].

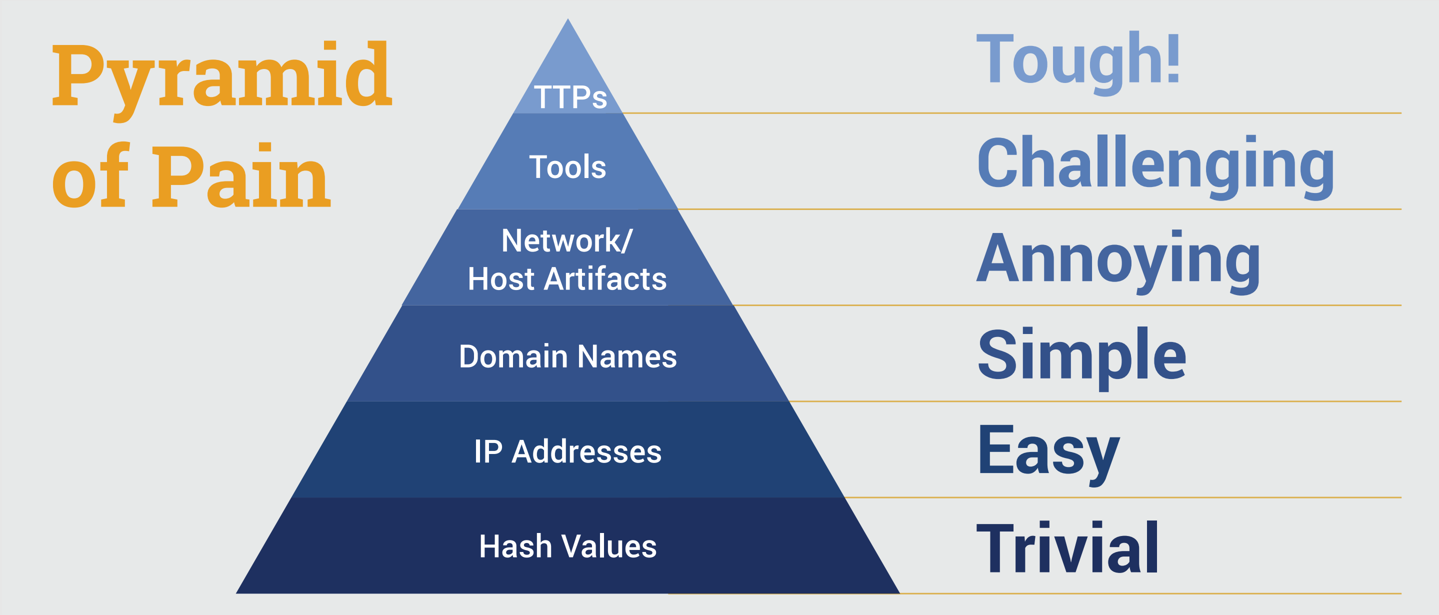
The incidents highlight that to have any hope of actionable attribution, open-source evidence is necessary, says Michael Farrell, associate director of attribution at the Institute for Information Security & Privacy at Georgia Tech and chief research scientist at the Georgia Tech Research Institute's Cyber Technologies & Information Security Lab. Without such attribution, nation states will have little reason to stop cyber operations.

"Cyber espionage has flourished due to a lack of [public] attribution," he says. "Nation states are practically compelled to leverage computer network operations for espionage — it's cheaper, easier, and more deniable than traditional spying techniques."

Public attribution appears to have some impact

Attribution is important, because the evidence suggests that deterrence based on public attribution produces policies that can reduce nation-state hacking.

In early 2013, incident response firm Mandiant produced a 74-page report laying the blame for more than 140 attacks firmly on the shoulders of an intelligence group within China's military[59], known as Unit 61398. Following the public outing, the United States gradually ramped up its policy against Chinese hacking, filing charges in May 2014 against five



Chinese operatives who were part of the intelligence unit[60]. And, in September 2015, the United States and China agreed that their governments would not conduct cyberattacks against each other for economic gain[61].

The efforts have apparently paid off. Starting in mid-2014, attacks attributed by FireEye to 72 Chinese-linked groups dropped off significantly[62].

"We attribute the changes we have observed among China-based groups to factors including President Xi's military and political initiatives, the widespread exposure of Chinese cyber operations, and mounting pressure from the U.S. Government," FireEye stated in the report.

Conversely, without attribution, deterrence seems unlikely. Security analysts and policymakers in the 21st century face a different reality in the digital world than during the Cold War, and the underlying fundamentals have changed. Farrell points to a key difference: militaries were the only ones building weapons 50 years ago, but today the Internet can be used by anyone for harm.

"The weapons are different; the timescales are different; the targets are much more diverse; and the players are more numerous and more diverse," he says. "America must be able to identify and discuss its adversaries in cyberspace. Military planners, policymakers, and network defenders alike all stand to gain from attribution."

There will not be a single path to security

Even with attribution, deterrence is not guaranteed. While the United States quickly pointed to North Korea as the source of the attack on Sony Pictures, in other cases, the U.S. government has refused to publicly attribute attacks. There is a reticence to talk about who is behind an attack, because businesses do not want to risk reputational damages and governments do not want to invite economic tension.

The solution to the problem may lay in analyzing the infrastructure that all Internet users — both defenders and attackers — have to use.

"Certainty is not likely possible for attribution but very high confidence is possible; difficult but doable," says Farrell.

Research in Focus

Science of Attribution

Internet miscreants rely on anonymity to conduct cyber campaigns. Many diverse threats share this common feature: DDoS attacks typically use spoofed packets to obscure the attacker; malware authors often strip identifying information from payloads; phishing attacks are categorically defined as a message with obscured, misleading origins.

Researchers at the Georgia Institute of Technology have pioneered early work in the field of traceback and attribution. These efforts help bring consequences to global cyberattacks. Georgia Tech's work frequently identifies miscreants, disrupts botnets, and assists those bringing justice to botmasters. Agencies and researchers are now looking beyond law-enforcement goals, and are interested in attribution for policy goals, diplomatic leverage, sanctions, and other consequences. There is a need to take the working examples GT has pioneered, and create tools and technologies that permit others to identify cyberattack origins. Attribution results must be accurate, timely, scalable, and perhaps most importantly sharable (if decision-makers chose to do so).

A team from GTRI, the School of Electrical & Computer Engineering, and the College of Computing have introduced a new framework for attribution. This framework recently was selected by DARPA for a large award under a new program entitled 'Enhanced Attribution.' The framework uses large public and private datasets to algorithmically attribute threats to virtual actors. As part of this program, Georgia Tech will provide unique datasets and efficient algorithmic attribution methods based on novel, tensor-based, machine learning methods.

One approach is to start by looking at targets: Who are the victims? Who is interested in the targeted information at the time? Farrell stresses that successful attribution research will have to climb what he calls the "attribution pyramid of pain." Harvesting data from each step is necessary to prove individual actor-level attribution and do it at scale, he says.

"At Georgia Tech, we believe this is possible and we are working to create foundational elements of the science of trackback."

As demand for security professionals rises, colleges adapt

The continuing supply-chain gap between qualified candidates and information-security roles means that today's millennials and Generation Z have been hearing about this problem their entire lives: a global shortfall of information-security workers that is expected to reach 1.5 million in just four years[63].

It appears that young adults are getting the message. Colleges and universities are experiencing record numbers of applicants to computer science degree programs, as younger generations pour into the discipline. The annual Taulbee Survey estimated that about 22,000 students graduated with a bachelor's in computer science in 2015 — a stunning 27 percent increase from the previous year[64]. Georgia Tech alone has experienced a 367 percent increase in applicants for its own undergraduate computer science program in the past five years.

It's a significant change from two years ago when government-designated Centers of Academic Excellence (181 colleges and universities) were found to have produced just 125 scholarship-for-service students each year, according to Seymour Goodman, professor in the Sam Nunn School of International Affairs, who led the study.

If the tide is turning, it still has a long way to go. The demand for cybersecurity professionals continues to build. Between 2010 and 2014, the number of cybersecurity job postings grew 91 percent, compared to 28 percent for information technology roles in general. Open positions are dominated by security engineers, administrators and managers, and security analysts, and it took 8 percent longer to fill those roles, compared to other information-technology positions[65].

The shortfall has led to an annual salary premium of $6,500 for cybersecurity workers[66], but even with that incentive, security professionals rarely stay in the same position for more than two years, leaving companies and organizations with a perpetual problem of filling empty desks.

Innovative companies are pairing up with universities

Young adults want to move into this lucrative field, but meeting their demand and closing the workforce gap requires innovative education delivery – online, on campus, or through continuing education at the worksite.

Contributors: Workforce Innovation

Nelson Baker
Dean,
Georgia Tech Professional Education

Mustaque Ahamad
Professor,
School of Computer Science
College of Computing

Zvi Galil
Dean,
College of Computing

Joe Bankoff
Chair,
Sam Nunn School of International Affairs
Ivan Allen College of Liberal Arts

Fred Wright
Deputy Director,
Cyber Technology & Information Security Lab,
Georgia Tech Research Institute

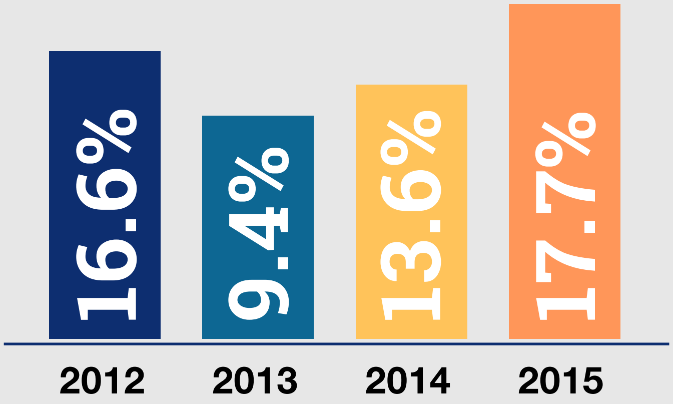
A variety of programs are trying to boost the numbers. In January 2014, for example, Georgia Tech launched its Online Masters in Computer Science (OMS CS) in cooperation with AT&T. Now numbering more than 4,000 online enrollees who take the same courses with the same professors as their on-campus counterparts, the OMS CS degree has been cited as capable of making an 8 percent dent alone in the workforce shortage[67]. The program represents a new kind of public-private partnership that could be used to boost cybersecurity knowledge around the world.

Creating the next generation of computer scientists also requires keeping curriculum fresh. With support from the National Science Foundation, Georgia Tech created two new courses and three new labs to integrate big data analytics and cybersecurity reasoning – a skill that every new computer scientist must know but has not been taught in an integrated fashion, says Assistant Professor Taesoo Kim in the School of Computer Science. Kim and fellow professor Hadi Esmaeilzadeh are collaborating on this effort.

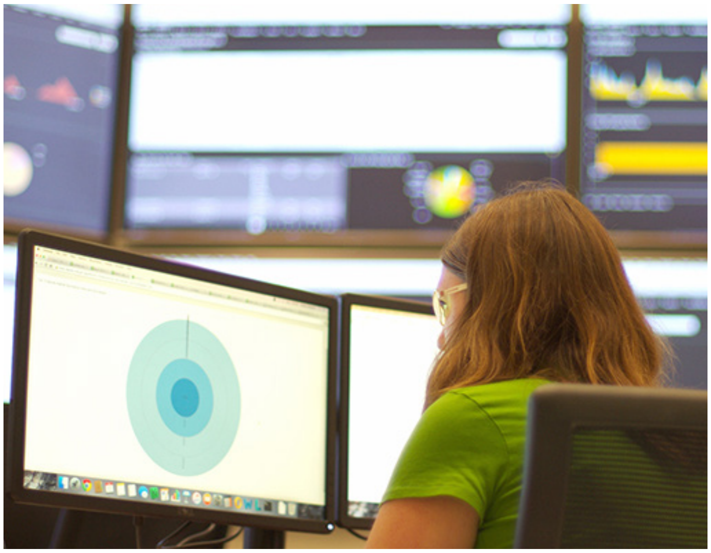
Well-crafted degree programs are needed to create a core group of cybersecurity experts who can design security into products, untangle advanced persistent threats, and train other workers. While this is a problem that the current volume of degree programs may not quickly solve, the increase in graduates can help guide future colleagues in the best way possible.

More Computer Science Graduates Fill Market Demand

More college students are graduating from schools with a bachelor's of computer science, with three of the last four years showing double digit growth in degrees awarded by U.S. institutions.



Computer Research Association's Taulbee Survey 2012 to 2015, http://cra.org/resources/taulbee-survey/. Data is a comparison between the current year and prior year for institutions that participated in the survey both years.



Corporate training also must adapt

Workers continue to be a weak point in organizational security, with more than half of all companies putting responsibility for a breach on negligent or malicious employees[68].   More than two-thirds of breaches involve phishing employees as a way to collect credentials, according to Verizon's latest Data Breach Investigations Report[69].

While most employees may be perceptive enough to spot phishing, the savviest attackers require just a single success. Given that more than 30 percent of phishing messages are opened and 12 percent of employees went on to click an attachment or link[70], businesses and government agencies are facing a major security problem, says Nelson Baker, dean of professional education programs at Georgia Tech.

"They can't hire their way out of these problems," he says. "The weakest link is your problem, and that's the humans."

Certified Information Security Systems Professionals (CISSPs) play an important role. Yet there are fewer than 120,000 holders of the various certifications offered by the International Information Systems Security Certification Consortium, or (ISC)2. In the United States alone, there were nearly 50,000 job openings in 2014, recruiting from a national pool of about 65,000 CISSP holders. Therefore, complete rank and file training is essential.

Developers and data analysts, for example, need to be knowledgeable in how to access sensitive data without compromising identities. The U.S. Army has created the U.S. Army Cyber School at Fort Gordon in Georgia to focus on training a new group of soldiers[71]. The school's basic class is Cyber Basic Officer Leaders Course, but the school plans to train soldiers throughout their careers. In addition, the military is training all its service members to hold some level of cybersecurity knowledge.

Training efforts needs to include C-suite and Board leadership, too. They require a broad view of the historical context and emerging threats in order to proactively manage, evaluate, and respond to employees, vendors, suppliers and hackers.

> *“...They can't hire their way out of these problems. The weakest link is your problem and that's the humans...”*
>
> — **Nelson Baker**
> Dean, Georgia Tech Professional Eduacation

“It is not only the worker bees that we need to worry about, we need to worry about the decision makers as well,” says Mustaque Ahamad, a professor at the College of Computing who helped organize a new, week-long training course at Georgia Tech for C-Suite executives and military officers this year. “Everyone is driving a computer down the Internet highway, and in order to do that safely requires some awareness and understanding of cybersecurity concepts. We need to educate people to use the equivalent of the “seat belt” so they can do it safely and safeguard whatever they do online.”

Although 73,000 students graduated with a bachelor's, master's or Ph.D. degree in computer science in 2014 (the latest numbers from the National Center for Education Statistics)[72], companies and universities need to be innovative in their solutions, Goodman says.

“There is no single way that this is going to be solved,” he says. “Companies need all these different things – formal degrees, online degrees, CISSPs, and other certifications – and the route can be different to each one.”

Research in Focus

Training Up Big Data + Cybersecurity

Only a handful of students in any major have taken courses in big data processing, machine learning and cybersecurity. Only a handful of graduates can meet the requirements of a secure, big data system analyst. College of Computing faculty Taesoo Kim and Hadi Esmaeilzadeh are taking are taking a bold first step of correcting this problem by integrating data analytics and security together.

The pair introduced new course modules and labs in 2015-16 to teach a data-driven approach to malware analysis using machine learning techniques with the goal of understanding the process of acquisition, de-obfuscation, and how big data analysis can address the challenges of malware stealthiness and scale.

The pair also hope to create a mobile game that helps K-12 students understand the concept of “approximate computing” – a technique used in large-scale data analysis to boost speed and energy needs. This concept is so new to computing that few students are aware of its impact and potential use.

Appendix of References

[1] Lee, Robert et al. “Analysis of the Cyber Attack on the Ukrainian Power Grid.” Electricity Information Sharing and Analysis Center, 18 March 2016. PDF.

[2] Greenberg, Andy. “Spies Can Track You Just by Watching Your Phone’s Power Use.” *Wired*. Conde Nast, 19 Feb. 2015. Web. 16 July 2016.

[3] Pollack, Doug. “Is Medical Identity Theft Really a Problem?” idExperts Blog, 17 Aug. 2015. Web. 16 July 2015.

[4] Fitzpatrick, David, and Drew Griffin. “Cyber-extortion Losses Skyrocket, Says FBI.” CNNMoney. Cable News Network, 15 Apr. 2016. Web. 21 June 2016.

[5] Goldberg, Rafi. “Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities.” National Telecommunications & Information Administration, 13 May 2016. Web. 5 July 2016.

[6] Barrett, Brian. “The Apple-FBI Battle Is Over, But the New Crypto Wars Have Just Begun.” Wired.com. Conde Nast Digital, 30 Mar. 2016. Web. 15 June 2016.

[7] Lomas, Natasha. “No Backdoors But UK Government Still Wants Encryption Decrypted On Request…” *TechCrunch*. AOL Inc., 14 Jan. 2016. Web. 17 July 2016.

[8] Leite, Julia. “WhatsApp Ordered Blocked Again in Brazil Over Data Dispute.” *Bloomberg*. Bloomberg, LP, 2 May 2016. Web. 17 July 2016.

[9] D’Orazio, Dante. “China passes controversial anti-terrorism law to access encrypted user accounts.” *The Verge*. Vox Media, 27 Dec. 2015. Web. 17 Jul 2016.

[10] Comey, James. “Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?” Brookings Institution, Washington DC. 16 Oct. 2014. Keynote Address.

[11] Hill, Kashmir. “The Snowden Effect: Yahoo to Join Gmail In Offering Users End-to-End Encryption.” *Forbes*. Forbes Media, 7 Aug. 2014. Web. 2 Aug. 2016.

and

Swire, Peter, Justin Hemmings and Alana Kirkland. Working Paper. “Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others.” Copy at http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.may_2016.PDF.

[12] Lemos, Robert. “Scuttling of Safe Harbor Leaves Companies in Holding Pattern.” *eWEEK*. QuinStreet, 11 Oct. 2015. Web. 4 June 2016

[13] Lemos, Robert. “U.S. Business Concerned Over E.U. Panel Rejecting Data Privacy Accord.” *eWEEK*. QuinStreet, 17 Apr. 2016. Web. 3 June 2016.

[14] Meng, Wei, Ren Ding, Simon P. Chung, Steven Han, and Wenke Lee. “The Price of Free: Privacy Leakage in Personalized Mobile In-Apps Ads.” *Proceedings of The 2016 Network and Distributed System Security Symposium (NDSS)*, San Diego, CA. Feb. 2016.

[15] “Replace Outdated Voting Machines.” Brennan Center for Justice. New York University School of Law, 4 Feb. 2016. Web. 21 June 2016.

[16] Nakashima, Ellen. “Cyber researchers confirm Russian government hack of Democratic National Committee.” *Washington Post*, 20 June 2016. Web. 20 June 2016.

[17] Nakashima, Ellen. “Russian government hackers penetrated DNC, stole opposition research on Trump.” *Washington Post*, 14 June 2016. Web. 17 June 2016.

[18] Bousquet, Steve. “Cybersleuth’s Hacking of Florida Elections Websites Draws Criminal Charges.” *Tampa Bay Times*. Tampa Bay Times, 4 May 2016. Web. 21 June 2016.

[19] Robertson, Jordan, Michael Riley, and Andrew Willis. “How to Hack an Election.” Bloomberg.com. Bloomberg, 31 Mar. 2016. Web. 21 June 2016.

[20] Tveten, Julianne. “Los Angeles County Voting to Shift from Inkblots to Open Source.” *Ars Technica*. Conde Nast, 13 June 2015. Web. 19 June 2016.

[21] Okun, Eli. “Travis County Forges New Territory in Creating Voting Machine.” *The Texas Tribune*. The Texas Tribune, 09 July 2014. Web. 21 June 2016.

[22] Lim, Andra. “Travis County, TX Developing Electronic Voting System With a Paper Trail.” *Government Technology*. E.Republic, 15 July 2014. Web. 21 July 2016.

[23] Fitzpatrick, David, and Drew Griffin. “Cyber-extortion Losses Skyrocket, Says FBI.” CNN Money. Cable News Network, 15 Apr. 2016. Web. 21 June 2016.

[24] Gallagher, Sean. “Sony Pictures Malware Tied to Seoul, ‘Shamoon’ Cyberattacks.” Ars Technica. Conde Nast, 04 Dec. 2014. Web. 21 June 2016.

[25] Liviu Arsene and Alexandra Gheorghe. “Ransomware, A Victim’s Perspspective.” Bitdefender, Feb. 2016. PDF.

[26] Lemos, Robert. “How Greed Could Destroy the Ransomware Racket.” PCWorld. IDG Consumer, 28 June 2016. Web. 22 July 2016.

[27] Nelms, Terry, Roberto Perdisci, Manos Antonakakis, and Mustaque Ahamad. “Towards Measuring and Mitigating Social Engineering Software Download Attacks.” *Proceedings of the 25th USENIX Security Symposium*, Austin, Texas. Aug. 2016.

[28] Mueller, Milton. “Is the West Giving Up on Freedom of Speech? Terror, Hate and the EU Internet Forum.” Internet Governance Project Blog. Internet Governance Project, 7 June 2016. Web. 6 July 2016.

[29] Kenner, Robert, Paul Taylor. “War Letters.” 2001 WGBH Educational Foundation. Public Broadcasting System

[30] Rosenberg, Eli. “Fake New York Times Article Claims Elizabeth Warren Endorsed Bernie Sanders.” The New York Times. The New York Times, 29 Feb. 2016. Web. 23 July 2016.

[31] Chen, Adrian. “The Agency.” The New York Times Magazine. New York Times Co., 2 June 2015. Web. 21 June 2016.

[32] Nunez, Michael. “Former Facebook Workers: We Routinely Suppressed Conservative News.” Gizmodo. Gawker Media, 9 May 2016. Web. 6 July 2016.

[33] Malik, Om. “Facebook’s News Feed: Often Changed, Never Great.” *The New Yorker*. Conde Nast, 1 July 2016. Web. 5 July 2016.

[34] Dye, Michaelanne; Ana Antón, and Amy S. Bruckman. “Early Adopters of the Internet and Social Media in Cuba.” *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work and Social Computing 2016*, San Francisco, CA. 27 Feb. – 2 Mar. 2016. Press Release.

[35] Liao, Xiaojing et al; “Seeking Nonsense, Looking for Trouble: Efficient Promotional-Infection Detection through Semantic Inconsistency Search.” *Proceedings of the 37th IEEE Symposium on Security and Privacy*, San Jose, CA. 23-25 May, 2016.

[36] Lynch, Sarah N. “Justice Department unveils ‘largest takedown ever’ to combat Medicare fraud.” Reuters, 22 June 2016. Web. 22 June 2016.

[37] Khazan, Olga. “U.S. Healthcare: Most Expensive and Worst Performing.” *The Atlantic*. The Atlantic Monthly Group, 16 June 2014. Web. 22 June 2016.

[38] “A Robust Health Data Infrastructure.” JASON. The MITRE Corp., Nov. 2013. PDF.

[39] “Internet Security Threat Report 2016.” Symantec (12 April 2016) 52-53. PDF.

[40] Schlesinger, Jennifer. “Tax Scammers New Target? Your Medical Records.” CNBC, 11 Mar. 2016. Web. 25 July 2016.

[41] Humer, Caroline, and Jim Finkle. “Your Medical Record Is worth More to Hackers than Your Credit Card.” Reuters. Thomson Reuters, 24 Sept. 2014. Web. 25 July 2016.

[42] Cha, Ariana Eunjung. “Researchers: Medical errors now third leading cause of death in United States.” *The Washington Post*. Washington Post, 3 May 2016. Web. 22 June 2016.

[43] “Internet of Things could be the low-cost ‘connectivity key’ that transforms lives in developing countries.” ITU Press Release. International Telecommunications Union, 19 Jan. 2016. Web. 10 June 2016.

[44] Nedeltchev, Plamen. “The Internet of Everything is the New Economy.” Cisco, 29 Sep. 2015. Web. 10 June 2016.

[45] Loper, Margaret. “Trusted Behaviors in Machine-to-Machine Systems.” Georgia Tech Research Institute, 10 March 2016. Unpublished concept paper.

[46] “Navigant Research Leaderboard Report: Smart City Suppliers.” Navigant Research, 29 Feb. 2016. Web. 20 June 2016.

[47] “NSTAC Report to the President on the Internet of Things.” The President’s National Security Telecommunications Advisory Committee, 18 Nov. 2014. PDF.

[48] “The DIGIT Act: Moving on to the US Senate.” *The National Law Review*. Morgan, Lewis & Bockius LLP, 29 Apr. 2016. Web. 20 June 2016.

[49] U.S. House of Representatives. Energy and Commerce Committee. *Latta and Welch Launch Bipartisan Internet of Things Working Group*. energycommerce.house.gov. N.p., 24 May 2016. Web. 18 July 2016.

[50] Lemos, Robert. “Tech Allies Lobby to Keep U.S. Rule From Fettering Security Research.” eWEEK. QuinStreet, 14 Sep. 2015. Web. 22 June 2016.

[51] Porter, Christopher. “Opinion: How to craft a meaningful cyberarms pact.” The Christian Science Monitor. The Christian Science Monitor, 23 June 2016. Web. 23 June 2016.

[52] Bilge, Leyla and Tudor Dumitras. “Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World.” Proceedings of the Conference on Communications and Computer Security. 16-18 Oct. 2012, Raleigh, NC. Association of Computing Machinery. PDF.

[53] Sage, Ola. “Prepared Testimony and Statement for the Record during the Hearing on ‘Oversight of the Cybersecurity Act of 2015’.” House Homeland Security Committee’s Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee. U.S. Congress, 15 June 2016. PDF.

[54] Eggers, Matthew. “Statement of the U.S. Chamber of Commerce on the Oversight of the Cybersecurity Act of 2015.” House Homeland Security Committee’s Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee. U.S. Congress, 15 June 2016. PDF.

[55] Grisham, Lori. “Timeline: North Korea and the Sony Pictures hack.” *USA Today*. USA Today Network, 5 Jan. 2015. Web. 13 June 2016.

[56] Zetter, Kim. “The Evidence That North Korea Hacked Sony Is Flimsy.” Wired.com. Conde Nast Digital, 17 Dec. 2014. Web. 21 June 2016.

[57] Nakashima, Ellen. “Cyber Researchers Confirm Russian Government Hack of Democratic National Committee.” *Washington Post*. The Washington Post, 20 June 2016. Web. 25 July 2016.

[58] Rid, Thomas. “All Signs Point to Russia Being Behind the DNC Hack.” Motherboard. Vice Media LLC, 25 July 2016. Web. 25 July 2016.

[59] “APT1: Exposing One of China’s Cyber Espionage Units.” Mandiant, 19 Feb. 2013. PDF.

[60] “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage.” U.S. Department of Justice, 19 May 2014. Web. 20 June 2016.

[61] Nakashima, Ellen and Steven Mufson. “U.S., China vow not to engage in economic cyberespionage.” *The Washington Post*. Washington Post, 25 Sep. 2015. Web. 20 June 2016.

[62] “Red Line Drawn: China Recalculates its Use of Cyber Espionage.” FireEye iSIGHT Intelligence, 20 June 2016. Web. 21 June 2016.

[63] Suby, Michael, Frank Dickson. "The 2015 ISC^2 Global Information Security Workforce Study." Frost & Sullivan, 16 April 2015.PDF.

[64] Zweben, Stuart and Betsy Bizot. “2015 Taulbee Survey.” *Computing Research News*, May 2016. Computer Research Association. PDF.

[65] Slide deck. “Job Market Intelligence: Cybersecurity Jobs, 2015.” Burning Glass, 2015. PDF.

[66] Slide deck. “Job Market Intelligence: Cybersecurity Jobs, 2015.” Burning Glass, 2015. PDF.

[67] Goodman, Joshua, Julia Melkers, and Amanda Pallais. Working Paper. “Can MOOCs Increase Access to Education?: Evidence from a Large New Computer Science Degree Program”. Copy at http://j.mp/13zEybo

[68] “Managing Insider Risk through Training & Culture.” Ponemon Institute. Experian Data Breach Resolution, May 2016. PDF.

[69] “2016 Data Breach Investigations Report.” Verizon (April 2016) 18-19. PDF.

[70] “2016 Data Breach Investigations Report.” Verizon (April 2016) 18-19. PDF.

[71] Seffers, George. “U.S. Army Build Cyber Branch One Step at a Time.” Signal. Armed Forces Communications and Electronics Association, 1 Apr. 2015. Web. 26 Jul 2016.

[72] “WebCASPAR: Integrated Science and Engineering Resource Data System.” National Science Foundation, n.d. Web. 2 Aug 2016.

266 Ferst Dr. NW
Atlanta, GA 30332

@IISPatGaTech

iisp.gatech.edu

Georgia Tech | Institute for Information Security & Privacy