GEORGIA TECH INFORMATION SECURITY CENTER

Emerging Cyber Threats Report for 2009

Data, Mobility and Questions of Responsibility will Drive Cyber Threats in 2009 and Beyond

On October 15, 2008, the Georgia Tech Information Security Center (GTISC) hosted its annual summit on emerging security threats and countermeasures affecting the digital world. At the conclusion of the event, GTISC released this Emerging Cyber Threats Report—outlining the top five information security threats and challenges facing both consumer and business users in 2009. This year's summit participants include security experts from the public sector, private enterprise and academia, reinforcing GTISC's collaborative approach to addressing information security technology and policy challenges.

"As one of the leading academic research centers focused on information security, GTISC believes strongly that a proactive and collaborative approach to understanding emerging threats will help us develop more effective information security technologies and strategies," said Mustaque Ahamad, director of GTISC. "The annual GTISC Security Summit on Emerging Cyber Security Threats and our annual Emerging Cyber Threats Report seek to give us a better understanding of the cyber security challenges we will face in the years ahead."

GTISC research and advance interviews with key information security experts from government, industry and academia uncovered five specific trends and some profound questions that will drive threats and countermeasures in 2009 and beyond, including:

Malware

Botnets

Cyber warfare

Threats to VoIP and mobile devices

The evolving cyber crime economy

In an effort to inform the broader community about current and future risks, this report will describe each emerging threat, existing or potential countermeasures, and how the threat may evolve in the coming year. In addition, our experts will offer their opinion on the role that Internet security education and regulation may play in further preventing the spread of cyber crime.

Emerging threats for 2009…all data-driven!

Data will continue to be the primary motive behind future cyber crime—whether targeting traditional fixed computing or mobile applications. According to security expert George Heron, "It's all about the data," whether botnets, malware, blended threats, mobile threats or cyber warfare attacks. And Heron expects data to drive cyber attacks for years to come. The data motive is woven through all five emerging threat categories, beginning with malware.

Malware

Ryan Naraine, security evangelist for Kaspersky, believes that malware delivery—the first step in creating a bot—will become more insidious by taking advantage of poorly configured Web sites, social networking sites and false domains.

"We are projecting a 10-fold increase in malware objects detected in 2008," said Naraine. "This is 'hockey-stick' growth driven by identity theft and data-focused cyber crime."

Naraine expects criminal senders to use better social engineering techniques to cloak malcode in what appears to be legitimate email with acceptable Web links. For example:

A Facebook message sent from one friend to another includes a link to a YouTube video of interest to the recipient. The recipient clicks on the link supposedly sent by his/her friend, and then sees a prompt to install the latest version of Flash Player in order to watch the video clip. The user clicks to install the update, but actually installs a piece of malware on the machine, effectively involving the computer in a botnet.

As cyber criminals move beyond mass-distribution style phishing scams, they are learning how to localize and personalize their attacks for better penetration. Social networking sites like MySpace, Facebook and others will likely be used as delivery mechanisms to get unsuspecting users to a malicious Web site link in order to deliver malware. In the coming year, GTISC and other security experts also expect more targeted spear-phishing vehicles to install malware and/or steal data. For example:

Attackers might target customers of a local credit union with a spoofed email referencing a local news story of interest. When customers click the bogus link in the email, the malware is installed and can log keystrokes and mine other personal data to be sent back to a malicious bot master or cyber criminal.

Naraine cited computing mono-cultures and slow or non-existent desktop application patching as fueling the malware/botnet crisis. "When you have nearly 100 percent of users standardized on a single application, it means that a single point of security failure can lead to infection of an entire computing ecosystem," said Naraine.

Naraine's research indicates that some of the largest botnets are comprised of corporate machines. "It takes the average corporation two to three months to apply a Windows patch across all devices, so malware and botnets will continue to take advantage of known vulnerabilities within enterprise environments."

On the bright side, many software vendors are now shipping auto-patch/update capability with each new software release. Firefox, Adobe and Apple all do this. And Naraine believes that Microsoft operating system security has improved with each successive release. The auto-update features help both corporate and consumer end users stay up to date with patches—which eliminates a lot of "low-hanging fruit" for the cyber crime community.

A total of 28940 different malicious and potentially unwanted programs were detected on users' computers in August. That is an increase of more than 8,000 on July's figures and points to a significant increase in the number of in-the-wild threats.

http://www.kaspersky.com/news?id=207575678

"We are so conditioned to click on links, and the bad guys know this," said Naraine. "The email lures, the enticements and the personalization of malware attacks are getting much better. Social engineering attacks on social networks are beginning to explode and will only get worse."

Ryan Naraine - Security Evangelist, Kaspersky Lab, Americas

Botnets

In 2008, botnets have become worse—a trend expected to continue next year. GTISC estimated in last year's report that 10 percent of online computers were part of botnets, groups of computers infected with malicious code and unknowingly controlled by a malicious master. This year, GTISC researchers estimate that botnet-affected machines may comprise 15 percent of online computers.

"Compared with viruses and spam, botnets are growing at a faster rate," said Wenke Lee, an associate professor at GTISC and a leading botnet researcher. Lee cites three unavoidable factors that are spurring botnet growth:

- Infection can occur even through legitimate Web sites
- Bot exploits/malware delivery mechanisms are gaining sophistication and better obfuscation techniques
- Users do not have to do anything to become infected; simply rendering a Web page can launch a botnet exploit

Bots can be delivered to a machine in a variety of ways—via Trojans, emails, an unauthorized instant message client or an infected Web site. Once installed, bots lie low to avoid notice by antivirus and anti-spyware technology. Periodically, the bot communicates to a "command and control" server and waits for a response. The communication—using the command and control server as an intermediary—can keep the malicious bot master's identity hidden.

Lee points out the distinction between botnets and malware: "What we think of as malware can be responsible for turning a machine into a bot," said Lee. "But traditional malware is a single-purpose attack. A bot actually remains on the machine, maintains a command and control mechanism to enable communication with the bot master, and can update itself based on those communications. The updates enable new bot communication and malicious capabilities, and are often used to avoid detection."

Bot communications are designed to look like normal (Web) traffic using accepted ports, so even firewalls and intrusion prevention systems have a hard time isolating bot messages. Lee agreed, "It's very difficult to filter bot traffic at the network edge since it uses http and every enterprise allows http traffic."

Prompted to act in unison, bots become bot armies that harness considerable computing power to engage in a variety of malicious activities, including:

— Data theft (social security numbers, credit card information, trade secrets, etc.)

— Denial of service attacks

— Spam delivery

— DNS server spoofing

According to a report compiled by Panda Labs, in 2Q 2008, 10 million bot computers were used to distribute spam and malware across the Internet each day[1]. Damballa continues to discover that 3-5 percent of enterprise assets are compromised on average by targeted threats such as bots—even in the presence of the best and most up-to-date security. Leading industry analysts predict this number to be even higher.

Most botnet command and control sites can be traced back to China[2]. But Lee cautions that this statistic could be misinterpreted because "a lot of Chinese are using

[1] http://www.darkreading.com/document.asp?doc_id=161524

[2] Source: Damaballa; http://www.damballa.com/downloads/press/GartnerITSecSummit_Q2Research_PRFINAL_2008-06-02_.pdf

Botnets Continue to Grow and Transform

Bot Army Name	Number of Binaries	Distinct Compromised Hosts in Typical Enterprise	Distinct Binaries per Compromise
RAT-SZ-1	10,493	155	67.7
Sality-1	886	18	49.2
IRC-VR-1	804	75	10.7
IRC-SD-1	541	11	40.2
Poebot-1	369	2	184.5
RAT-DL-1	212	14	15.1
Metcash-1	194	47	4.1
IRC-SD-2	139	21	6.6
RAT-SM-1	54	4	13.5
Kraken	48	301	0.2

pirated software which doesn't receive security updates."

According to Lee, "That means many Chinese computers are rife with vulnerabilities, making them a haven for botnet command and control sites."

Botnets en masse are considered a bot army and these malicious computing forces may be used to conduct cyber warfare in the future. In addition, bot payloads are becoming increasingly complex to avoid evolving security measures. According to Lee's research at GTISC, several recent bot variants have exhibited more than 100 distinct binary payloads used to hide the communications path and to vary the command and control IP address. The net effect makes botnets and bot masters harder to track.

However, new technologies can pinpoint the Internet communications between botnets and bot masters and shut down the vital links required for cyber crime and cyber warfare. Signature-based defenses like antivirus and intrusion detection are no match for the subtle communications between bot and bot master. But newer behavior analysis techniques can help identify bots without signatures.

Lee's research team at GTISC is developing algorithms to analyze traffic patterns from internal machines to outside machines. Strange anomalies in connection duration, time of day, or type of information uploaded/downloaded can indicate a botnet command and control attempt. Lee's research also examines how botnets use the Internet infrastructure. For example, look-up requests to DNS servers might provide information on which domain is used for botnet communications. In addtion, global sensor networks are now using specialized algorithms to pinpoint bot army communications. Once the command and control links are found and disrupted, the bot army threat can be neutralized as long as layered security is already in place.

Cyber Warfare

Security experts consulted by GTISC believe cyber warfare will accompany traditional military interaction more often in the years ahead. They expect it will also play a more shadowy role in attempts by antagonist nations to subvert the U.S. economy and infrastructure.

Consider the cyber attacks that occurred between Russia and Georgia earlier this year as a model for military cyber engagements in 2009 and beyond. Don Jackson, director of threat intelligence for SecureWorks, compiled the following research to implicate direct Russian government involvement in cyber attacks against Georgia:

Physical and cyber attack targets and timing align:

- Logs of DDoS traffic and changes in network routing indicate that Russian cyber warfare operations coincided almost exactly with the final "all clear" for Russian Air Force attacks sometime between 0600 and 0700 on August 9, 2008.
- Both cyber attack targets (media outlets and local government communication systems) and air force targets were located in the Georgian city of Gori.
- The exact timing of cyber attacks against new classes of targets in Gori and Russian Air Force attacks indicated coordination between known hacking groups and military operators.

Source of Russian cyber attacks against Georgia:

- The vast majority of Georgian Internet traffic is routed through Turkey and Russia. As of August 10, 2008, traffic routed through Turkey was almost completely blocked, and IP traffic through Russia (via Azerbaijan) was slow and effectively unusable.
- Russian government-run Rostelecom conducted most of the routing changes that blocked traffic to Georgian IP address space.
- The Moscow-based COMSTAR network also cooperated with government demands to follow suit, as did other network operators that control routing through the ostensibly neutral Moscow Internet Exchange (MSK-IX).
- DDoS and cache poisoning attempts targeting DNS servers for major Georgian networks were also launched from the state-operated Rostelecom and Moscow-based COMSTAR networks. These attempts utilized the same tools, tactics and target lists as attacks from portions of Turkish networks controlled by former associates of the Russian Business Network (RBN). The associates are believed to have connections to local St. Petersburg government, the former powerbase of Putin and those now in charge of the FSB state security organization.

Attack types:

- In addition to DDoS attacks against Georgian media outlets and government Web sites, researchers observed:
  - — Route hijacking
  - — Brute force server compromise
  - — Data theft
  - — Multi-factor DDoS attacking network and application layers
  - — Defacement and hosting of fake Georgian Web pages containing misinformation and propaganda.

Some DDoS attacks, route hijacking, and system intrusions originated from sources not previously affiliated with known hacking groups and appear to have been coordinated in a manner that would allow attackers to disable or intercept Georgian government communications in accordance with Russian military and intelligence objectives.

Jon Ramsey, chief technology officer for SecureWorks attributes increasing cyber warfare activity to the following:

- The low cost to launch cyber attacks compared with physical attacks
- The lack of cyber defenses
- The "plausible deniability" the Internet affords
- The lack of "cyber rules of engagement" in conflicts between nation states

George Heron, founder of BlueFin Security and former chief scientist for McAfee believes cyber warfare will play a significant role between China and the U.S. "Cyber threats originating from China are very real and growing," said Heron. "Other evidence supports this, such as the majority of bot masters being traced back to China, along with malware and other disruptive threats."

Heron pointed to the U.S. transportation system infrastructure, the telecommunications system, nuclear energy plant communications, the water supply IT infrastructure and other entities as prime cyber targets of enemy nations.

"We now know that it only takes infiltrating the DNS operator vulnerability to subvert an entire DNS sector," Heron continued. "Cyber warfare efforts could take this approach to exploit vulnerable servers and gateways controlling the power grid or water/dam flow control."

Howard A. Schmidt, a GTISC professor of practice agrees. "Our critical infrastructure systems are fundamentally dependent on the Internet and IP-based technology, and there are interdependencies between them that our enemies will seek to exploit," said Schmidt. "Cyber warfare completely evens the playing field as developing nations and large nations with a formidable military presence can both launch equally damaging attacks over the Web."

The U.S. government is already bracing for the inevitability of cyber warfare and hosted the second annual Cyber Storm exercise in March 2008—involving nine states, four foreign governments, 18 federal agencies and 40 private companies in a weeklong cyber attack scenario[3].

"Cyber Storm II is a successful instance of public and private partnership to identify cyber warfare threats and plan effective countermeasures," said Heron. "We need more information sharing and more collaboration like this to defend our national interests against an onslaught of cyber terrorism."

Schmidt advocates a three-step approach to bolstering U.S. cyber defenses:

- Identify the Internet-enabled systems we depend on and also the interdependencies between them.
- Develop a comprehensive plan to protect those systems, including roles and responsibilities, vulnerability identification and remediation, threat mitigation and response.
- Design information security for the future as software improvements, network enhancements and new technologies like mobile communications gain traction.

[3] Source: Federal Computer Week, Cyber Storm II Stirring; Feb. 29, 2008; http://www.fcw.com/online/news/151806-1.html

> "The future threat goes beyond what we think of as cyber-espionage and intellectual property theft, although that certainly remains a factor," said Heron. "I think we're going to see more technologically savvy, state-sponsored attacks to the IT systems that support foundational services here in the U.S."
>
> **George Heron - Founder, BlueFin Security**

Threats to VoIP and Mobile Convergence

The cell phone is becoming an entirely new tool—especially outside the U.S., where accessing the Internet from a mobile device can provide a better experience than traditional fixed computing. VoIP technology also continues to improve and will rival landline and mobile communications in terms of reliability and call quality. As Internet telephony and mobile computing handle more and more data, they will become more frequent targets of cyber crime.

From the outset, VoIP infrastructure has been vulnerable to the same types of attacks that plague other networked computing architectures. When voice is digitized, encoded, compressed into packets and exchanged over IP networks, it is susceptible to misuse. Cyber criminals will be drawn to the VoIP medium to engage in voice fraud, data theft and other scams—similar to the problems email has experienced. Denial of service, remote code execution and botnets all apply to VoIP networks, and will become more problematic for mobile devices as well.

"Criminals know that VoIP can be used in scams to steal personal and financial data so voice spam and voice phishing are not going away" said Tom

Cross,a researcher with the IBM Internet Security Systems X-Force team. "Denial of service will also continue to be a significant threat to VoIP. If a large number of VoIP phones become infected by malware and flood a network with traffic, the results could be extremely disruptive. We expect some cyber criminals to attempt to blackmail carriers based on a DoS attack scenario."

According to Cross, large telecom companies in Europe are now servicing customers with VoIP. And where phone service is concerned, users have a different mentality about sharing personal information and a higher expectation of quality.

On the bright side, Cross believes the IT and telecom communities have learned valuable security lessons from the spam and phishing problems that have plagued the Simple Mail Transfer Protocol (SMTP).

"VoIP providers and users want to avoid the spam crisis that has inundated email," said Cross. "Current research efforts at university-based centers like GTISC are studying how reputation networks based on inherited trust could be applied to VoIP to prevent voice fraud. In this type of system, good security reputations will improve VoIP peering and call ranking so that legitimate calls get through, and voice spam and phishing are blocked."

Cross also cited the need for intrusion prevention systems at the VoIP carrier level, along with endpoint security for Session Initiated Protocol (SIP) phones and other VoIP devices.

When it comes to the mobile experience, the iPhone has dramatically changed the perception of what mobile devices can do, and who is using them. Now in addition to business users, consumers are more likely to want the advanced capabilities of a smartphone for everything from mobile banking to iTunes access.

"While exploits targeting the iPhone have circulated publicly, I'm somewhat surprised that there haven't been more attacks to date," said Cross. "Financial motivation and increased adoption will increase attacks to smartphones in the years to come. As more payment infrastructure gets placed on these devices, they will become a more attractive target."

Dave Amster, vice president of security investigations for Equifax also sees the security challenges presented by mobile computing. "More and more financial transactions will take place over mobile devices," said Amster. "Consumers are ordering credit reports from their Blackberrys, which puts valuable information at risk. The challenge for businesses and banks is going to be maintaining secure mobile applications and ease of use at the same time."

Patrick Traynor, an assistant professor in the School of Computer Science at Georgia Tech and a member of GTISC, discussed the concept of the "digital wallet," in which smartphones store personal identity, payment card information and more. Already in Japan, people use their cell phones at vending machines and subway token dispensers.

According to Traynor, "malware will be injected onto cell phones to turn them into bots. Large cellular botnets could then be used to perpetrate a DoS attack against the core of the cellular network. But because the mobile communications field is evolving so quickly, it presents a unique opportunity to design security properly—an opportunity we missed with the PC."

Traynor pointed out that most people buy a new mobile device every two years—a much shorter life cycle than the typical PC and Windows installation, which is closer to 10 years.

"The short life cycle of mobile devices gives manufacturers, developers and the security community an opportunity to learn what works from a security standpoint and apply it to devices and applications more quickly," said Traynor. "However, it is not going to be an easy problem to solve."

Traynor pointed to battery power as a primary security hurdle, "If you place antivirus software on a mobile device, it will run the battery down, so mobile security will require new approaches and partnerships between manufacturers, carriers and application developers." Researchers like Traynor and Cross expect open standards for handset security to gain more ground in 2009. They both cited Google's Android platform for mobile applications as a step in the right direction. Android

"Most people have been trained to enter social security numbers, credit card numbers, bank account numbers, etc. over the phone while interacting with voice response systems," said Cross. "Criminals will exploit this social conditioning to perpetrate voice phishing and identity theft. At the same time, customers will demand better availability from phone service than they would from an ISP, so the threat of a DoS attack might compel carriers to pay out on a blackmail scam."

Tom Cross - X-Force Researcher, IBM Internet Security Systems

"At this point, mobile device capability is far ahead of security," said Traynor. "We'll start to see the botnet problem infiltrate the mobile world in 2009."

Patrick Traynor - Assistant Professor, School of Computer Science at Georgia Tech, and member of the Georgia Tech Information Security Center

makes the mobile application development environment publicly available so that it becomes easier for application developers to apply security to programs designed for smartphones. Traynor and Cross also support a layered approach to security on mobile devices that encompasses carriers, manufacturers and application developers.

The evolving cyber crime economy

Sources of cyber crime will become increasingly organized and profit-driven in the years ahead. Gunter Ollmann, chief security strategist for IBM Internet Security Systems describes today's (and tomorrow's) cyber criminals as "an international conglomerate of professionally trained authors motivated by high profit."

You can buy, lease, subscribe and even pay-as-you-go to obtain the latest malware kits, which are much more sophisticated than their predecessors. "Malware transitioned to the criminal world just over three years ago," said Ollmann. "The new sophisticated malware-for-sale features encrypted command and control channels, built-in Web services for hosting phishing content, man-in-the-browser proxy engines for identity theft, along with drive scanners for capturing sellable data like email addresses and credit card details."

Ollmann reports that several malware kits are supported by product guarantees and service level agreements. A few malware developers are even offering multiple language "customer support" in order to reach a wider audience of criminals. New Web-based attack platforms have been developed in tandem so that social engineering and end-user action are no longer required for exploitation. All of these trends are expected to evolve further in the coming year.

The managed service approach basically extends the functionality of a malware purchase. One malicious managed service model revolves around breaking CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart). CAPTCHAs are used to prevent brute-force attacks and fraudulent account creation on Web sites and require end users to correctly enter a string of characters and login details before access is granted. As CAPTCHA systems were continuously broken by attackers and then subsequently strengthened against compromise, the cyber crime MSPs saw a business opportunity.

"The managed service operators provide cheap human labor to battle through CAPTCHAs," said Ollmann. "These predominantly Russian-operated entities offer pay scales starting at $1 per 1,000 CAPTCHAs broken, and provide an extensible API structure for easy integration into malware. This combined approach will continue in the future."

Ollmann divides the cyber criminal industry into three tiers:

- Low-level criminals who use kits to create the specific malware required for their targeted crimes.
- Skilled developers and collectives of technical experts creating new components to embed within their commercial malware creation kits.
- Top-tier managed service providers that wrap new services around malware kits to increase propagation and enable organized fraud on a global scale, feeding gains back into existing money laundering chains.

He warns of a tough road ahead in the battle against malware.

> "The Web-based attack platforms come in a variety of packages and are available for lease, purchase or any payment model in between," said Ollmann. "And for those criminals that don't want to host their attack platforms, managed service providers have emerged to rent existing installations for global malware delivery. Some of the MSPs charge on a per-click basis just like Web advertising."
>
> **Gunter Ollmann - Chief Security Strategist, IBM Internet Security Systems**

Expert opinion on Internet security education and regulation

Members of the security community have been engaged in debate over responsibility for security education and potential regulatory schemes to govern online behavior. The conversation may only become more heated in 2009. While the decentralized and open nature of the Internet can be extremely positive characteristics, malicious criminals are threatening the very foundations of the Internet.

Michael Barrett, the chief information officer for PayPal frames the debate in concrete terms, "Even if customers are confident in PayPal's security, but still don't think the Internet as a whole is safe, then we all lose." Barrett believes a robust debate will go on for the next few years between public and private entities about how best to protect the Internet ecosystem. "I think we have about 10 years to figure out how to structure Internet security principles and regulation before the problem of online fraud and cyber crime completely gets away from us," he said.

The borderless nature of the Internet, the astounding growth of online users, the difficulty in establishing trusted identity online and the lack of standardization around protection all contribute to the challenge of developing a regulatory scheme. But phishing and e-crime losses may compel interested parties to action.

So what would Internet security regulation look like? According to Barrett, it could follow the model of road and airline safety…

"We can even draw comparisons between car insurance and antivirus software," said Barrett, who believes that voluntary car insurance penetration would be about the same as antivirus software. "Most people buy car insurance because it is mandated by the government. Perhaps we need a similar mandate for keeping security protection up-to-date."

Barrett was also quick to point out his optimism when it comes to security. "I believe phishing is a completely preventable crime when you combine technology with education," he said. "Our anti-phishing efforts with Yahoo over a 10 month period prevented more than 85 million phishing emails from ever reaching the intended victim. And if we can teach end users some simple rules, it will have a big impact."

With a focus on preventing phishing emails from arriving in the inbox, PayPal now uses DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) to sign its customer emails. When the major ISPs see an email supposedly from PayPal—but without the proper DKIM or SPF signature—they block it.

"Technology is one piece of the puzzle, regulation is another and user education is the final hurdle," said Barrett. "Just 15 years ago, Mosaic 1.0 was released and the Internet as we know it was born. Back then about 1,000 people were using the Web. Today, there are more than one billion active Internet users. Yet despite this explosive growth, we've had no formal education about safe behavior on the Internet, and the security industry has never spoken with one voice."

Mustaque Ahamad, the director of GTISC, supports a combination of security awareness, education and personal responsibility. "Although we can argue that end users could do more to protect themselves and the online community, we should also expect more from the security industry in terms of viable solutions," said Ahamad.

Howard A. Schmidt believes the government should play a role in security regulation for cyber defense. "The government should establish a regulatory construct for assessing the state of security and setting minimum standards of security for entities that are part of our critical infrastructure," he said. "The goal would be to identify deficiencies and assess certain sectors with a security grade. It could be supported with a tax credit for businesses that make the grade. Most importantly, any government involvement should not inhibit innovation or investment."

"We can think of security as the environment of the Internet and cyber crime as the pollution that could effectively kill it," said Jon Ramsey of SecureWorks. "The problem is bigger than industry, end users and government boundaries. That's why GTISC research and the public/private collaboration it promotes is so important to finding solutions to the threats of the future."

> "If you own a dangerous old jalopy that can't pass emission standards and you want to drive it around your private 10-acre field, that's fine. But as soon as you take that unsafe car out onto the public road, you become a threat to others," said Barrett. "The same is true of a PC running Windows 98 and Internet Explorer 3 without any meaningful AV or firewall protection. If that machine never connects to the Internet, fine. But once it does, it can become infected and in turn be used to compromise more machines."
>
> **Michael Barrett - Chief Information Security Officer, PayPal**

GTISC Emerging Cyber Threats Report Contributors

Mustaque Ahamad
Director of the Georgia Tech Information Security Center

Dave Amster
Vice President of Security Investigations, Equifax

Michael Barrett
Chief Information Security Officer, PayPal

Tom Cross
X-Force Researcher, IBM Internet Security Systems

George Heron
Founder, BlueFin Security

Don Jackson
Director of Threat Intelligence, SecureWorks

Jeff King
Doctoral Student, Georgia Tech Information Security Center

Wenke Lee
Associate Professor, Georgia Tech Information Security Center

Ryan Naraine
Security Evangelist, Kaspersky Lab, Americas

Gunter Ollmann
Chief Security Strategist, IBM Internet Security Systems

Jon Ramsey
Chief Technology Officer, SecureWorks

Howard A. Schmidt
Professor of Practice, Georgia Tech Information Security Center

Patrick Traynor
Assistant Professor, School of Computer Science at Georgia Tech,
and member of the Georgia Tech Information Security Center

GEORGIA TECH INFORMATION SECURITY CENTER