script for GTCSS

From
La Bouff, Tara
To
Farrell, Michael D; Wenke Lee; Griessman, Gloria G; Doan, Trinh T; Panetta, Lindsey B; McPherson, Rojauna K; Formby, David J; Swire, Peter P; Kintis, Panagiotis
Recipients
Michael.Farrell@gtri.gatech.edu; [redacted]; Gloria.Griessman@gtri.gatech.edu; trinh.doan@iisp.gatech.edu; lindsey.panetta@gtri.gatech.edu; rojauna.mcpherson@iisp.gatech.edu; djformby@gatech.edu; Peter.Swire@scheller.gatech.edu; kintis@gatech.edu

Hi all, Attached is a draft script for the Summit. This largely represents Michael's script as emcee and will be used / adapted to help him introduce portions of the program, including your session at GTCSS – Georgia Tech Cyber Security Summit.

Please open this page to view the Summit agenda: http://iisp.gatech.edu/2017-cyber-security-summit

--

Tara La Bouff

Marketing Communications Manager

Institute for Information Security & Privacy at the Georgia Institute of Technology

(404) 769-5408 | tara.labouff@iisp.gatech.edu

266 Ferst Drive, Room KACB-3146

Atlanta, GA 30332

cyber.gatech.edu | @GaTechCyber

Script_GTCSS 17_recovered2.docx

Script_GTCSS 17_recovered2.docx

SCRIPT v1 – GT CSS 17

15th Annual Georgia Tech Cyber Security Summit

Sept. 27, 2017

c. Close D. Formby **Michael Farrell**

d. Close D. Dagon **Wenke Lee**

XI. Cocktail Mixer NA

I. ***Welcome / Call to Order & Thank Bo*** **Chris Jones**

Key message: cyber requires cooperation and creativity across all sectors.

9:00 a.m.

May I have your attention please?

[pause, repeat as needed]

Good morning and thank you for coming. We have a crowded Auditorium today. If you are an employee or student of Georgia Tech and see someone looking for a place to sit, please offer your chair to a guest. We have overflow seating in the room next door with a live video stream. Thank you.

[pause]

Good morning, I'm **Chris Jones, associate vice president for research** here at Georgia Tech.

We believe cybersecurity is **the MOST interdisciplinary field** of any in science today. Cybersecurity no longer is just a computer scientist's problem. With more connected devices than people in the world, **cybersecurity is EVERYONE'S problem**. It demands from all of us NEW focus, tenacity, creativity, and NEW cooperation.

Here at Georgia Tech, our cybersecurity research draws from all disciplines – computer science and engineering, of course, and also business, aeronautics, manufacturing, public policy… even vaccine creation in our top-ranked biomedical program, where cybersecurity researchers right now are working to protect the data behind vaccine construction while also making it readily usable in times of emergency. **As progress presents new challenges to solve, Georgia Tech is there.**

Earlier this month, we announced a new chapter for cybersecurity at Georgia Tech – a change in leadership. Bo Rotoloni has ceded his role as co-director of the Institute for Information Security & Privacy to a rising, young leader, Michael Farrell. Bo served as the founding co-director of the Institute for Information Security & Privacy – the organizing body for all cyber activity across campus and GTRI, Georgia Tech's applied research-and-development organization that contracts with you to create high-impact solutions. Bo led 500 cybersecurity researchers to regularly achieve more than $100-million annually in cyber research. His cyber labs have been the fastest growing, so now we're going to employ his talents to guide ALL areas of research at GTRI. Although he's not going far, he will be missed.

In appreciation, Bo, your staff, your fellow co-director Dr. Wenke Lee, and I, have a gift for you. *[presentation of gift –plaque)* Thank you, Bo, for your service to Georgia Tech, to the communities we serve, and to the advancement of cybersecurity.

II. ***Mission Speech & Introduction of Michael Farrell*** **Bo Rotoloni**

Key message: Cyber is a deep bench at GT and growing.

9:05 a.m.

Thank you, Chris. Thank you, everyone. It has been my pleasure to establish the Institute for Information Security & Privacy – or IISP – and create a bold, new framework to tackle cybersecurity. There certainly is no shortage of work to do.

When we formed the IISP two years ago, there were nine teams working as a lab or center to address cybersecurity, performing approximately $____ million in research annually. Today, there are **12 cybersecurity labs across Georgia Tech** – ranging in size from one that performs $86-million worth of annual work alone with 200 researchers… to one just established this fall with __ students, led by new faculty member Brendan Salt-a-form-aggi-o, who came to us from Purdue. It's an exciting time for cybersecurity – as you'll hear today – and a time of tremendous growth for cybersecurity at Georgia Tech. We are **doubling down** on our efforts to solve the most challenging problem of our time.

In turning over my reigns as co-director to Michael Farrell, I'm able to help all of GTRI deliver more solutions that support national defense, economic continuity and personal freedom.

Michael has the right combination of tenacity and technical skill to help organize others around the quest for better cybersecurity. His new role as co-director of the IISP aligns well with his work in the CIPHER Lab and his recent role as an associate director of attribution. For the past two years, Michael has led the largest research thrust of the IISP -- dedicated to attribution – and, along with colleagues on campus, has won more than $17-million in research awards to help solve that problem. He is chasing two more awards right now, which we hope to announce soon.

As a Ph.D. Alumnus of Georgia Tech, Michael has firsthand knowledge of the classroom experience, research instruction, as well as a deep history of performing sensitive technical operations with the U.S. Department of Defense, National Security Agency, and Intel Corp. I'm excited to watch Michael develop new conversations with many of you – *with any of you* who are interested in working alongside Georgia Tech to **create the next** cybersecurity solutions.

Please welcome Co-director Michael Farrell.

III. ***Overview of Theme & Introduction of Keynote*** **Michael Farrell**

Key message: This is a pivotal moment for Attribution, and what we're doing about it.

9:10 a.m.

[high energy] **Thank you, Bo. Hello and thank you** for joining us today at the 15th Annual Georgia Tech Cyber Security Summit! It is an honor to work alongside Dr. Wenke Lee as the next co-director of the I-I-S-P.

This… is the golden age of Attribution, and THAT is the theme of this year's Summit.

How do we do attribution well, persuade others it was done well, and how do we to maximize the deterrence effect of future cyberattacks by leveraging attribution?

There's no shortage of reasons right now to talk about attribution – the process of identifying who is behind a cyberattack… *[pause, slow down]* … The Equifax breach in our own backyards, voter rolls in multiple states that were hacked, questions over how the USS McCain crashed near Malaysia, and let's not forget *[speed up]* Target, Sony Pictures, Shadow Brokers, Merck, Maersk, Macron, Cloudbleed, and WannaCry.

Here are a few others you might recall this year: *[show slide?]*

Xbox, InterContinental Hotels Group, Arby's, Verifone, Dun & Bradstreet, Saks Fifth Avenue, Chipotle, Gmail, Brooks Brothers, DocuSign, Washington State University, Blue Cross Blue Shield (again), and Verizon.

Despite what feels like a blitzkrieg of attacks from every direction, we're here to tell you that **this is a transformational moment for attribution**.

Michael – I need you to elaborate on little more on why. I took this cue from Stewart and am suggesting reasons below that you may/may not agree with. Feel free to copiously correct/edit…

The volume of attacks has captured everyone's attention. Whether you are a lawmaker in D.C., the commander of a squadron, an executive, retail clerk, or a pre-teen toying with PlayStation…. if you weren't aware before, you are now. Awareness is the first step toward resolving any ill. That's one reason we call this a transformational moment.

The second is that recent high-profile cases proved that attribution *can* be done. Georgia Tech alum Dmitri Alperovitch and his team at Crowdstrike responded when the DNC called. They pinpointed Russia as the "cozy bear" and "fancy bear" behind that attack. While his methods are still a topic of much debate among information security circles, Crowdstrike's bold claims charted a path and an example for others as they decide whether to "name names" publicly in the wake of an attack.

Now, the leading question is …. *Which one from the pre-panel list do you want to call out?*

Researchers at the Institute for Information Security & Privacy at Georgia Tech are working across several fronts of the attribution problem set -- spanning activities such as cyber espionage, cyberattack, and cyber influence. Today, we're going to discuss the **new techniques and considerations** for corporations, diplomatic relations, and law enforcement which impact all of us.

Our MISSION at Georgia Tech is to act ACROSS ALL SECTORS to:

· be **the CENTRAL point of conversation** for all of you -- gathering government, industry and academia for cross-talk that truly creates the next solution.

· to coordinate large-scale research projects with diverse partners

· **and to continually EXPAND cybersecurity** into non-traditional areas of campus so that all future professionals under any field can ensure that data is protected as we use it and kept private when we don't.

[with energy and determination] **Georgia Tech is where big questions lead to new ideas, and those ideas lead to solutions. It is innovative research with practical impact**.

Whether you work at a government agency, = are the CTO of a private company, an entrepreneur, a student or faculty member, the *[slowly, clearly]* **Institute for Information Security and Privacy** is where you can *[upbeat, strong]* **ambitiously explore new solutions with Georgia Tech**. We invite you to learn more about our work throughout the day, to **think critically with us** to discover and **solve the grand challenges of cybersecurity**.

We have a great program today. Let's begin…

[if needed] Again – I'll remind you that we have a crowded Auditorium today. There is overflow seating next door with a live video stream. If you are a Georgia Tech or GTRI employee, please offer your seat to a guest. Thank you.

We're excited to present to you **a keynote this morning, delivered by Stewart A. Baker.**

Mr. Baker is a partner in the Washington office of Steptoe & Johnson LLP. He returned to the firm following 3½ years at the Department of Homeland Security as its first Assistant Secretary for Policy. At DHS, Mr. Baker created and staffed the DHS Policy Directorate and was responsible for policy analysis, as well as for the Department's international affairs, strategic planning and relationships with law enforcement and public advisory committees. He led successful negotiations with European and Middle Eastern governments over travel data, privacy, visa waiver and related issues. He devised a new approach to visa-free travel, forged congressional and interagency consensus and negotiated acceptance with key governments. Mr. Baker managed one of the nation's premier technology law practices at Steptoe before accepting the DHS post. His practice includes issues relating to government regulation of international trade in high-technology products; the antidumping and countervailing duty laws of United States, European Union, Canada, and Australia; foreign sovereign immunity, and compliance with the Foreign Corrupt Practices Act. Mr. Baker has handled the arbitration of claims exceeding $1 Billion dollars, and has had a number of significant successes in appellate litigation and appearances before the United States Supreme Court.

Please welcome Mr. Stewart A. Baker.

IV. **Keynote Stewart Baker**

9:15 – 10 a.m.

V. **Post-Keynote Interlude Michael Farrell**

[post keynote…]

~10:00 a.m.

Thank you, Stewart, for a riveting presentation. There's certainly more to discuss. We're going to take a **10-minute break** and return right here to this Auditorium at **10:15 a.m.** for a panel discussion with Stewart and representatives from Microsoft, the Council on Foreign Relations, FBI, and members of the media. Stay close.

VI. ***Panel*** **Stewart Baker**

Intro by Michael Farrell

10:15 a.m.

May I have the room's attention please? *[pause, repeat as needed]*

Welcome back. We're about to begin the next portion of our morning – a panel discussion. We know you have burning questions based on what you heard Stewart share moments ago.

Have Advocates of Attribution Really Won? And what does that mean for the future of cybersecurity policy?

Joining us for the discussion this morning are:

Cristin Flynn Goodwin.

Ms. Goodwin is the Assistant General Counsel for Cybersecurity and Digital Trust at Microsoft. She has been Microsoft's lead counsel for the Microsoft Security Response Center (MSRC), and since 2015 has specialized in adversary incidents, helping protect over a billion customers around the world. She also provides counsel to the Microsoft Threat Intelligence Center (MSTIC) on operational issues. Cristin also advises on a range of cybersecurity and cybercrime policy issues, and provides legal counsel to Microsoft's Government Security Program (GSP) which provides governments with a structured, legal means to access source code and affirm there are no back doors in Microsoft products or services, as well as to share information about threats and vulnerabilities.

Cristin joined Microsoft in 2006, where she initially served as policy counsel in Microsoft's Washington, DC office. Prior to joining Microsoft, Cristin worked for several telecommunications companies. She began her career as a trial lawyer in New York City. **Please welcome Ms. Cristin Goodwin.**

Chad Hunt.

Chad Hunt leads the computer intrusion squad for the Federal Bureau of Investigation in Atlanta. Mr. Hunt entered duty as a special agend with the FBI in 2003. With over 10 years of experience investigating cybercrime, he brings in-depth knowledge to support the FBI Cyber Division's mission to identify, pursue, and defeat cyber adversaries. **Please welcome Agent Chad Hunt.**

Robert K. Knake.

Robert Knake is the Whitney Shepardson senior fellow at the Council on Foreign Relations. His work focuses on Internet governance, public-private partnerships, and cyber conflict. He previously served as director for cybersecurity policy at the National Security Council. A frequent writer and speaker on cybersecurity, he has been quoted by the *New York Times*, the *Wall Street Journal*, and the *Washington Post* and appeared on MSNBC, CNN, and National Public Radio. He has testified before Congress on the problem of attribution in cyberspace and written and lectured extensively on cybersecurity policy. Knake is an adjunct lecturer at Georgetown University's McCourt School of Public Policy and a senior advisor to the machine learning company Context Relevant. He holds a master's in public policy from Harvard's Kennedy School of Government and undergraduate degrees in history and government from Connecticut College and is a term member of the Council on Foreign Relations. **Please welcome Mr. Robert Knake.**

Hannah Kuchler.

Hannah Kuchler is a journalist, columnist and public speaker specialising in finance and technology. Since moving to San Francisco four years ago, she has specialised in writing about cyber security and social media. Her work makes important, complex cyber security stories accessible for a broad business audience. She reports on the threats facing companies and the security industry's potential solutions, coordinates the FT's cyber security special reports and chairs FT cyber security summits. **Please welcome Ms. Hannah Kuchler.**

Kim Zetter.

Kim Zetter is an award-winning investigative journalist and book author who has been covering computer security and the hacking underground since 1999, first for *PC World* magazine and more recently for WIRED, where she wrote about security, cybercrime, surveillance and civil liberties for more than a decade. She has broken numerous stories over the years about NSA surveillance, WikiLeaks, and the hacker underground and has three times been voted one of the top ten security journalists in the U.S. by her journalism peers and security industry professionals. She's considered one of the world's experts on Stuxnet, a virus/worm used to sabotage Iran's nuclear program, and published a highly-acclaimed book on the topic - *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. **Please welcome Ms. Kim Zetter.**

This will be an interactive panel, moderated by Stewart Baker. Feel free to ask questions at any time. We have two runners in the audience with microphones to the left and right of the room.

Additionally, this conversation will be recorded and edited for Stewart Baker's long-running podcast: the Steptoe Cyberblog. Cyberblog began in March 2012 and is well into its fifth year – covering topics that arise at the intersection of law, information technology, and security. Thank you, Stewart. Take it away.

VII. ***Post-Panel Interlude & Dismiss for Lunch*** **Michael Farrell**

12:15 p.m.

Let's give our panelists another round of applause!

We're now going to break for lunch. A delicious buffet is outside in the atrium and seating is available in the room next door. Georgia Tech kindly requests no food or drink in the Auditorium please. Those of you with reserved seats will find your tables down the hallway, across the lobby.

We'll resume here in the Auditorium at 1:30 p.m. Thank you.

VIII. ***Reconvene & EduTalks*** **Michael Farrell**

IX. *Key message: GT is advancing the science of Attribution.*

1:30 p.m.

Good afternoon! Welcome back! This morning, you heard from a range of experts about the **political, business, and human considerations** of cyber attribution. This afternoon, you're going to hear from Georgia Tech researchers about the **technical and legal solutions** we're creating now.

Attribution is a significant area of cybersecurity research at Georgia Tech and GTRI. Last fall, we were awarded a $17-million grant from the U.S. Department of Defense to **develop a methodology and the mechanics that will help you perform cyber attribution**. Our work is not to point fingers, but rather to create a plexi-glass funnel that anyone can pour their data into and analyze what comes out.

Some of the findings you'll hear about today are the result of our first year of work on that project. Additionally, we'll share results from projects funded by the U.S. Department of Commerce, National Science Foundation, and Air Force Research Laboratory. Peter Swire will share his research, supported by the Hewlett Foundation, Future of Privacy Forum, Microsoft and Facebook. Georgia Tech works closely with partners across the United States in every sector – public, private, government, military and non-profit – to create the solutions you can't find on a shelf.

Let's begin.

[exit stage and turn over to Manos, who will self-introduce…]

IX. ***Interlude, Plug for GTPE*** **Michael Farrell**

3:00 p.m.

Thank you, Chaz.

You've just heard three presentations about **ideas developed right here at Georgia Tech**. It's our goal to move these ideas out to market, into the hands of the public, where they can serve you. You can license our I.P. to continue the research or apply our results to your own products and projects. Any of us today wearing a GT lapel pin would be happy to talk further with you about that.

It's also our goal to **educate you** about cybersecurity. If you were intrigued by what you heard today and find yourself wanting to know more, take a look at **Georgia Tech Professional Education**. Working professionals can advance their understanding through 10 short courses we offer. Working adults can earn a certificate in cybersecurity without leaving their day jobs. These courses are beneficial for the C-suite decision makers, project managers, network defenders, or anyone in your organization who wants to gain a wider perspective. These courses are not just for the IT department; They are useful for every function – HR, Marketing, Legal, Contracting and IT. Our students are excited to learn from the same Georgia Tech faculty and scientists on the front-lines of our cybersecurity research every day, and our students give us a more than a 90% approval rating. Information is out in the lobby if you'd like to know more.

Next, we're going to take a 30-minute break for networking and, during that time, you can meet our students who are also in the lobby. **Georgia Tech students have brought examples of the cybersecurity solutions they are working on right now**, and they'd love to tell you more about them. In fact, we're asking you to **vote for your favorite ideas** as students compete for $125,000 in prizes that will help them continue their work. So, your vote matters. It could help someone move their idea to market or fund additional research! Please give their projects a hearty review and challenge them with your questions.

At 3:30 p.m., our breakout sessions will begin. Refer to your program. David Dagon will be digging deeper into profiles of attackers. David Formby will be sharing solutions to catch malware on the energy grid and industrial systems. Our associate directors of cybersecurity research will be in the atrium for the rest of the afternoon if you'd like to personally discuss a cybersecurity problem. Thank you and enjoy what we have outside. ….

[Michael – at this point, the crowd breaks. No further remarks are needed until 4:30 p.m. when you and Wenke can tag-team intro & closing comments at each breakout session. See pg. 1.]