

Topics in Computer Security Series – Sept. 2019

ISC2 San Diego Chapter

Board Introduction
<https://isc2-san-diego-chapter.org/board/>



O'Dell Hobson
President



Nelson Mozzini
Vice President & Treasurer



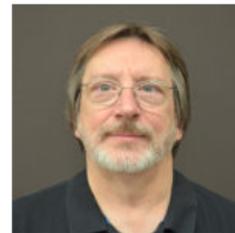
Christine Muzquiz
Secretary



Jonathan Gerard
Membership Chair



Claudia Judge
Recorder



Gerard (Gerry) Sieracki
Director of Public Relations



Lynn Hajar Hoffman
Director of Training & Education

Topics in Computer Security

- Each Member...
 - Should keep up to date with latest in computer security news
 - Has experience and expertise to Offer
 - Should benefit from meetings via networking, communication, and exchange of ideas

Topics in Computer Security

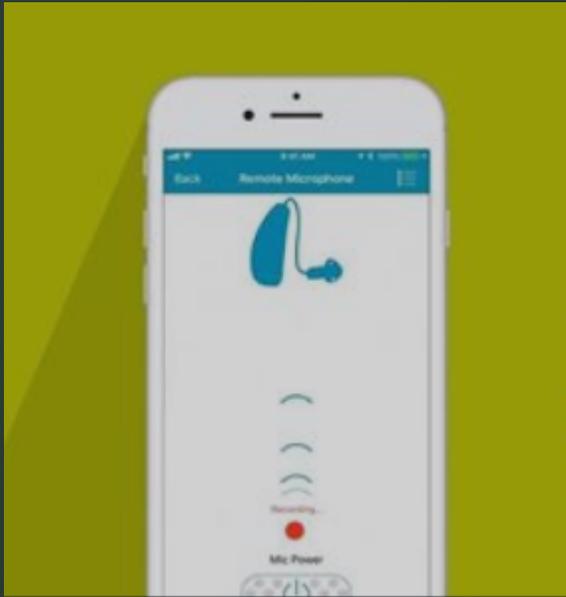
- Some Guidelines...
 - There's no set number of topics we must get through, though meetings generally go until 8pm (and beyond)
 - This is a trial run, so feedback is encouraged! (Shall we do this again?)



Hearing Aids



▶ Hearing Aids Can Now Record
<https://www.starkey.com/blog/2018/06/How-to-record-conversations-with-hearing-aids>



- “Cool” features become Security Concerns
- The examples given on their website include visiting a doctor’s office
- This is an example of a product that might get “past the door” where other recording devices would not.



Electrical Grid Vulnerabilities



US Grid CyberAttack – March 5 Analysis
<https://www.eenews.net/stories/1061111289>

- A vulnerability in the web interface of a vendor's firewall was exploited, allowing an unauthenticated attacker to cause unexpected reboots of the devices. This resulted in a denial of service (DoS)¹ condition at a low-impact control center and multiple remote low-impact generation sites. These unexpected reboots resulted in brief communications outages (i.e., less than five minutes) between field devices at sites and between the sites and the control center.

US Grid CyberAttack – March 5 Analysis
<https://www.eenews.net/stories/1061111289>

- “The more recent cyberthreat appears to have been simpler and far less dangerous than the hacks in Ukraine. The March 5 attack hit web portals for firewalls in use at the undisclosed utility. The hacker or hackers may not have even realized that the online interface was linked to parts of the power grid in California, Utah and Wyoming.”



DOD File Sharing Vulnerability

ARMY File Sharing Site Shutdown

<https://www.fifthdomain.com/dod/army/2019/08/29/how-one-teenager-took-out-a-secure-pentagon-file-sharing-site/>

- On Oct. 25, Jack Cable, who worked for the Defense Digital Service and was a freshman at Stanford University, reported a problem to the department through the Pentagon's HackerOne vulnerability disclosure page.
- At age 17, he found 30 vulnerabilities in Air Force websites during the 2017 rendition of the "Hack the Air Force" competition. He ended up winning the contest.

Jack Cable at the “Future of Everything” Conference



Current Site & How the Exploit Worked

/verify.php#

UNCLASSIFIED//FOUO USE ONLY

 **DoD SAFE** Logged on as user: **GERARDJONATHAN.E**

[Home](#) [Drop-Off](#) [Request a Drop-Off](#) [Pick-up](#) [Outbox](#) [Help](#) [Logout](#)

PLEASE NOTE

NO CLASSIFIED INFORMATION IS ALLOWED ON DOD SAFE

Any files containing PII/PHI **must** be encrypted prior to upload.

Uploaded files are scanned for viruses.

Uploading...

Uploaded: 57%

This web page will allow you to drop-off (upload) one or more files for anyone (either a DoD user or others). The recipient will receive an automated email containing the information you enter below and instructions for downloading the file.

From:
GERARDJONATHAN.E <jonathan.gerard@navy.mil> USN

To:


Short note to the Recipients:

Encrypt every file (REQUIRED FOR PII/PHI)
 Send me an email when each recipient picks up the files

1000 / 1000 left



YouTube Settlement for Children's Privacy

Children's Online Privacy Protection Act

- The act, effective April 21, 2000, applies to the online collection of personal information by persons or entities under U.S. jurisdiction about children under 13 years of age including children outside the U.S., if the company is U.S.-based.
- Details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online including restrictions on the marketing of those under 13.

Google To Pay \$170 Million To Settle FTC Claims That YouTube Collected Kids Data Illegally

- The fine is a record in a case related to alleged violations of the Children's Online Privacy Protection Act (COPPA), according to the FTC. "YouTube touted its popularity with children to prospective corporate clients," said FTC Chairman Joe Simons. "Yet when it came to complying with COPPA, the company refused to acknowledge that portions of its platform were clearly directed to kids. There's no excuse for YouTube's violations of the law."
- Under the settlement, YouTube is required to develop and maintain a system that lets channel owners to identify "child-directed content" so that YouTube can ensure it is complying with COPPA. In addition, Google and YouTube must notify channel owners that their child-directed content may be subject to COPPA's obligations and provide annual training about complying with COPPA for employees who deal with YouTube channel owners.

▶ YouTube vowed to halt comments on videos with kids (in March). It still hasn't.

<https://www.cnet.com/news/youtube-kids-videos-still-allow-comments-machine-learning-ai-failing-to-suspend-disable/>

- Six months later, CNET's single search found more than 100 videos posted in the last month by more than 100 different channels. They all featured young children -- babies, toddlers and kids clearly no older than elementary school students. All had comments enabled.

Platform vs Publisher

- **Platform**
 - Open “public” space for discussion
 - So much data, that it couldn’t possibly be analyzed
 - YouTube: 60 hours of video uploaded per minute
 - May have generic, broad rules of enforcement
- **Publisher**
 - Cultivates content
 - May have arbitrary rules for which content is allowed
 - A publisher may be liable for the content which remains present



Scraping Other's Collected Data

Web scraping doesn't violate anti-hacking law, appeals court rules
<https://arstechnica.com/tech-policy/2019/09/web-scraping-doesnt-violate-anti-hacking-law-appeals-court-rules/>

- Scraping a public website without the approval of the website's owner isn't a violation of the Computer Fraud and Abuse Act, an appeals court ruled on Monday. The ruling comes in a legal battle that pits Microsoft-owned LinkedIn against a small data-analytics company called hiQ Labs.



Hong Kong Protestors Find Ways to Communicate

▲ Hong Kong Protestors Using Bluetooth Mesh Messaging App (Bridgefy)

<https://www.forbes.com/sites/johnkoetsier/2019/09/02/hong-kong-protestors-using-mesh-messaging-app-china-cant-block-usage-up-3685>

The screenshot shows the BBC News website interface. At the top, there is a navigation bar with the BBC logo, a 'Sign in' button, and various news categories: News, Sport, Reel, Worklife, Travel, Future, Culture, Music, TV, Weather, and Sounds. A search bar is located on the right. Below the navigation bar is a red banner with the word 'NEWS' in white. Underneath the banner is a secondary navigation bar with links for Home, Video, World, US & Canada, UK, Business, Tech, Science, Stories, Entertainment & Arts, Health, In Pictures, Reality Check, World News TV, and More. The 'World' section is active, and 'China' is selected under the 'Asia' category. The main content area features a 'NOW PLAYING' video player with a 'UP NEXT' section. The 'UP NEXT' section contains seven video thumbnails with titles and dates:

- Hong Kong protesters call for US intervention** (08 Sep)
- BBC reporter hit in the face during HK protest** (05 Aug)
- People beaten on Hong Kong metro by police** (01 Sep)
- Hong Kong protests: Students rally in their thousands** (02 Sep)
- How Hong Kong got trapped in a cycle of violence** (17 Aug)
- Violence erupts in HK train stations** (12 Aug)
- Police officer points gun at Hong Kong protesters** (30 Jul)

Hong Kong Protestors Use Bridgefy to Avoid Chinese Surveillance

- Hong Kong Protestors Using Mesh Messaging App China Can't Block: Usage Up 3685%
- The app can connect people via standard Bluetooth across an entire city, thanks to a mesh network. Chatting is speediest with people who are close, of course, within a hundred meters (330 feet), but you can also chat with people who are farther away. Your messages will simply "hop" via other Bridgefy users' phones until they find your intended target.

Equifax to pay at least \$575 million as part of FTC settlement

- Hackers stole the personal information -- including Social Security numbers and home addresses -- of nearly 148 million Americans from Equifax's servers in a data breach that ran from May to July in 2017.
- A December 2018 House Oversight Committee report called the breach "entirely preventable," saying Equifax didn't take action to prevent it and wasn't prepared for the aftermath.
- You were probably affected.
- As a security expert, you may have more claim to money than others do...



Equifax Settlement



<https://www.equifaxbreachsettlement.com/>

https://www.equifaxbreachsettlement.com

EQUIFAX DATA BREACH SETTLEMENT

[Home](#) [Key Dates](#) [Important Documents](#) [FAQs](#) [I Would Like To... ▾](#)

Welcome To The Equifax Data Breach Settlement Website

In September of 2017, Equifax announced it experienced a data breach, which impacted the personal information of approximately 147 million people. A federal court is considering a proposed class action settlement submitted on July 22, 2019, that, if approved by the Court, would resolve lawsuits brought by consumers after the data breach. Equifax denies any wrongdoing, and no judgment or finding of wrongdoing has been made.

[FILE A CLAIM TODAY](#)

A recent change may mean less money and the requirement to prove monitoring

lement.com/en/amendclaim

EQUIFAX DATA BREACH SETTLEMENT

[Key Dates](#) [Important Documents](#) [FAQs](#) [I Would Like To... ▾](#)

Validate or Amend Your Claim: Alternative Compensation Cash Payment or Credit Monitoring

Did you file a claim on or before August 2, 2019 to receive "alternative compensation cash payment" of up to \$125 from the consumer restitution fund established to settle the Equifax class action lawsuit related to the 2017 data breach? If so, you can use this online form to (1) provide the name of the credit monitoring service you had when you filed your claim so that your claim can be considered or (2) amend your claim to request credit monitoring instead of the alternative compensation cash payment option.

Please note the amount you receive in connection with your alternative compensation cash payment claim may be significantly reduced depending on how many valid claims are ultimately submitted by other class members for this relief.

Please enter your claim number below to get started. If you recently received an email from the settlement administrator, you can find your claim number at the top of that email. If you cannot find your claim number, you can contact the settlement administrator by clicking [here](#).

Claim Number:

You must take action in order for your claim to be considered. Please note that you only have until October 15, 2019, to validate or amend your claim if you already filed one or your claim for the alternative compensation cash payment will be denied.

[NEXT](#)



Deepfakes and AI Implications



▲ Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

<https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>

- Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 (\$243,000) in March in what cybercrime experts described as an unusual case of artificial intelligence being used in hacking.
- Phishing attacks can now become more effective...



Ransomware



New Bedford Hit With \$5.3m Ransomware Demand

<https://www.infosecurity-magazine.com/news/new-bedford-hit-with-53m/>

- A Massachusetts city has revealed that cyber-criminals tried to hold its data ransom to the tune of more than \$5m over the summer, in a sign of the growing risk to organizations from online extortionists.
- The hackers wanted \$5.3m in Bitcoin, a figure he countered with a much lower sum of \$400,000 as this apparently would have been covered by cyber insurance.
- The attackers rejected that sum outright, highlighting just how high the bar is now for victims of ransomware attacks. In New Bedford's case the relatively small number of machines affected meant restoring from back-up was pretty straightforward and no critical systems were impacted.



Mayors Unite Against Ransoms

<https://www.infosecurity-magazine.com/infosec/as-mayors-unite-against-ransoms/>

- 170 cities have now been impacted
- A survey found 40% of IT Pros believe ransomware should be illegal
- Resolutions by a group of city mayors has pledged to not pay ransomware at 87th Annual US Conference of Mayors (USCM). This includes Mayor Faulconer of San Diego.
- Paying is common. Most cyber insurance groups simply pay up.



Cloud vs OnSite Security



▀ CISOs: Cloud is Now Safer Than On-Premises

<https://www.infosecurity-magazine.com/news/cisos-cloud-is-now-safer-than/>

- The perception of cloud security appears to have reached a tipping point, with a majority of cybersecurity leaders now believing the risk of a breach is the same or lower than in on-premises environments, according to [Nominet](#).
- However, concerns persist: 71% were moderately, very or extremely concerned about malicious activity in the cloud. Over half (56%) cited regulatory fines as their biggest concern, whilst a similar number (54%) pointed to the increasing sophistication of cyber-criminals.
- Multiple Vendors Increases Footprint
- Offloading to cloud may reduce liability\ransomware likelihood



Questions? Comments? Feedback?

Upcoming Events

October 10

Rahul Raghavan

Co-Founder and Chief Evangelist, we45

Topic: AWS Security



November 14

Matt Bossom

Presidio, Inc.

Topic: Security Strategy for Today's
Expanded Attack Surface



December 12

Chris Newborn & Paul Shaw

Defense Acquisition University

