

Cyber@UC Meeting 53

Cross-Site Request Forgery

If You're New!

- Join our Slack: ucyber.slack.com
- **SIGN IN!** (*Slackbot will post the link in #general*)
- Feel free to get involved with one of our committees:
Content Finance Public Affairs Outreach Recruitment
- Ongoing Projects:
 - Malware Sandboxing Lab
 - Cyber Range
 - RAPIDS Cyber Op Center



Announcements

- More workstations arrived in the lab!
- **Dr. Sylvertooth** wants to talk to us! (**DHS Cybersecurity SME**)
 - <https://www.linkedin.com/in/dr-randall-e-sylvertooth-55b35b47>
 - We need a date for him to talk to us.
- **UC Open House** for our **Lab and Cyber Range** **May 29th 9am**
- Partnership with **Galois** in the works...still....



Public Affairs

Useful videos and weekly livestreams on **YouTube**:

youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us for club updates and cybersecurity news:

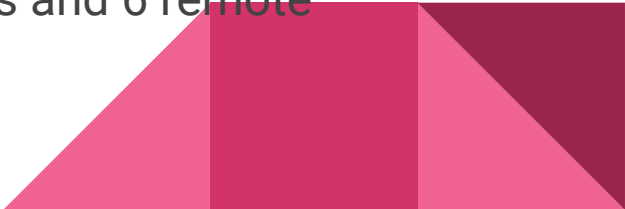
- **Twitter:** [@CyberAtUC](https://twitter.com/CyberAtUC)
- **Facebook:** [@CyberAtUC](https://facebook.com/CyberAtUC)
- **Instagram:** [@CyberAtUC](https://instagram.com/CyberAtUC)

For more info: cyberatuc.org




Weekly Content

Vuln Report on BMW Cars

- Keen Security Lab conducted a year long security audit on BMW cars
 - Same company that found some of Tesla's vulns
 - Found 14 different vulnerabilities
 - Published a technical report of their findings
 - left out some technical details until next year, when BMW is expected to be 100% patched
 - Focused on 3 areas: Infotainment, Telematics Control, and Gateway Module
 - 8 infotainment for music and media
 - 4 TCU for controlling of accident assistance services and locking/unlocking of doors
 - 2 flaws in CGM for diagnostics of the other two systems and transfer on CAN buses
 - 4 flaws require usb, 4 require indirect physical access and 6 remote
 - Vulns allow attackers to take complete control
- 

Spectre Variant 4

- Found by Microsoft and Google
 - Dubbed Speculative Store Bypass
 - Speculative Execution: processor makes a guess and operates based on that assumption, continues if right, discards if wrong
 - Unlike Meltdown, variant 4 is expected to affect Intel, AMD, IBM, and ARM
 - This means almost all devices: laptops, PCs, smartphones, tablets, embedded devices
 - Classified as medium risk, so far demonstrated in “language-based runtime environment” like JavaScript but mitigated by most browsers
 - BIOS updates are coming
 - Mitigations expected to cause a performance hit: off by default
 - 2-8% performance hit on intel
- 

How Secure Is Your City?

- Coronet, a cloud security vendor, conducted an analysis of the 55 most populated areas in the US
- Risk level is a scale of 0-10, 10 being grandparent level security
- 6.5 or less is considered acceptable
- Here are a few cities:
 - Las Vegas:10, Memphis:9.8, Charlotte:9.8, Houston:9.2, Providence:9.0, Birmingham:9.0, Jacksonville:8.9, West Palm Beach:8.9, Orlando-Daytona Beach:8.5, Tampa:8.3
 - Richmond:5.8, Greensboro:6.2, Norfolk:6.2, Seattle:6.3, St. Louis:6.3
- In Vegas: 43% chance of connecting to a high or medium risk network
 - 20% of devices don't have password protection




ZipperDown


- Named by Pangu Lab
- Caused by a common programming error, estimate 10% of IOS apps are vulnerable, also on Android as found since article was written
- Attacker must control WiFi network of the device and the app must be running outside the IOS sandbox
- The could allow an attacker to run applications on the device
- Technical details have not been released
 - Suspected to be a path traversal issue in ZipArchive utility



#Dont\$hareTheWhere

- Our phones constantly give our approximate location to our mobile provider
 - Necessary for call quality and 911 location sharing
 - Major mobile providers in the US: AT&T, Sprint, T-Mobile, and Verizon are selling this location info to third parties in real time
 - Without Consent
 - Without Court Order
 - Seemingly no accountability on how the data is used, stored, shared, or protected
 - Only way to stop this is remove the SIM card and never put it back in
 - Data-broker Securus was selling the ability to look up the precise location of any cell phone, then Securus was hacked
- 

T-Mobile SIM Swap

- An attacker scammed a T-Mobile employee into doing a SIM swap to allow the attacker access to a customer's phone data and the ability to gain access to the victim's Instagram
 - The attacker's goal was to acquire the victim's Instagram account name "par",
 - apparently there is a business of selling short account names
 - The victim never actually received a notification from T-Mobile about the SIM swap, which is what allowed this theft to occur
 - T-Mobile's current policy is to send a text to the new phone after the swap occurs, because that is very useful
- 

Cross-Site Request Forgery

What is CSRF?

- Attack where a hacker makes fraudulent requests on behalf of a user
- Completely silent; happens just by a user visiting a malicious site
 - Works even with JS disabled in some cases
- OWASP Top Ten rank
 - #5 in 2007
 - #5 in 2010
 - #8 in 2013
 - unranked in 2017



Who's been hit?

- YouTube in 2008 was vulnerable for all sorts of actions
- ING Direct was vulnerable for **money transfers**. Not kidding.
- Others: Netflix, McAfee, Facebook
 - Links will be on cyberatuc.org meeting page



Web forms

- User fills out fields and clicks submit button
- Via JS or <form> tag, a request is made
 - GET or POST
 - Includes cookies and whatnot



CSRF

- Sequence
 - User is logged into VulnSite
 - User visits EvilSite
 - EvilSite makes a request to VulnSite
 - VulnSite honors the request
- Can be executed with img tags, script tags, etc; or with Ajax
- What the developers did wrong?
 - HTTP requests are not privileged



Demo time!

- Mock bank website: unsafe.schiff.io/csrf-demo
- Objective: Make a website that, when anyone visits it, will transfer their money to your account.



Wrap-up

- Prevention: **Use CSRF tokens**
 - Requests aren't privileged, but responses are
 - Built into most web frameworks
- Any questions? :)

