Cyber@UC Meeting 66

Welcome New Members!

If You’re New!

- Join our Slack: **ucyber.slack.com**
- **SIGN IN!** *(Slackbot will post the link in #general at 6:30)*
- Feel free to get involved with one of our committees:

  Content *Finance* *Public Affairs* *Outreach* *Recruitment*
- Ongoing Projects:
  - RAPIDS Lab!
  - NSA Cyber Operations Competition Research

Lab updates

- We have **desks**!!
- Next steps
  - Setting up iDRAC
  - Flashing CentOS
  - Setting up servers with OpenStack, FOG, and Puppet

More info at cyberatuc.org/blog

Other announcements

- **Board Game Night!**
  - This Friday @ 6pm, 649 Baldwin
- Planned visits
  - NSA visit with **Enigma Machine** (Sept 18)
  - **US Bank** visit planned for (week of Sept 24)
- Opportunities
  - **Air Force Research Lab Partnership**
    NSA Scholarship Opportunities!
  - **NSA Research Grant** in Cyber Operations
  - **Blackpoint Cyber** SOC Analyst Job applications! (thanks Mike!)
- Our **logo** has made progress! DAAP may help too.

Public Affairs

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

youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

(or just search for "cyber@uc")

Follow us for club updates and cybersecurity news:

- **Twitter:** @CyberAtUC
- **Facebook:** @CyberAtUC
- **Instagram:** @CyberAtUC

For more info: cyberatuc.org

Weekly Content

WannaCry

- Ransomware Cryptoworm
- Targeted computers running Microsoft Windows
- Propogated through EternalBlue
  - Exploit developed by the NSA, leaked by “Shadow Brokers” hacker group
  - Also used in the notPetya cyberattack
  - Mishandling of Server Message Block (SMB) protocol allowed arbitrary code execution
  - Patches were available two months before WannaCry attack occurred
- > 200k computers across 150 countries
- Attack believed to have come from North Korea

Equifax

- Equifax fails to patch Apache Struts on one of their servers
- September 7, 2017 Equifax announces a breach > 140M americans data leaked, >200k credit card numbers
- Equifax discovered the breach July 29, then hired a forensics firm
- Equifax had a terrible response
  - Website telling people if they were affected gave differing responses
  - Website allowing enrollment in identity protection couldn't handle traffic and was constantly down
  - That same page also had cert errors
  - Wrong link in Twitter
- Cost Americans an estimated 1.4 B in credit freeze fees

Blueborne

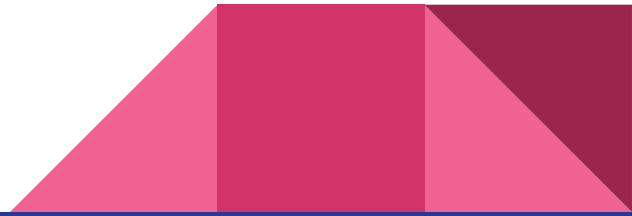
- Discovered by Armis
- Airborne and spreads via bluetooth
- Utilized 8 new zero-day vulnerabilities
- Could have allowed attackers to take control of devices, access corporate networks and penetrate air-gapped networks
- Android, iOS, Windows, and Linux were all vulnerable
- Does not require being paired to the devices or for the victim device to be discoverable
- Exploits the high level privileges bluetooth inherently recieves on all OSs
- Estimated > 8.2 billion vulnerable devices at discovery

Blueborne (continued)

- No victim interaction required
- Allows both C&C and MiTM
- Attack Stages:
  - Locate active Bluetooth devices
  - Obtain the device’s MAC address
  - Run an exploit for the proper OS

Spectre/Meltdown

- Vulnerability caused by flaws in speculative execution
- Processor recognizes patterns and attempts to make predictions on results of processes and operates on those before results come in
- Discarded computation is stored in unsecured memory
- Patches have been developed but cause slow downs
    - Can’t be avoided until new architecture and system designs are developed



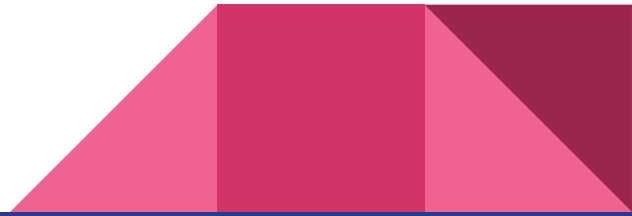
Cross Site Scripting (XSS)

What is XSS?

- Attacker writes malicious code, makes a website serve it to other visitors
- Exists b/c the web wasn't originally interactive
- Reflected & Persistent (demo)
- The fix: input sanitization
  - Change... `<script>doEvilThings("yes");</script>`
    to... `&lt;script&gt;doEvilThings(&quot;yes&quot;);&lt;/script&gt;`

Notable examples

- Self-retweeting tweet
- "but most of all, samy is my hero"
- Banks doing the Harlem shake
- Many, many more
  - See list on schiff.io/talks/xss



Interactive demo

Try to hack my website! **bit.ly/haydenxssregister**

Goal: Change the XSS Champion from "no one" to your name.

(please refrain from completely annihilating the page -- don't ruin the demo for the rest of us!)

Further info

This was a short version of a presentation I gave last spring.

Full slides and video at schiff.io/talks/xss