

Cyber@UC Meeting 63

Contributing to the Website

If You're New!

- Join our Slack: ucyber.slack.com
- **SIGN IN!** (*Slackbot will post the link in #general every Wed@6:30*)
- Feel free to get involved with one of our committees:
Content Finance Public Affairs Outreach Recruitment
- Ongoing Projects:
 - RAPIDS Lab!



Announcements

- Our desktop PCs are now dwarves
- We will have a table at **FELD Fest** and **UC Mainstreet** event
- We've been asked to **give a lecture** this Fall semester
- Lab server room should be cleaned by **next Tuesday**
- **CiNPA Security Meetup** next Thursday
 - Physical Security Night
 - [225 Pictoria Drive, Springdale, Ohio 45246](#)
 - 6:30pm



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

Drupal Symfony Flaw

- Vulnerability in Symfony HttpFoundation makes Drupal 8 vulnerable to
- Symfony is a popular web app framework
- Vulnerability rises from legacy and risky HTTP headers
- 'X-Original-URL' and 'X-Rewrite-URL' HTTP headers allowed for potential bypass of access restrictions
- Both Symfony and Drupal have released patches
- Similar vulnerabilities found in Zend Feed and Diactoros libraries

<https://thehackernews.com/2018/08/symfony-drupal-hack.html>



Facebook Fizz

- Library designed for helping developers implement TLS 1.3 protocol with all security and performance configurations
- Article includes some descriptions on what TLS is and benefits of 1.3
- Now open source on GitHub, link in the article
- Transfers data securely at 10% faster speeds

<https://thehackernews.com/2018/08/fizz-tls-ssl-library.html>



WhatsApp Vulnerabilities

- Discovered by Israeli security firm CheckPoint
- Exploits vulnerability in WhatsApp's security protocols to change message content
- Flaw in mobile app connection to WhatsApp web and decryption of end-to-end messages using protobuf2 protocol
- Can only be exploited by a user already a part of the group conversation
- Attack types:
 - Change correspondent's replay, change sender identity, and send private message with public replies
- WhatsApp has decided that this is insignificant and decided not to patch

<https://thehackernews.com/2018/08/whatsapp-modify-chat-messages.html>

New Method of Hacking WPA/WPA2

- Discovered by Jens 'Atom' Steube, lead developer of hashcat tool
- Relies on using PMKID, Pairwise Master Key Identifier, to get Pre-shared key, PSK
- Previous WPA hacks have relied on waiting for a user to login, this method does not
- Discovered when reviewing WPA3 security standard
- Using a tool, like hcxdumptool, PMKID is requested and dumped as a pcap
- The pcap is then made into a hashformat acceptable by hashcat
- Use Hashcat to obtain WPA PSK password

<https://thehackernews.com/2018/08/how-to-hack-wifi-password.html>

Recommended Reading

<https://www.welivesecurity.com/2018/07/26/fake-banking-apps-google-play-leak-stolen-credit-card-data/>

<https://krebsonsecurity.com/2018/08/reddit-breach-highlights-limits-of-sms-based-authentication/>

<https://www.welivesecurity.com/2018/08/02/reddit-reveals-breach-staffs-2fa/>

<https://thehackernews.com/2018/08/ccleaner-software-download.html>

<https://thehackernews.com/2018/08/android-9-pie.html>



Recommended Reading (continued)

<https://thehackernews.com/2018/08/snapchat-hack-source-code.html>

<https://krebsonsecurity.com/2018/08/florida-man-arrested-in-sim-swap-conspiracy/>

<https://krebsonsecurity.com/2018/08/credit-card-issuer-tcm-bank-leaked-application-data-for-16-months/>

<https://thehackernews.com/2018/08/fin7-carbanak-cobalt-hackers.html>

<https://thehackernews.com/2018/08/mikrotik-router-hacking.html>



Recommended Reading (Apple WannaCry)

<https://www.welivesecurity.com/2018/08/07/apple-chip-wannacryptor-shutdowns/>

<https://thehackernews.com/2018/08/tsmc-iphone-computer-virus.html>

<https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html>





Contributing to the website

Getting started

- Make a GitLab account
 - gitlab.com
- Request org access
 - gitlab.com/cyberatuc
- Install dependencies and clone the repo
 - gitlab.com/cyberatuc/cyberatuc.org#readme
- **Hayden's master guide: cyberatuc.org/guides/website**
- Jekyll docs: jekyllrb.com

