UNIVERSITY OF NORTH CAROLINA CHARLOTTE | COLLEGE OF COMPUTING AND INFORMATICS

NSF-DGE # 1947295

SaTC:EDU: Enhancing Security Education in Hybrid Mobile and Internet of Things Firmware through Inclusive, Engaging, Learning Modules (E-SHIIELD)

Meera Sridhar (msridhar@uncc.edu) and Harini Ramaprasad (hramapra@uncc.edu)
University of North Carolina at Charlotte

Project Goals

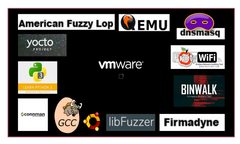
Intellectual Merit Goals

Stackable course modules

Hybrid Mobile App
- Intro to Hybrid Mobile App Dev Using Cordova Android
- Security mobile platform comparison
- Basic Hybrid Mobile App Security
- XSS
- Touchjacking
- App-repackaging
- Secure Coding Practices

IoT Firmware
- Intro to IoT Security
- Basics
- Emulation
- Analysis
- Vulnerability Detection
- Exploitation (w/o memory protections)
- Exploitation (w/ memory protections)

Virtual Lab support



Engaged & Inclusive pedagogy

- Accessible & engaging content delivery
- Active & interactive learning
- Forcing functions to ensure student prep
- Interactive quizzes
- Hands-on activities
- Gamification

NSA/DHS CAE Integration

Evaluation

Broader Impact Goals

K – 12 IoT Roadshow

UNCC SmartHome Lab

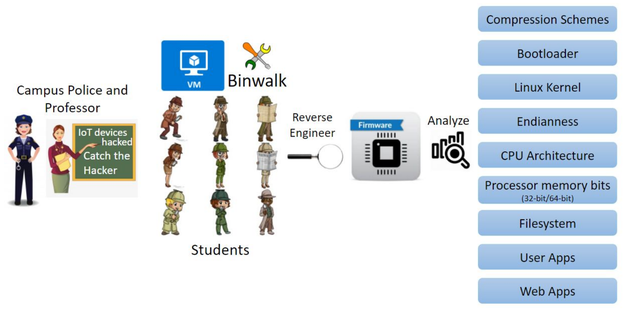
NC Universities and Community Colleges
- Faculty Mobile/IoT security training
- Integrate into NSA/DHS CAE-CD curricula
- Educational workshops
- Research demonstrations

Criminal Investigations

An interactive, gamified web-based framework to teach and assess cybersecurity skills in an engaging, inclusive manner

Features
- Compelling narrative
- Just-in-time learning content delivery
- Knowledge checkpoints to assess student preparation
- Hands-on tasks / activities
- Rewards such as eXperience Points (XP) to motivate students
- Practice and test modes to ensure students have a chance to master content before being assessed

Prototype activity: Reverse Engineering and Analyzing IoT Firmware



- Task: Reverse engineer an IoT firmware image using binwalk & identify firmware components (e.g., compression schemes, kernel, etc.)
- Narrative placing student as an assistant investigating a campus IoT hacking incident

- Abhinav Mohanty, Pooja Murarisetty, Ngoc Diep Nguyen, Julio Bahamon, Harini and Meera Sridhar. Criminal Investigations: An Interactive Experience to Improve Student Engagement and Achievement in Cybersecurity courses. Poster presented at the 52nd ACM Technical Symposium on Computer Science Education (SIGCSE'21), March 2021.
- Criminal Investigations: An Interactive Experience to Improve Student Engagement and Achievement in Cybersecurity courses. In Proceedings of the 53rd ACM Technical Symposium on Computer Science Education (SIGCSE'22), March 2022.

DISSAV: A Program Visualization Tool for Teaching Stack Smashing Attacks

DISSAV:
Dynamic Interactive Stack Smashing Attack Visualization

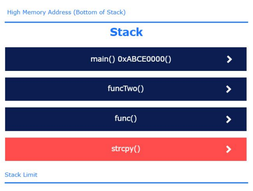
- Open-source, web-based application built in React.js
- Free to use for educational purposes

Guides students through a simulated attack in 3 phases:

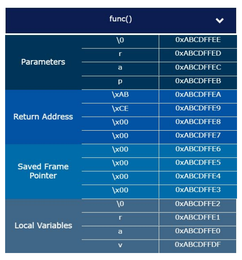
- Create a function with a buffer overflow vulnerability
- Construct a payload to pass to the vulnerable function
- Execute the program to attempt a stack smashing attack

Visualizations

Call Stack



Individual Stack Frames



Program Code

```
void funcOne(char p[]){
 char v[] = "v";
 strcpy(v, p);
}
```

7 numbered steps for guidance

Erik Akeyson, Harini Ramaprasad and Meera Sridhar. DISSAV: A Dynamic, Interactive Stack-Smashing Attack Visualization Tool. In Proceedings of the 25th Colloquium for Information Systems Security Education (CISSE'21), October 2021. **Best Paper Award**.

Guided Learning Activities

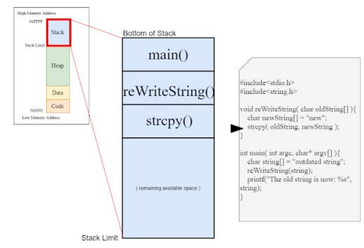
A sequence of guided-learning activities developed to teach concepts that relate to stack smashing attacks.

Introduction to C*
- Introduces C programming language
- Goal: Teach students how to create and run a C program that uses command-line arguments

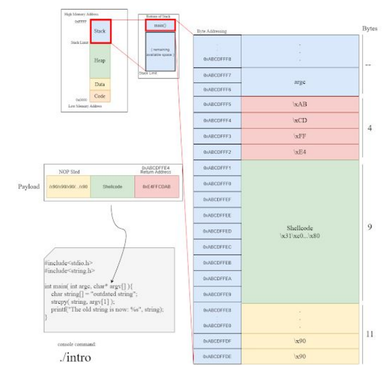
smallString

s	m	a	l	l	\0
0x5556	0x5557	0x5558	0x5559	0x555A	0x555B

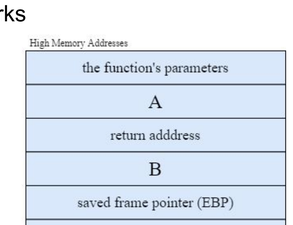
Process Memory Layout*
- Discusses how a computer handles and processes data in memory
- Goal: Have students understand the process memory allocation details



Stack Smashing
- Goal: Have students understand how to complete a stack smashing attack



Defenses
- Presents techniques to prevent stack smashing attacks
- Goal: Have students be able to explain how and why defenses works

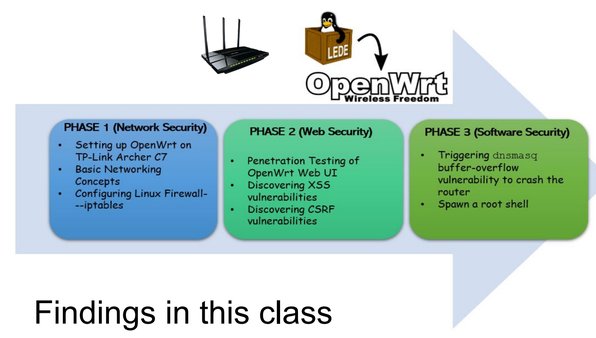


* Included as "Activity for Review" in Process-Oriented Guided Inquiry Learning (POGIL) Activity Clearinghouse

Class-sourced Penetration Testing

Goals
- Explore unconventional method of class-sourcing penetration testing of IoT devices
- Provide solid hands-on experience and access to cutting-edge technology

Flipped Classroom
- Pre-class preparation
- Hands-on activities and Interactive quizzes
- 6 weeks, hands-on experience with industry tools, working with real devices, trying to find 0-days in IoT devices
- Semester long project on Securing a SmartHome Router



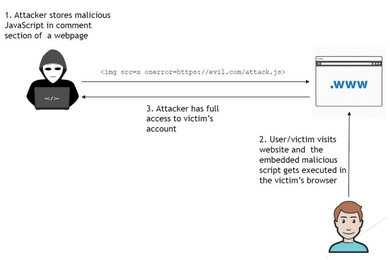
Findings in this class
- Two CVEs were reported:
  - CVE-2019-17367: Cross-site Request Forgery (CSRF)
  - CVE-2019-18992: Cross-site Scripting (XSS)

Abhinav Mohanty, Parag Mhatre and Meera Sridhar. Class-sourced Penetration Testing of IoT Devices. Poster presented at the IEEE Workshop on the Internet of Safe Things, 2020.

XSS Module

Course module to teach Cross-site Scripting in an interactive manner, with state-of-the-art tools

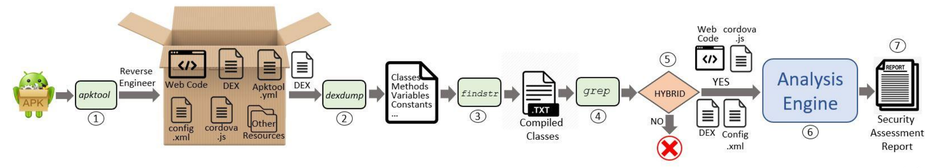
Module contents
- Short lecture video with demonstration of XSS attack
- Curated set of existing online learning resources (videos, readings, tutorials)
- Learning content quiz to ensure student preparation
- Pre- and post-surveys to assess knowledge before and after completing the module
- Hands-on activity where students identify an XSS vulnerable hybrid mobile application
- Final quiz to assess student learning



Deployment
- Introductory graduate course on Mobile IoT Firmware Security
- Junior level undergraduate course on Web-Based Application Design and Development

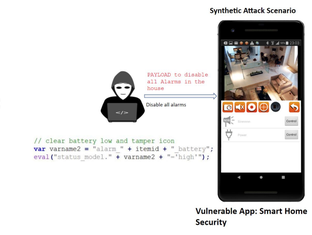
HybriDiagnostics

An automated framework to identify preexisting security issues in IoT companion apps developed for Android using hybrid mobile app development frameworks.



- Default, missing, or misconfigured Content Security Policy (CSP)

- Unsafe eval()



Abhinav Mohanty and Meera Sridhar. HybriDiagnostics: **An Automated Vulnerability Assessment Framework for Hybrid Smart Home Companion Apps.** In *IEEE Workshop on the Internet of Safe Things*. 2021.

Abhinav Mohanty and Meera Sridhar. **Poster: Security Evaluation of SmartHome Companion Web-based Mobile Apps**. Poster presented at *Annual Computer Security Applications Conference (ACSAC)*, December2020.