

Cybersecurity Education with Generative AI: Creating Interactive Labs from Microelectronic Fundamentals to IoT Security Exploitation

Authors: Kushal Badal, Xiaohong Yuan, Huirong Fu, Darrin Hanna, Jason Gorski

The Cybersecurity Education Challenge

months per lab module

Materials obsolete by deployment

High expertise & infrastructure costs

Technology outpaces curriculum

Traditional development cannot keep pace with evolving threats

Our Solution - The Breakthrough

MONTHS → **21 DAYS**

AI

Claude AI Opus 4

15,247

lines of code

40

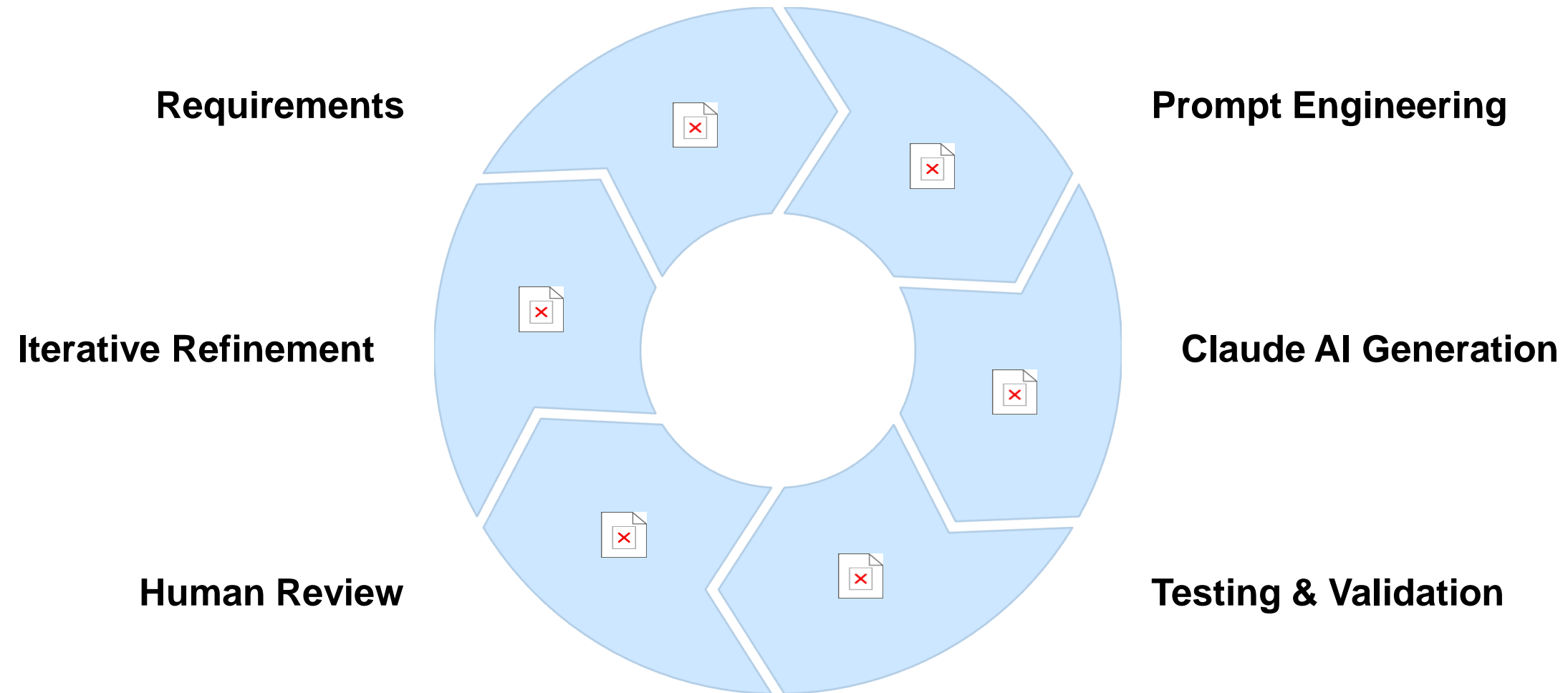
K-12 students

2025

GenCyber Camp

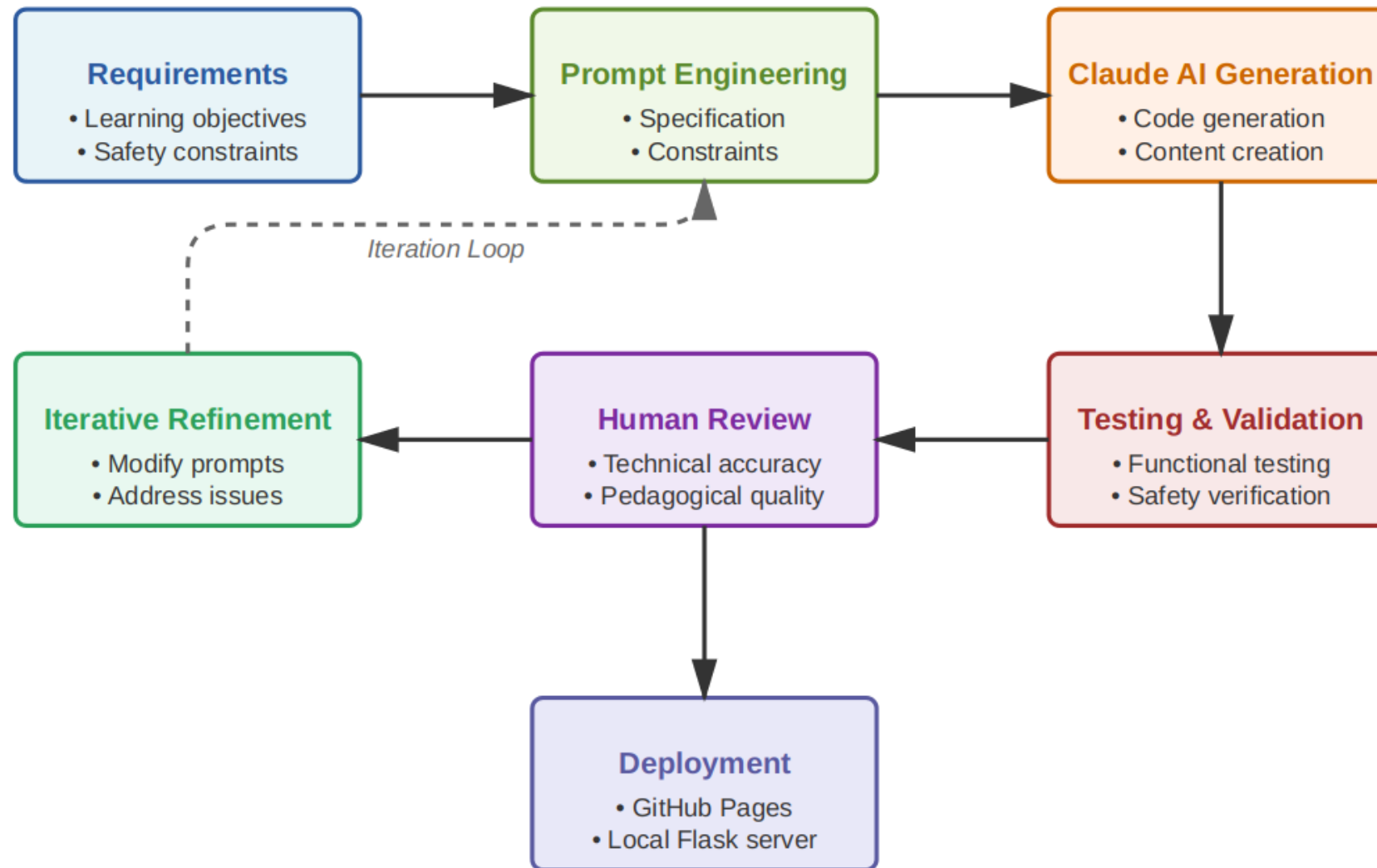
AI-Assisted Development: 80%+ Time Reduction

AI-Assisted Development Process



20 major prompts • ~30 refinements • 15% manual corrections

AI-Assisted Development Process



Complete Educational Platform

Interactive Content

- 12 HTML5 presentations
- Vacuum tubes → IoT evolution
- Gamified quizzes + leaderboards

Security Tools

- SlowLoris DoS tool
- Dictionary password cracker
- Built-in safety controls

Real Target

- AmpliPi IoT audio system
- Open-source platform
- Genuine vulnerabilities

📄 All materials open-source on GitHub

Slide 1 of 12

MICROELECTRONICS & SECURITY

GenCyber Summer Camp 2025


SECURE SYSTEM ACCESSED



Microelectronics Evolution

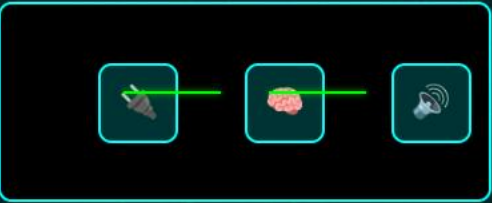
Journey from vacuum tubes to modern semiconductors. Explore how technology shrank from room-sized to nanoscale.






AmpliPi Architecture

Multi-zone audio streaming system powered by Raspberry Pi. 6 zones, 6 sources, infinite possibilities.



Previous Home Next



Security Testing

Real penetration testing on AmpliPi: Network scanning, password attacks, MitM, and DoS vulnerabilities discovered.

```
Terminal
$ nmap -sV 192.168.1.0/24
$ Scanning network...
  Found 5 devices
$ hydra -l admin -P pass.txt
192.168.1.100
  Password found: admin123
$ arpspoof -t 192.168.1.1
192.168.1.100
  ARP poisoning active
$ slowloris 192.168.1.100
  DoS attack initiated
```

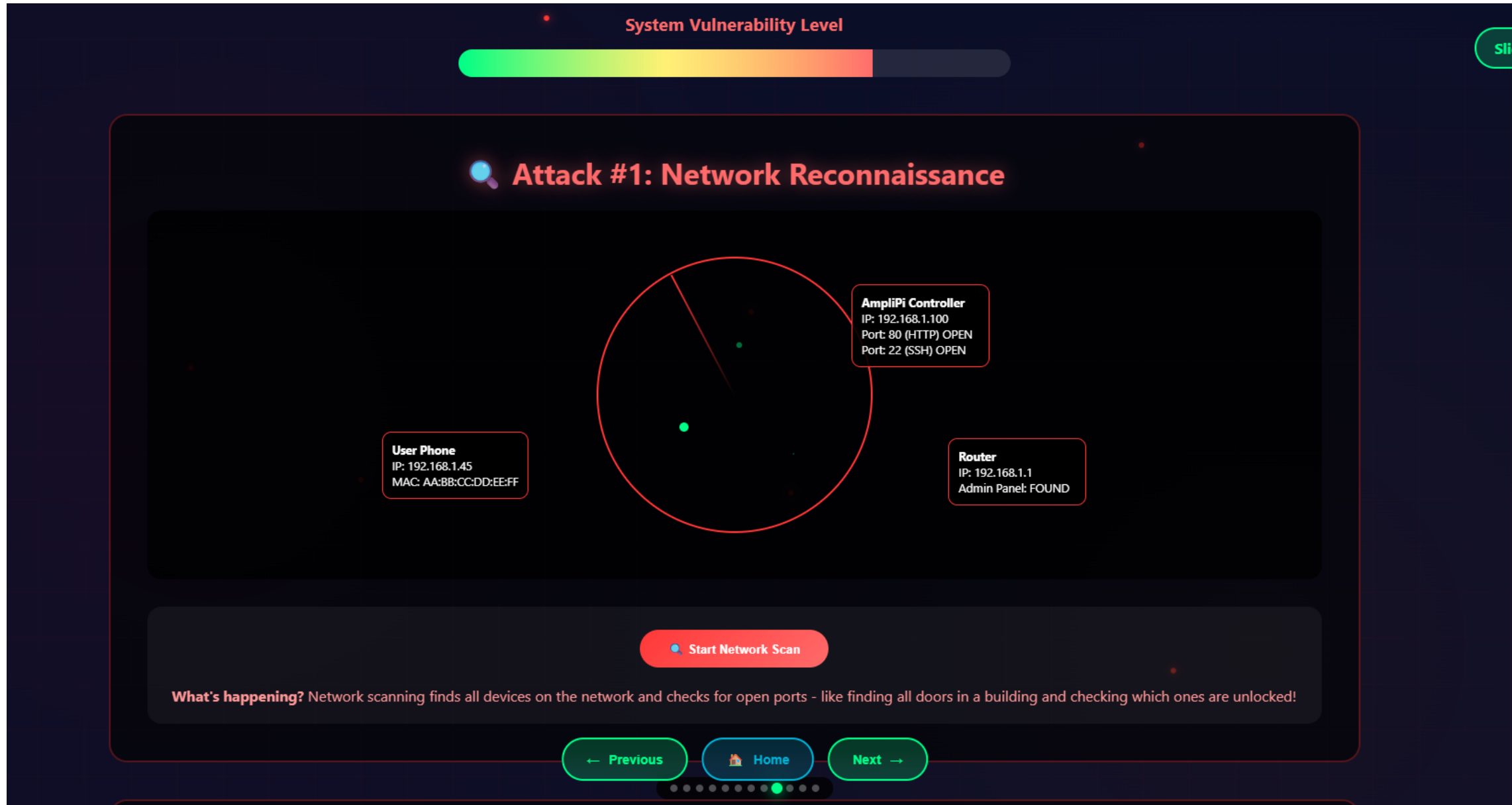
Teaching Through Visualization: Network Discovery

Key Features

- Progressive revelation - devices appear one by one
- Visual + audio feedback
- Learning by doing, not reading

Educational Value

- Students understand scanning process
- Immediate engagement
- Concepts become tangible



The screenshot displays a network discovery tool interface. At the top, a "System Vulnerability Level" bar shows a gradient from green to red, indicating a moderate level of vulnerability. The main content area is titled "Attack #1: Network Reconnaissance" and features a central network map with three nodes:

- User Phone**: IP: 192.168.1.45, MAC: AA:BB:CC:DD:EE:FF
- AmpliPi Controller**: IP: 192.168.1.100, Port: 80 (HTTP) OPEN, Port: 22 (SSH) OPEN
- Router**: IP: 192.168.1.1, Admin Panel: FOUND

Below the map is a "Start Network Scan" button. A text box explains: "What's happening? Network scanning finds all devices on the network and checks for open ports - like finding all doors in a building and checking which ones are unlocked!". Navigation buttons for "Previous", "Home", and "Next" are visible at the bottom.

Teaching DoS Attacks: The Restaurant Analogy

The Metaphor

Network connections = Restaurant tables

Partial HTTP requests = Customers holding tables

Never completing requests = Never ordering food

"It's like someone sitting at all tables but never ordering food"

Understanding SlowLoris: The Restaurant Analogy

The Restaurant

Your web server is like a restaurant with limited tables (connection slots). It can only serve a certain number of customers at once.

The SlowLoris Attacker

The attacker sends many "customers" who sit at tables but order very slowly, never finishing their order and holding tables indefinitely.

The Attack Method

Each fake customer keeps saying "I'm still deciding..." every few seconds, preventing the waiter from giving the table to real customers.

The Impact

Eventually all tables are occupied by slow fake customers. Real customers can't get in - the restaurant appears "Full" but no one is actually eating!

READY

Current Status

0

Active Connections

50ms

Response Time

0

Blocked Attempts

Attack Control Panel

Target IP (AmpliPi Device)

192.168.1.127

Target Port

80

Number of Connections (Fake Customers)

50

TEST CONNECTION


LAUNCH SLOWLORIS ATTACK

STOP ATTACK

How SlowLoris Works:

Live Results & Impact

Attack Visualization



Attacker

AmpliPi Server

NORMAL

Defense Mechanisms

Connection Timeout

Kick out slow customers after 30s

Rate Limiting

Max 20 tables per customer group

Reverse Proxy

Bouncer Filters Fake customers

All Defenses

Maximum restaurant security

STOP ATTACK

How SlowLoris Works:

- Open many TCP connections to the target server (reserve tables)
- Send partial HTTP headers very slowly (order extremely slowly)
- Keep connections open by sending more headers (keep saying "still deciding")

Real-Time Response Graph



The graph plots Response Time (milliseconds) on the y-axis (0 to 3,500) against Time on the x-axis (3:07:34 PM to 3:07:41 PM). A red line with circular markers shows the response time, which starts at a normal baseline of approximately 1,500ms and spikes to about 3,500ms at 3:07:36 PM, remaining elevated until 3:07:41 PM. A green dashed line at the bottom represents the normal baseline.

Dictionary Attack & Password Strength Analysis

Attack Features

- Real-time attack progress
- Multiple authentication formats
- AmpliPi-specific handling

Educational Components

- Password strength analyzer
- Educational feedback
- Rate limiting: 3 workers max

All students successfully discovered weak default passwords

[Back to Home](#)



PASSWORD SECURITY LAB

Educational demonstration of password strength and brute force attacks

WARNING: This tool performs REAL password attacks!
 Only use on your own AmpliPi device for educational purposes!

Target AmpliPi Configuration

AmpliPi IP Address	Username	Test Password
<input type="text" value="192.168.1.130"/>	<input type="text" value="admin"/>	<input type="text" value="Enter password to test"/>

TEST LOGIN

OPEN AMPLIPI

● Ready for password testing

Password Strength Analyzer

Enter Password to Analyze

Password List Configuration

Common Password Lists (Download & Upload):

Top 1000 Passwords

Top 10000 Passwords

SecLists Password Collection

WeakPass Lists

Download a password list, save as "passwords.txt" and upload here:

No file chosen

UPLOAD PASSWORD LIST

Password Cracking Controls

Password Source	Concurrent Workers
<input type="text" value="Built-in Common Passwords"/>	<input type="text" value="3"/>

START PASSWORD ATTACK

STOP ATTACK

Real-Time Cracking Progress

10/10000 passwords tested (0.1%)

10	barefeet	4.91	2.1s	2033.6s	password
Password Attempts	Current Password	Attempts/Second	Elapsed Time	Est. Remaining	Found Password

```

[10:22:53 AM] Username: admin
[10:22:53 AM] Passwords to test: 10000
[10:22:53 AM] This will attempt real login attacks!
[10:22:53 AM] Using 10 workers with batches of ~1000 passwords
[10:22:54 AM] Failed: hercules (1253ms)
[10:22:54 AM] Failed: thumbnails (1260ms)
[10:22:54 AM] Failed: rrrrr (1284ms)
[10:22:54 AM] Failed: odyssey (1298ms)
[10:22:54 AM] Failed: pregnant (1391ms)
[10:22:54 AM] Failed: barefeet (1388ms)
[10:22:54 AM] Failed: china (1413ms)
[10:22:54 AM] Failed: sprint (1424ms)
[10:22:54 AM] Failed: quasar (1462ms)
[10:22:54 AM] SUCCESS! Password found: password
[10:22:54 AM] Progress: 10/10000 passwords tested
[10:22:54 AM] PASSWORD CRACKED! Username: admin, Password: password
          
```

Real-World IoT Target: AmpliPi Audio System

Open-source multi-room audio system

REST API with multiple endpoints

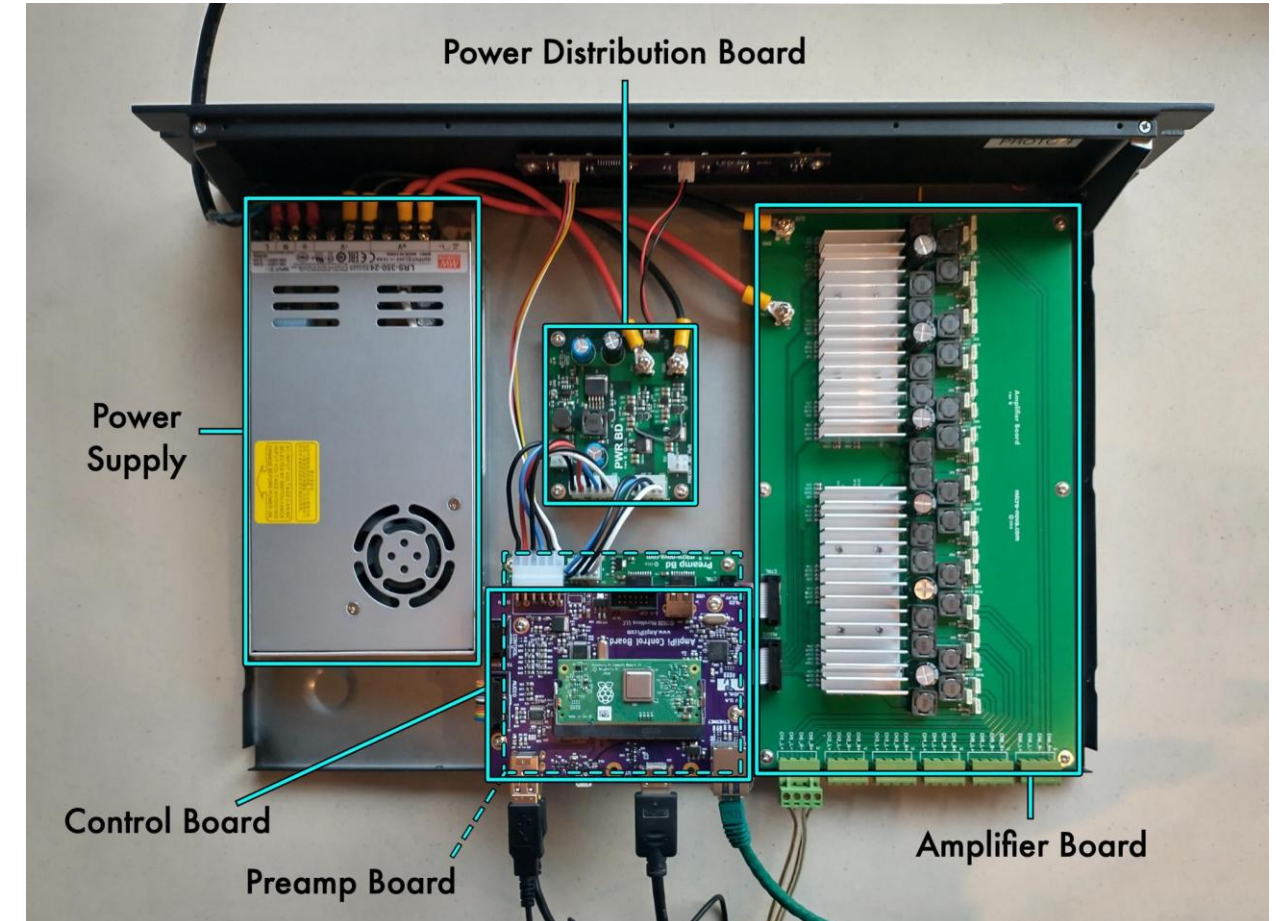
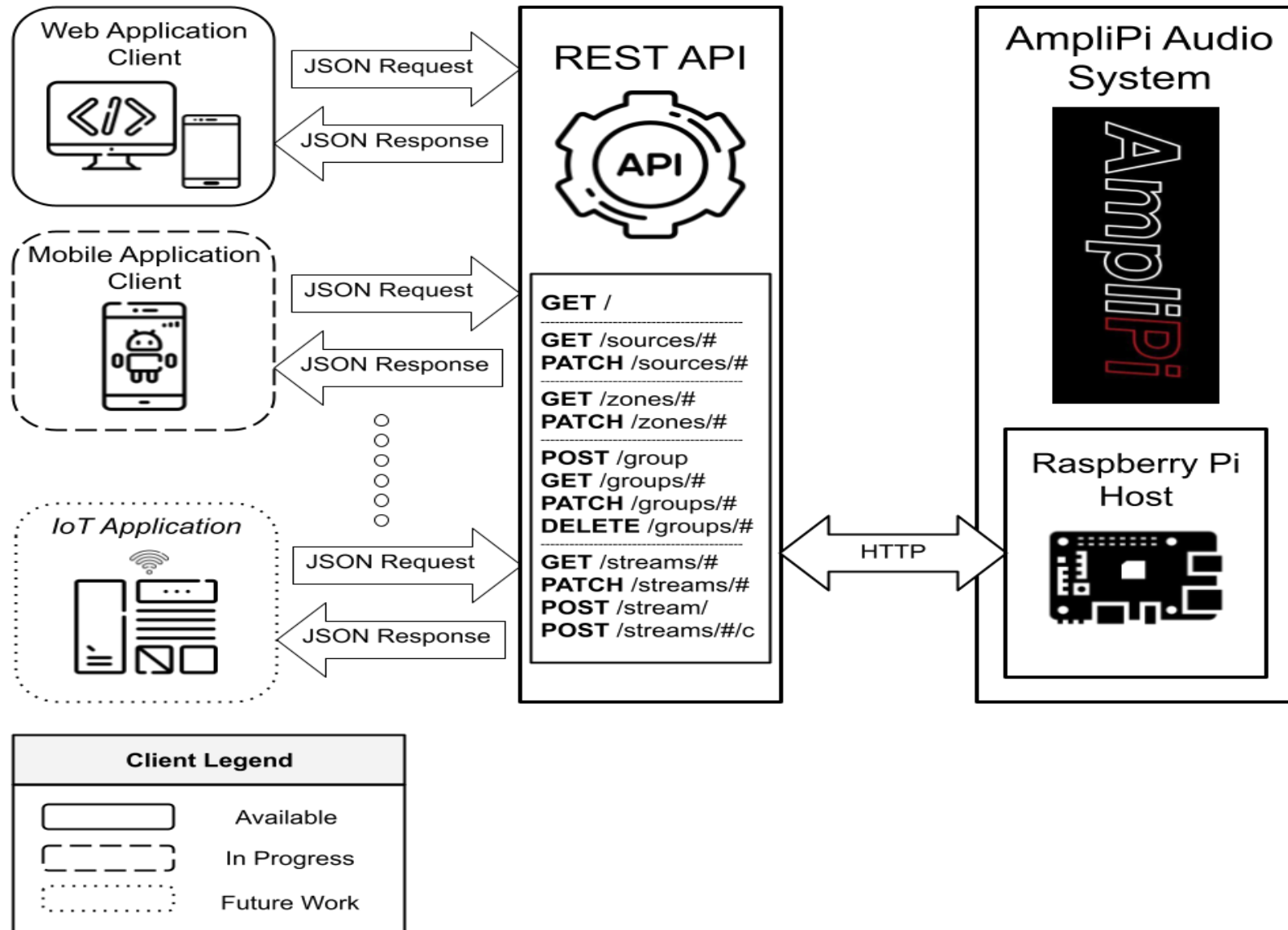
Runs on Raspberry Pi

Representative of real IoT deployments

Attack Vectors Explored

- Authentication weaknesses
- Denial of service vulnerabilities
- API endpoint exploitation

AmpliPi Audio System



Real-World Deployment: GenCyber Summer Camp 2025

40

K-12 Students

2

Weeks, 2 Cohorts

1

Isolated Lab Network

Lab Environment

20

Lab computers

1

Instructor machine (Flask
server)

2

AmpliPi devices

VLAN

192.168.1.0/24

All exercises supervised with safety controls



A1 | fx Timestamp

	A	B	C	D	E	F	G	H	I	J	K
1	Timestamp	Name	Score	Completion Time (seconds)	Percentage	Q1 Answer	Q2 Answer	Q3 Answer	Q4 Answer	Q5 Answer	Session ID
2	31/07/2025 09:13:46	Al [REDACTED]	5	10.4	100%	c	b	b	c	c	2025-07-31T13
3	31/07/2025 09:13:58	E [REDACTED] He	5	19.5	100%	c	b	b	c	c	2025-07-31T13
4	31/07/2025 09:14:02	K [REDACTED] ako-F	5	28.6	100%	c	b	b	c	c	2025-07-31T13
5	31/07/2025 09:13:57	Z [REDACTED] vis	4	13.1	80%	c	c	b	c	c	2025-07-31T13
6	31/07/2025 09:13:52	Els [REDACTED] row	4	22	80%	c	b	b	c	a	2025-07-31T13
7	31/07/2025 09:14:25	K [REDACTED] parte	4	30	80%	c	b	b	c	-	2025-07-31T13
8	31/07/2025 09:14:48	J [REDACTED] n	4	33	80%	c	b	b	c	a	2025-07-31T13
9	31/07/2025 09:14:02	K [REDACTED] th	3	30	60%	c	b	b	-	-	2025-07-31T13
10	31/07/2025 09:14:01	ch [REDACTED]	2	30	40%	c	c	b	b	-	2025-07-31T13
11	31/07/2025 09:14:10	Ka [REDACTED]	2	30	40%	c	-	-	a	c	2025-07-31T13
12	31/07/2025 09:14:32	gav [REDACTED] son	2	30	40%	c	c	b	b	-	2025-07-31T13
13	31/07/2025 09:14:35	Ja [REDACTED] Major	2	30	40%	a	c	b	c	-	2025-07-31T13
14	31/07/2025 09:14:13	Ju [REDACTED] thing	1	30	20%	b	a	b	-	-	2025-07-31T13
15	31/07/2025 09:14:01	lak [REDACTED] uri	0	30	0%	-	-	-	-	-	2025-07-31T13

Keeping Students Engaged: Gamification in Action

Real-time leaderboard

Google Sheets integration

Immediate feedback

Competitive element

100% participation • Sustained attention • Active competition

Student Achievements: Real Vulnerabilities Discovered

Dictionary Attack Success

✓ 100% of students discovered weak passwords

SlowLoris DoS Demonstration

✓ All students successfully executed DoS attacks

AI-Generated Code: Strengths & Limitations

✓ What Worked Well

- Functional code with minimal modifications
- Creative pedagogical approaches
- Rapid iteration capability
- Constitutional AI safety guardrails
- 85% code used without changes

⚠ Required Human Oversight

- Domain-specific edge cases (HTTP 302)
- Browser compatibility fixes
- Pedagogical appropriateness review
- Technical accuracy validation

📌 AI as accelerator, humans ensure quality & safety

Challenges & Solutions

1

Technical Challenges

- Flask server: 20 user limit
- Authentication detection issues
- Browser inconsistencies

2

Educational Challenges

- Hardware dependency (AmpliPi devices)
- Network setup complexity (VLAN configuration)
- Instructor technical expertise required

3

Solutions Applied

- Iterative refinement process
- Manual validation protocols
- Clear safety boundaries

1

Complete Methodology

- Prompt engineering strategies
- Iterative refinement process
- Safety control implementation

2

Functional Tools

- Working penetration testing demos
- Educational scaffolding
- Built-in safety mechanisms

3

Validated Results

- 40 student deployment
- Real vulnerability identification
- GenCyber camp success

4

Open Source

- All materials on GitHub
- Reproducible by educators
- Community contribution

📄 All materials available at microelectronics2025.github.io

Key Takeaways & Future Directions

Key Insights

**AI reduces development time
80%+**

**Human expertise remains
essential**

**Effective learning outcomes
achieved**

Future Research

- Model comparison (GPT-4, Gemini)
- Expanded IoT target platforms
- Real-time AI-human co-creation

Thank You

Questions?

GitHub repository: [microelectronics2025.github.io](https://github.com/microelectronics2025)

All materials open-source and freely available

Contact: kbadal@aggies.ncat.edu, xhyuan.ncat.edu