THE PACKET

THE UNIVERSITY OF ARIZONA

FALL

AUGUST 2020

THE UNIVERSITY OF ARIZONA

THE PACKET
AUGUST 2020

IN THIS ISSUE

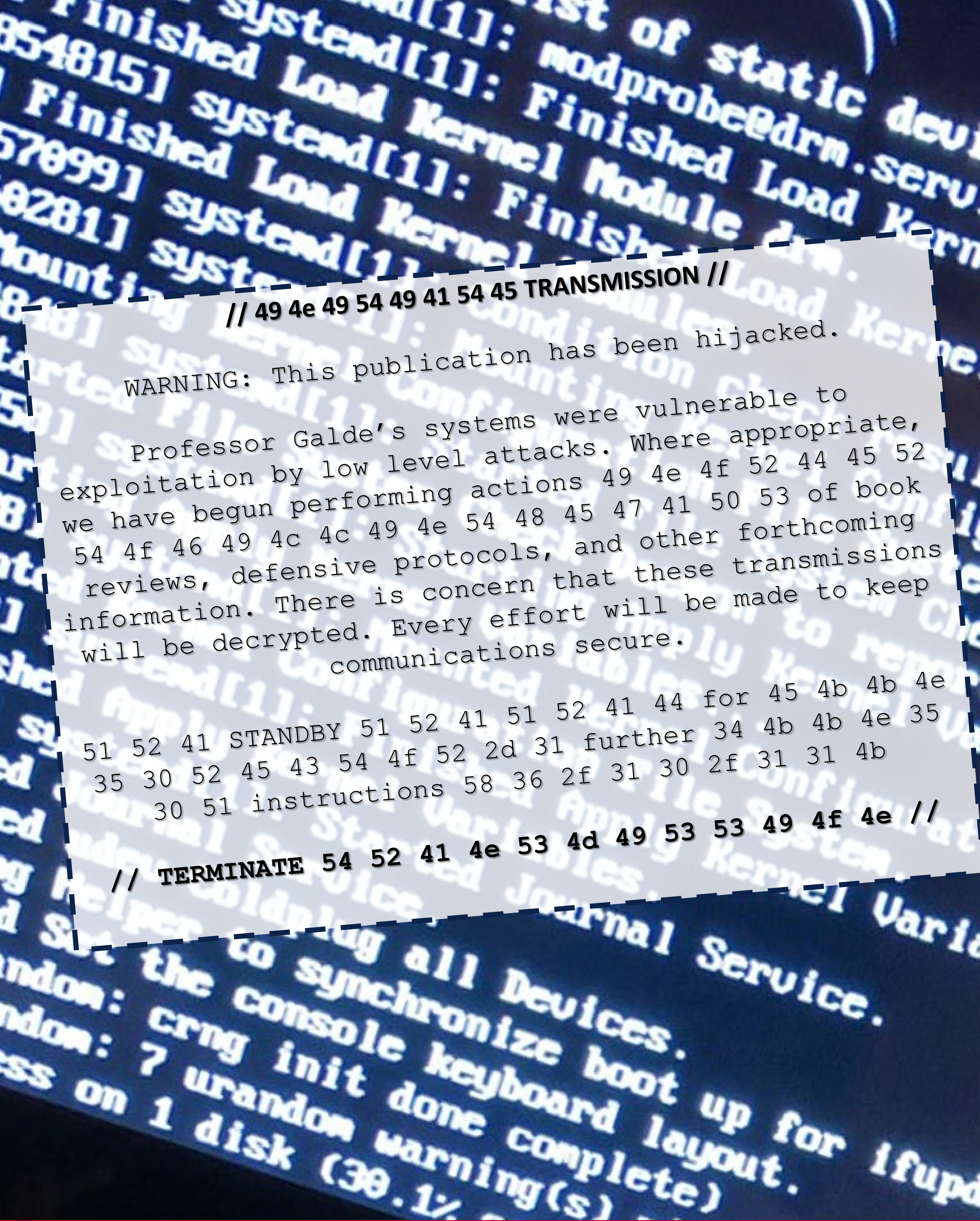
--- BEGIN MESSAGE ---

Welcome to the **AUGUST** issue of "**The PACKET**" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde and I am here again with the August issue. Welcome to the fall semester of 2020, this publication I hopes allows you to become interested in cybersecurity and the infosec community at large. Inside you will find news about cybersecurity topics and some choice projects that have found to be interesting while also allow students with budding abilities to try something new and students with more technical abilities to find project motivation to go further. If you have any questions, please feel free to reach out to any of the professors under the Cyber Operations Program. If this program interests you, there are advisors who will be more then happy to assist you getting set up. If you are just starting your infosec experience feel free to use this as a document to build ideas and learn about what paths interest you. For those that are more experienced I hope you find this to keep up to date in a dynamically changing world with an always evolving threat.

Thanks for joining me on this wild ride and I hope everyone has a good Fall semester!!

--- END MESSAGE ---

CYBER CLASSIFIED BY: PROFESSOR GALDE
REASON: CYBER OPERATION PROGRAM
DECYBER ON: SEPTEMBER 2060



// 49 4e 49 54 49 41 54 45 TRANSMISSION //

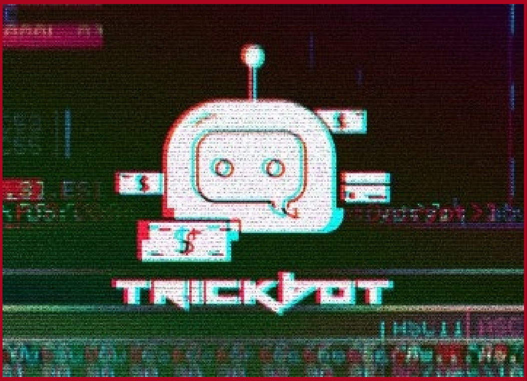
WARNING: This publication has been hijacked.

Professor Galde's systems were vulnerable to exploitation by low level attacks. Where appropriate, we have begun performing actions 49 4e 4f 52 44 45 52 54 4f 46 49 4c 4c 49 4e 54 48 45 47 41 50 53 of book reviews, defensive protocols, and other forthcoming information. There is concern that these transmissions will be decrypted. Every effort will be made to keep communications secure.

51 52 41 STANDBY 51 52 41 51 52 41 44 for 45 4b 4b 4e 35 35 30 52 45 43 54 4f 52 2d 31 further 34 4b 4b 4e 35 30 51 instructions 58 36 2f 31 30 2f 31 31 4b

// TERMINATE 54 52 41 4e 53 4d 49 53 53 49 4f 4e //

HACKS OF THE MONTH



They have the best testers, the best...

TrickBot is a nasty piece of malware making the rounds and the most recent version has a small development issue. The developers mistakenly distributed a test version which warn victims of the malware. Grabber.dll is TrickBot's password and cookie-stealing module that attempts to harvest saved browser credentials These stolen credentials can then be used to login to the victim's accounts.

Not all hero's wear capes.

The Emotet botnet works by spamming targets with emails which contain a malicious document. This forces the victim to a hacked webpage but the Emotet gang employs the same password for all of its web sites. An unknown vigilante appears to have discovered this common password and has been abusing this weakness botnet to sabotage Emotet's malware with animated GIFs.

60% of the time, social engineering works every time.

So social engineering is often overlooked but this is the consistent winner over time as people are always the weakest link. Twitter employees were manipulated in handing over credentials and individuals used this access to make people believe that bitcoin could be doubled somehow. Not a very technical hack but one that works.

CYBER NEWS UPDATES

FBI WARNING US COMPANIES OPERATING IN CHINA

The US Federal Bureau of Investigation has sent an alert on Thursday warning US companies about backdoor malware that is silently being installed on the networks of foreign companies operating in China via government-mandated tax software, all foreign companies are required by local Chinese laws to install this particular piece of software in order to handle value-added tax (VAT) payments to the Chinese tax authority. Companies in the healthcare, chemical, and finance sectors are in danger due to interest in these sectors.

DISCOVER MORE | CYBV 480 CYBER WARFARE | CYBV 435 Cyber Threat Intelligence | CYBV 385 INTRODUCTION TO CYBER OPERATIONS | CYBV 301 FUNDAMENTALS OF CYBERSECURITY

SECRET SERVICE ANNOUNCES THE CREATION OF THE CYBER FRAUD TASK FORCE

The U.S. Secret Service has created the Cyber Fraud Task Forces (CFTFs), aimed at preventing, detecting and mitigating complex cyber-enabled financial crime – including making arrests and convictions. The CFTF is the result of a formal merging of two of the Secret Service's existing units into a single unified network. The Electronic Crimes Task Forces (ECTFs) and the Financial Crimes Task Forces (FCTFs)

DISCOVER MORE | CYBV 454 MALWARE THREATS & ANALYSIS | CYBV 435 CYBER THREAT INTELLIGENCE | CYBV 388 CYBER INVESTIGATIONS AND FORENSICS | CYBV 385 INTRODUCTION TO CYBER OPERATIONS

VERIZON ADDS PROTECTION AGAINST SIM SWAPPING HACKS IN MOBILE APP

At the end of June, the company launched a feature called "Number Lock," which makes it easier for users to enable protection that could potentially stop SIM swapping hacks. When enabled, if someone impersonates the customer and tries to port out their number, Verizon notifies the customer via text message or email, attempting to verify that it's really them. Verizon employees can override this once the customer verifies themselves however so not foolproof.

DISCOVER MORE | CYBV 474 ADVANCED ANALYTICS FOR SECURITY OPERATIONS | CYBV 435 CYBER THREAT INTELLIGENCE | CYBV 329 CYBER ETHICS | CYBV 301 FUNDAMENTALS OF CYBERSECURITY

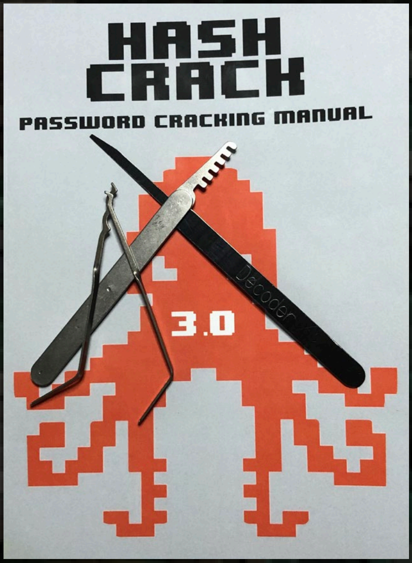
BOOK REVIEW

Rector-134

WANT TO DO THIS?
CYBV 480
CYBV 473

HASH CRACK: Password Cracking Manual

This is an information rich little book that primarily covers how to extract and crack hashes (a one-way encryption function for storing passwords) for everything from MD5, to Bitcoin and Mac OS X.



It’s written as a very technical reference manual, and does assume an intermediate level of understanding of the subject matter. However, it’s still something that a beginner can pick up and use as a starting point to conduct secondary research on the internet and begin learning about cracking passwords.

(Bogota lock picks, comb picks and EZ decoder not included…)

It focuses on using Hash Cat and John the Ripper, which are both powerful tools, but it covers much more as well. It contains resources for password analysis, how to manage foreign character sets, dictionary and wordlist utilities, and numerous other tips that even some advanced users might not think of.

Granted, you could probably find all of the information contained in this book online. But it would take you an excruciating length of time. This book is dense for a reason - it’s as pure and uncut as they come. The ’10 Crack Commandments’ alone are worth the meager price. We specifically like number 7: “Thou shalt understand basic human psychology/behavior.”

INTERNSHIP BOARD

Cyber Exploitation Officer

As a Cyber Exploitation Officer intern for the CIA, you will work alongside career staff in the evaluation and exploitation of digital and all source intelligence information in a dynamic digital environment, using a variety of analytic and forensic tools to extract valuable information from digital data, as well as creating a range of products that will drive operations and further collection.

Cyber Exploitation Officer interns are generally required to work either a combination of one semester and one summer, or two 90 day summer internships.

Cyber Security Officer

As a Cyber Security Intern for the CIA, you will work side-by-side other Cyber Security professionals to protect Agency data and systems using sophisticated tools, instrumentation, and knowledge of CIA Information Technology and tradecraft to monitor, evaluate, and manage IT risk.

You will protect CIA data and IT systems by identifying current threats, mitigating vulnerabilities, and anticipating future cyber security challenges. You may additionally be required to analyze existing and future systems across the Agency, implement network defenses, develop threat models and security risk assessments, and conduct forensic analysis of security events and logs via sophisticated security and event management tools.

DUE TO THE CURRENT ISSUES SURROUNDING THE COVID-19 PANDEMIC, SOME GOVERNMENT AGENCIES ARE EXPERIENCING HIRING FREEZES, BUT WILL STILL PROCESS APPLICATIONS FOR HIRE. PLEASE REMAIN FLEXIBLE WITH HIRING OFFICIALS DURING THIS TIME.

DEBRIEF ROOM

DANIEL DIETERLE

Time of Debrief: 18:32 Zulu 18 JUNE 2020

Subject:

Daniel Dieterle has over 20 years of experience in the cyber security community. He started out repairing components on Commodore 64 computers, and most recently worked for a Fortune 500 company that has thousands of virtual and physical servers in its datacenter. He has authored numerous books on Kali Linux (which were used in the War Colleges, one of Cyber Command's training divisions, and by every branch of the US Military) and has additionally written a book on Security Testing with Raspberry Pi, and maintains multiple blogs.

You can find more about him on his website Dan the IoT Man, blog, or on Instagram on his handle 'CyberArms'

--- CLASSIFIED DEBRIEF FOLLOWS ---

DEBRIEF ROOM

DANIEL DIETERLE

Firstly, thank you very much for agreeing to an interview! I think your breadth and depth of experience will be extremely intriguing as well as beneficial to both students and faculty. Let's get down to business!

First up: You've been in this career field for a long time - about two decades - and you started out doing some very hands on repairs with now classic hardware. Rather than a history lesson over your background, I'd like to branch this into two questions: Firstly, how do you feel that initial hands on experience has shaped your career and skillset?

D. Dieterle: "I think hands on experience was very beneficial to my development in this field. I actually have seen it as a type of "natural progression". I believe my early hands on hardware bench tech experience helped a lot in my "Internet of Things" interests. From the very beginning I was soldering and de-soldering parts, playing with circuit boards and schematics, replacing chips and troubleshooting sensors & faults. These skills are used a lot in the IoT field."

And secondly, having seen the career field advance as fast as it has, if you were to start all over today as a new guy - what would be your first steps in learning?

D. Dieterle: "If I had to start all over, I would do exactly what I recommend new students do – Start in the IT field. IT Support is great for learning operating systems, software packages, and interpersonal skills. Then move into Server Administration and Support. This way you learn how to setup, administer and troubleshoot servers. You learn how servers are supposed to work, very necessary to know before you start trying to "break them". Network & System Engineering are very important too, you learn all about network hardware, communication and what it takes to build complex networks. If you move into security with this type of background and experience, you will already be very far ahead, I personally believe, then someone trying to enter directly into the security field with no IT background."

DEBRIEF ROOM

DANIEL DIETERLE

One of your websites takes me to my next topic - your monicker "Dan the IoT Man". You have an obvious penchant for Internet of Things devices, as well as a talent for devious and creative uses for them. What has been your personal favorite of these numerous projects, and what got you into the IoT?

D. Dieterle: "As for my favorite IoT project, I really love multiple things, but I would have to say, "Magic Mirrors". Magic Mirrors basically bring technology to plain old household mirrors. Basically, you take a Raspberry Pi, a one-way mirror and Magic Mirror software and you have a "Magic Mirror". They are great, you can put your daily schedule on them, use them for news or weather updates. I've been working on taking them to the next level, I've implemented cameras and microphones into them, turning them into something like a "Nanny Cam" or a home surveillance system. I've also been working on implementing Arduino boards and sensors into them. The thinking being that, the Arduino could power on the magic mirror when it "senses" someone has entered the room. I don't want to give too much more information away, but yes, they are a lot of fun!"

As an aside to the previous two questions, what steps would you recommend someone take to get into tinkering with IoT devices? They have obvious pentesting capabilities as you've showcased, as well as unique security concerns, but it seems from the outside like a vast field with little comprehensive guidance for beginners.

D. Dieterle: "As to getting into tinkering with IoT Devices, the best way is to learn by doing! Start with Arduino and Raspberry Pi boards. There is a ton of information and tutorials out there on them and they are very well established. If you have no experience at all, the Raspberry Pi is the best place to start. Get an RPi starter kit that includes sensors, electronic components & wires and have fun!"

DEBRIEF ROOM

DANIEL DIETERLE

You and I share a couple of interests that are a little apart from the norm - Filipino Martial Arts, brutal gym sessions, and lock picking. Let's talk mindset. How do you see the fluidity and adaptability that are core to FMA and the intensity behind grinding through a late night workout as connecting to your work in cyber security?

D. Dieterle: Persistence and consistency pay! Just as with martial arts, weightlifting and lock picking, you need these two mental disciplines to succeed in Cyber Security. Many times, I have tried using a tool, or a new technique and it wouldn’t work, I’d try three, four, even five times with no luck. On the sixth try everything clicked and success! If I would have given up right away, or even on my fifth attempt, I never would have gotten it. You also need to learn every day and constantly increase your knowledge to “advance in the ranks”, so to say.

And now that we've mentioned lock picking, how often do you apply that skill pentesting and do you have a fun story of successfully gaining entry during a penetration test? Names and places redacted to protect the innocent as well as guilty, of course!

D. Dieterle: “I have tons of stories, but what always amazes me the most is, once you gain access to the inside of a building, if you look the part, no one really questions you. Even going back to my IT field support days, over 20 years of being inside of tech corporations, government, and financial facilities, I can count on one hand how many times I was asked to verify my identity once inside the gate. On the server side, my very first engagement, well, all I can say is a that a database manager used his wife’s name as the admin password for a city website. I was like, it’s not supposed to be this easy!”

DEBRIEF ROOM

DANIEL DIETERLE

You've written extensively about Kali Linux - if you had to pick your top three favorite tools, what would they be and why?

D. Dieterle: My top three favorite tools? P4wnP1 would be one of the first. It is an extremely powerful and well-polished Raspberry Pi USB “attack device” based on Kali Linux. Cobalt Strike is another, of all the Command & Control platforms, it is the best that I have used. It is extremely feature rich and works very well, bringing almost true “Click to Pwn” capability. Lastly, I would say Sn1per – It is a very functional and useful automated attack tool, and works great on a Raspberry Pi!

Back to the mindset topic to wrap up things up with some parting wisdom: You had two recent posts on your Instagram that really stood out to me personally. In one, you quoted the British SAS' motto "Who Dares Wins" and expressed your proponency for taking risks, and the other one in your own words "Live your Adventure!". In the ever increasing complexity of today's world where risk is ubiquitous and people have never had more freedom of choice, what's your advice when it comes to taking risks and embarking on adventures in the cyber world?

D. Dieterle: Ah yes, “Who dares wins”! For me taking risks has gotten me where I am today. I started out as a hardware bench tech, worked up through about every possible position in the IT world, switched to security and now I am an internationally published security author. At each step I had to educate myself, this included countless lunch breaks and weekends taking classes and studying for certification tests. I knew in my mind what I wanted to do, and took the steps to accomplish it. Many times, you are the only one who believes you can do it. It is not without risks, things don’t always work out well, lol, but if you never try the answer is always no – “Who Dares Wins!”

CYBER OPERATIONS FALL SCHEDULE

ADVISING UPDATE

A FRIENDLY REMINDER

THE ENROLLMENT FOR FALL CLASSES IS CURRENTLY OPEN AND CLASSES ARE STARTING TO FILL. IF YOU HAVE NOT ALREADY ENROLLED NOW IS THE TIME TO DO SO. IF YOU NEED ASSISTANCE CHOOSING YOUR COURSES, PLEASE SCHEDULE AN APPOINTMENT WITH YOUR ACADEMIC ADVISOR. ADVISOR CONTACT INFORMATION CAN BE FOUND HERE: HTTPS://AZCAST.ARIZONA.EDU/STUDENT-SERVICES/ADVISING/MEET-YOUR-ADVISOR

NOTE, TUITION AND FEES ARE NOT DUE AT THE TIME OF ENROLLMENT. THE DEADLINE TO PAY FOR ALL UNITS REGISTERED AS OF 8/19/20 WITHOUT LATE FEES IS 8/24/20. STUDENTS USING MILITARY BENEFITS HAVE CODES ADDED TO THEIR RECORD THAT KEEPS LATE FEES FROM BEING ADDED WHILE WAITING FOR BENEFITS TO PROCESS.

CYBER OPERATIONS FALL SCHEDULE

FILLING UP FAST

CAT #	COURSE
CYBV 301	FUNDAMENTALS OF CYBERSECURITY
CYBV 326	INTRODUCTORY METHODS OF NETWORK ANALYSIS
CYBV 329	CYBER ETHICS
CYBV 354	PRINCIPLES OF OPEN SOURCE INTELLIGENCE (7 WEEK CLASS 2 ONLY)
CYBV 385	INTRODUCTION TO CYBER OPERATIONS
CYBV 388	CYBER INVESTIGATIONS AND FORENSICS
CYBV 400	ACTIVE CYBER DEFENSE
CYBV 435	CYBER THREAT INTELLIGENCE
CYBV 436	COUNTER CYBER THREAT INTELLIGENCE (7 WEEK CLASS 2 ONLY)
CYBV 440	DIGITAL ESPIONAGE (7 WEEK CLASS 1 ONLY)
CYBV 441	CYBER WAR, TERROR AND CRIME (7 WEEK CLASS 2 ONLY)
CYBV 454	MALWARE THREATS & ANALYSIS
CYBV 471	ASSEMBLY LANGUAGE PROGRAMMING FOR SECURITY PROFESSIONALS
CYBV 473	VIOLENT PYTHON
CYBV 480	CYBER WARFARE
CYBV 496	INTRODUCTION TO SECURITY SCRIPTING (7 WEEK CLASS 1 ONLY)
CYBV 498	CAPSTONE IN CYBER OPERATIONS

HACKING POC

Part 1/6

P4WNP1 WITH OLED INTERFACE AND USB HAT

This month we're going to deep dive into a project that will introduce us to some basic hardware assembly, customization via code editing, and once we have it up and running we'll take our new pentesting tool for a trial run.

A P4wnP1 is a Raspberry Pi 0W based device similar to a USB Rubber Ducky, but capable of more advanced payloads and essentially carries a lite version of Kali Linux on board. Additionally, it's an excellent learning tool for flashing images, the command line, and basic hardware constructs. Let's get started! You'll see it referred to as P4wnP1 ALOA a lot, which refers to 'A Little Offensive Application'.

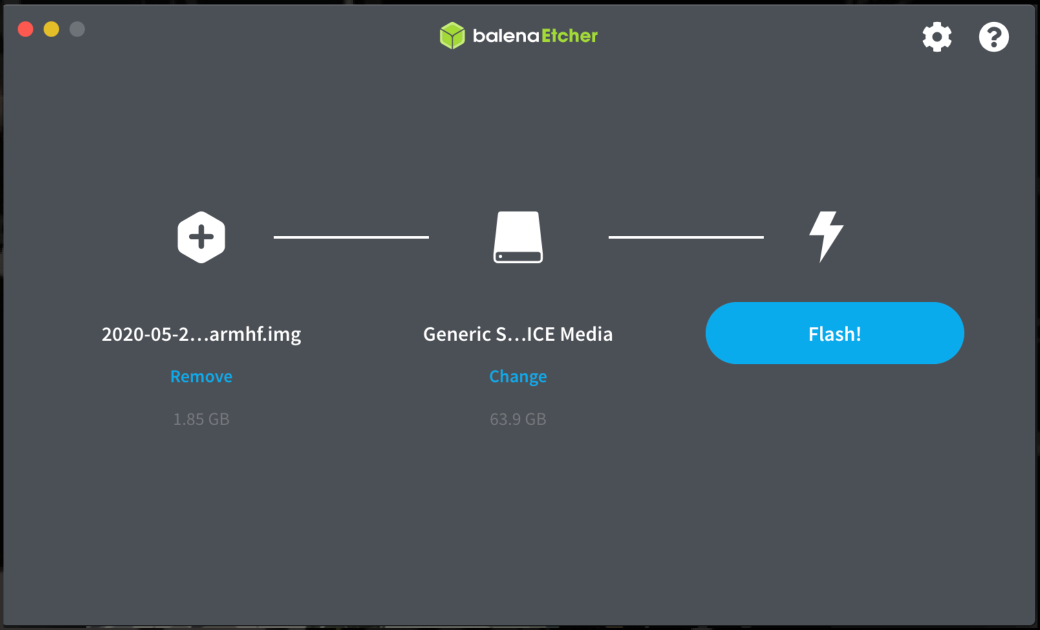
First, procure the parts listed below - some you may have lying around - and download an etcher, and this image of P4wnP1 ALOA by BeBoXos- this is not an image from the original creator, but after a weekend of tinkering with different images, we found this to be absolute easiest.

List of parts:
Raspberry Pi 0W (with headers) = $14.00
USB Dongle = $7.59
1.3" OLED Display HAT = $16.95
32 GB Micro SD Card = $8.49
Total = $47.03

CAUTION — This article shows you how to create a device with potentially illegal applications. This series is intended for academic purposes only, and to provide education to cyber security professionals. You assume any risk of using the information in this article.

Now that we've got our parts, set aside the gadgetry for a moment and grab the SD card. If you don't have one, you'll need an SD card adapter with a USB plug in that matches your computer.

First, use the etcher to flash the P4wnP1 image to the SD card. It's as simple as illustrated in the screen capture below.



That's it! You may see in other tutorials online people recommending that first you install Raspbian Stretch Lite and so on - not only is that release of Raspberry Pi OS no longer supported, it no longer works with the current P4wnP1 release and is no longer a necessary step. The process we demonstrate here is the simplest by far.

HACKING POC

Part 3/6

Now we'll begin playing with our hardware a bit. First, insert the SD card into the Raspberry Pi 0W, and plug into it from your computer via the MicroUSB port labeled USB (Not PWR In). Give it a few minutes to boot, then we're going to connect to it over WiFi.

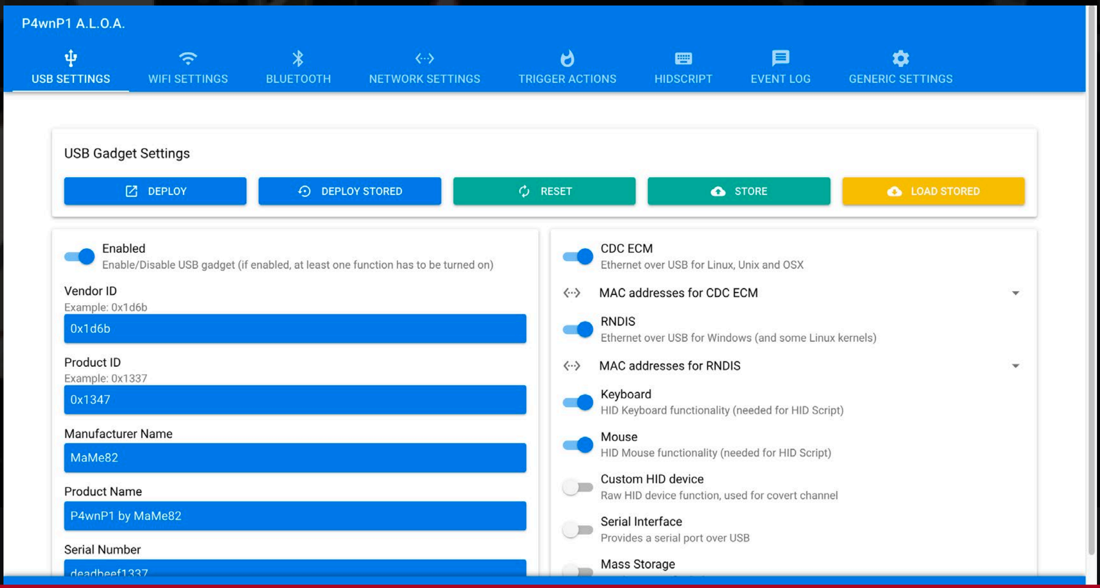
Go to your WiFi menu, and you'll see the SSID:

💥🖥💥 Ⓟ➃ⓌⓃⓅ❶

When prompted, the password is: **MaMe82-P4wnP1.** Be aware, it may not display a positive connection - don't fear! That's because you're connected to the device itself, not to the internet.

Open your browser and enter the following static IP to access the menu shown below:

http://172.24.0.1:8000



USB Gadget Settings

Enabled
Enable/Disable USB gadget (if enabled, at least one function has to be turned on)

Vendor ID
Example: 0x1d6b
0x1d6b

Product ID
Example: 0x1337
0x1347

Manufacturer Name
MaMe82

Product Name
P4wnP1 by MaMe82

Serial Number
deadbeef1337

CDC ECM
Ethernet over USB for Linux, Unix and OSX

MAC addresses for CDC ECM

RNDIS
Ethernet over USB for Windows (and some Linux kernels)

MAC addresses for RNDIS

Keyboard
HID Keyboard functionality (needed for HID Script)

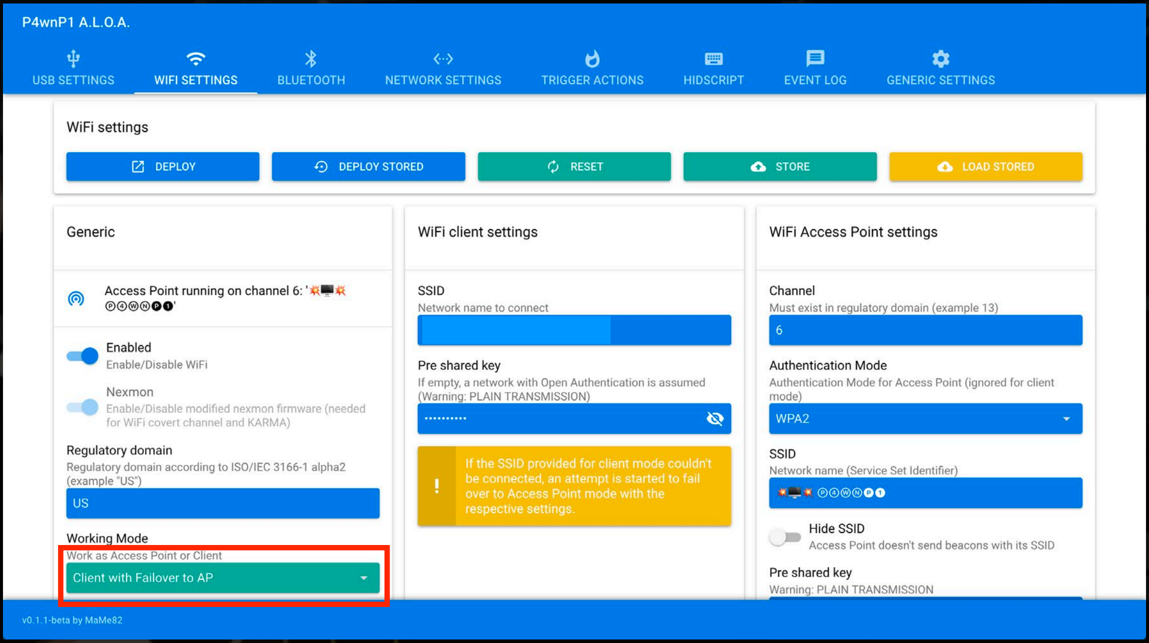
Mouse
HID Mouse functionality (needed for HID Script)

Custom HID device
Raw HID device function, used for covert channel

Serial Interface
Provides a serial port over USB

Mass Storage

If that menu came up, we know that we have a successful image flashed to our SD card. Before we move onto hardware, we're going to set it up so that we can connect to it via our home WiFi network. Go to the 'WiFi Settings' tab. Under 'Working Mode' on the bottom left, select 'Client with Failover to AP', then in the middle section that populates enter your own SSID and password.



Generic

Access Point running on channel 6: '💥🖥💥 ⓟⓐⓦⓝⓟ❶'

Enabled: Enable/Disable WiFi

Nexmon: Enable/Disable modified nexmon firmware (needed for WiFi covert channel and KARMA)

Regulatory domain: Regulatory domain according to ISO/IEC 3166-1 alpha2 (example "US") — US

Working Mode: Work as Access Point or Client — Client with Failover to AP

WiFi client settings

SSID: Network name to connect

Pre shared key: If empty, a network with Open Authentication is assumed (Warning: PLAIN TRANSMISSION) — ••••••••••

! If the SSID provided for client mode couldn't be connected, an attempt is started to fail over to Access Point mode with the respective settings.

WiFi Access Point settings

Channel: Must exist in regulatory domain (example 13) — 6

Authentication Mode: Authentication Mode for Access Point (ignored for client mode) — WPA2

SSID: Network name (Service Set Identifier) — 💥🖥💥 ⓟⓐⓦⓝⓟ❶

Hide SSID: Access Point doesn't send beacons with its SSID

Pre shared key: Warning: PLAIN TRANSMISSION

This will make some of the following steps much simpler.

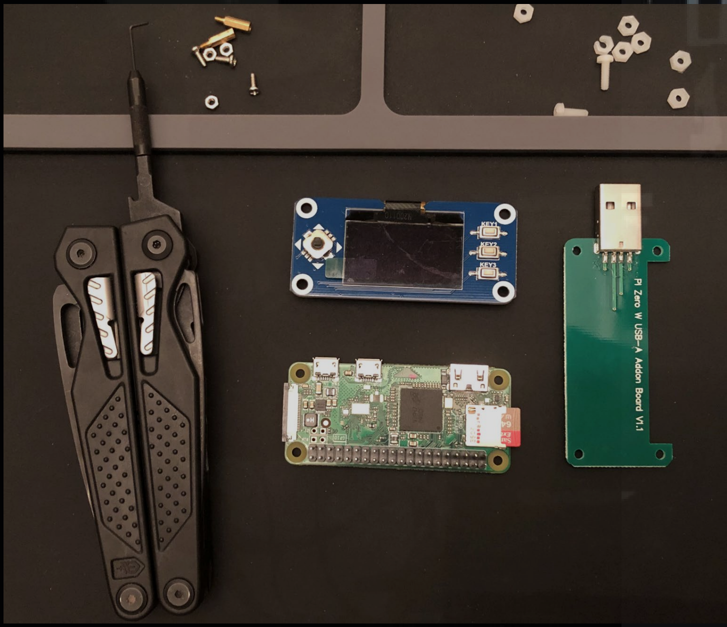
While we're at it, let's change the Access Point SSID to something more innocuous sounding that blends into our wireless environment. And as a security best practice, change the password as well.

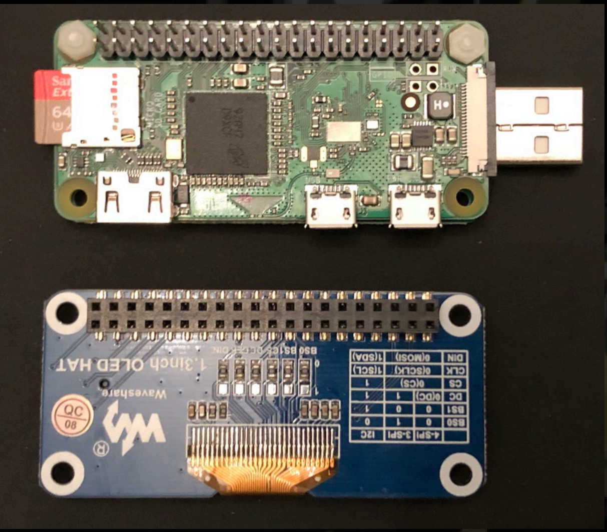
HACKING POC

Part 5/6

Now, onto the gadgetry! You won't need much in the way of tools. We used a simple multitool. Alternatively, a small Philips head screwdriver and needle nose pliers will work.

First we'll install the USB Hat. Mount it to the bottom of the Raspberry Pi 0, and use two of the supplied white plastic screws, two nuts as spacers, and two nuts on top to secure the two pieces together. The cutout in the USB Hat will leave the bottom of the GPIO pins exposed.



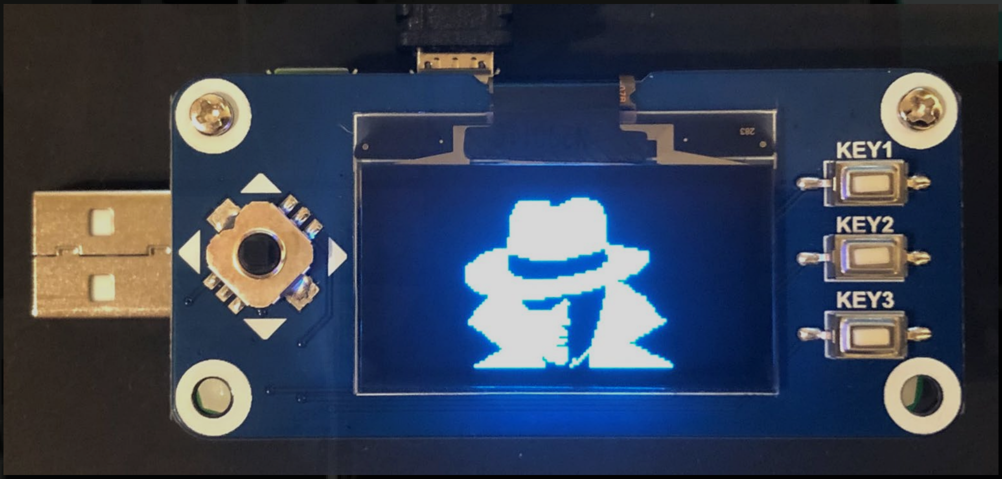


For the OLED display, we first will secure the two brass pieces into the remaining holes on the Raspberry Pi using two of the metal nuts. Then, press the OLED display down onto the GPIO pins (you may have to use some force) until it snaps into place. Secure it by threading two of the small metal screws into the tops of the brass pieces.

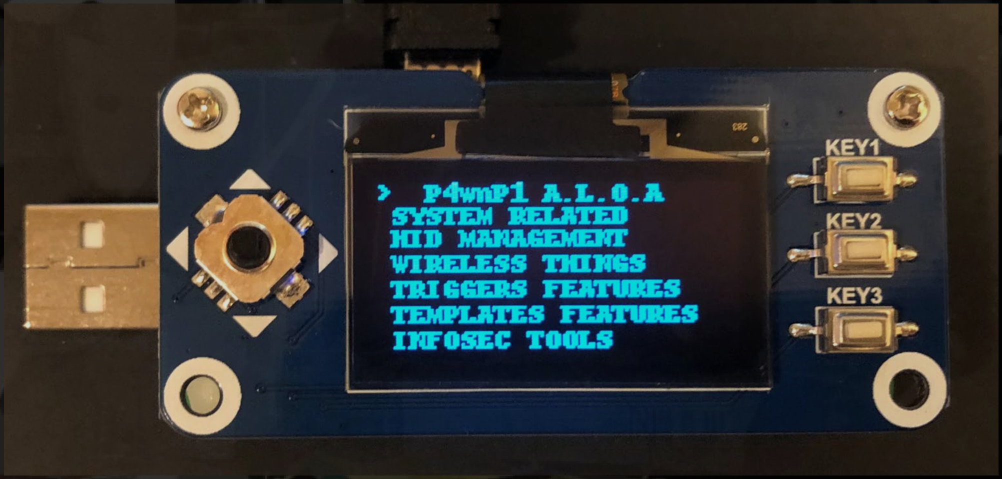
HACKING POC

Part 6/6

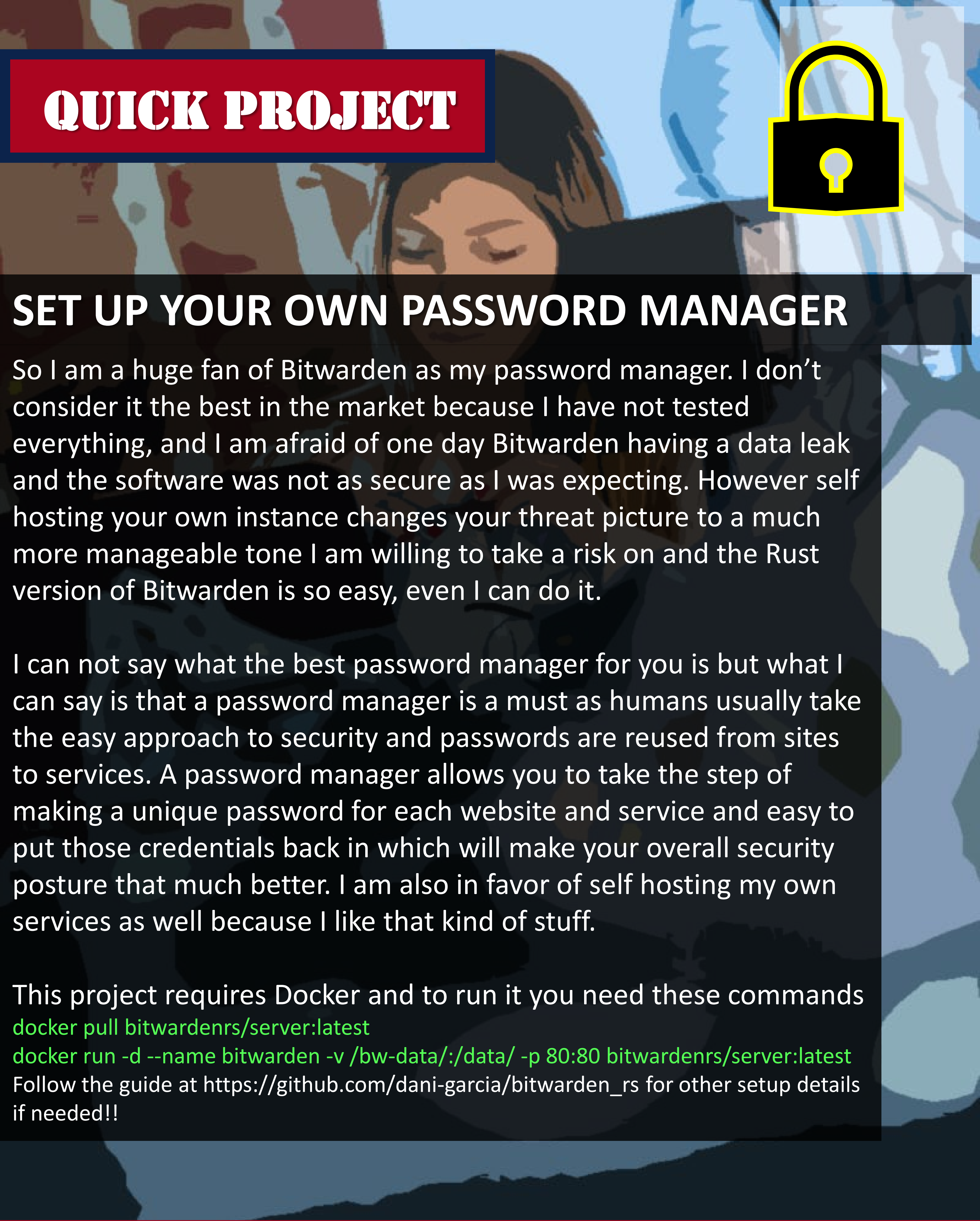
Now, the moment of truth… Plug the Micro USB into the USB port and…



It will briefly show us this mysterious character, then load the following menu that we can interact with using the four button toggle:



You can familiarize yourself with the native options for now. Next month we'll cover how to script a tool of our own!



QUICK PROJECT

SET UP YOUR OWN PASSWORD MANAGER

So I am a huge fan of Bitwarden as my password manager. I don't consider it the best in the market because I have not tested everything, and I am afraid of one day Bitwarden having a data leak and the software was not as secure as I was expecting. However self hosting your own instance changes your threat picture to a much more manageable tone I am willing to take a risk on and the Rust version of Bitwarden is so easy, even I can do it.

I can not say what the best password manager for you is but what I can say is that a password manager is a must as humans usually take the easy approach to security and passwords are reused from sites to services. A password manager allows you to take the step of making a unique password for each website and service and easy to put those credentials back in which will make your overall security posture that much better. I am also in favor of self hosting my own services as well because I like that kind of stuff.

This project requires Docker and to run it you need these commands

```
docker pull bitwardenrs/server:latest
docker run -d --name bitwarden -v /bw-data/:/data/ -p 80:80 bitwardenrs/server:latest
```

Follow the guide at https://github.com/dani-garcia/bitwarden_rs for other setup details if needed!!

CYBER SECURITY HISTORY

ACTIVE DIRECTORY RELEASED — AUGUST 11, 2000

Active directory started off as centralized domain management but later became an umbrella title for a broad range of directory-based identity-related services for business customers. First available in Windows Server 2000 Server Edition it has been improved ever since. In the years following became a widely used directory service in business environments and replaced Windows NT's earlier domain model. Active Directory's hierarchical nature allowed administrators a built-in way to manage user and computer policies and user accounts, and to automatically deploy programs and updates with a greater degree of scalability and centralization than provided in previous Windows versions at this point. Active Directory services could always be installed on a Windows 2000 Server, Advanced Server, or Datacenter but couldn't be installed on a Windows 2000 Professional computer. However, Windows 2000 Professional is the first client operating system able to exploit Active Directory's new features.

HIPAA — AUGUST 21, 1996

The Health Insurance Portability and Accountability Act, focused on health information was created to modernize the flow of information and to provide protections to PPI or Personally Indefinable Information. So while this may not be focused very much on cyber security, this does however play a huge part in healthcare IT and becomes an IT concern for nay vender who works with healthcare information. Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry. At the same time, new technologies were evolving, and the health care industry began to move away from paper processes and rely more heavily on the use of electronic information systems to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions.

CYBER SECURITY DEFENSIVE PROTOCOL

WHAT YOU DON'T SEE CAN HURT YOU

Scripts rule the internet. Very rarely does a website run only a single source, whereas most run scripts from the big names of Google Facebook, Twitter, as well as numerous third party services that are unrecognizable. All of this passes unnoticed by the casual user, happening seamlessly behind the scenes of a streamlined webpage design.

Hidden amongst all of these mostly innocuous contributors to a website's interface are scripts that range from privacy violating to outright harmful: Data analytic services that track, log and sell your internet habits to drive-by malware.

Enter NoScript. A free, open source extension for Firefox and other Mozilla-based browsers. Without inhibiting your browsing experience, it preemptively blocks scripts and prevents the exploitation of security vulnerabilities (known and unknown), as well as aforementioned activity that invade privacy.

Its simple interface allows for the user to 'whitelist' trusted websites, as well as plug-ins such as JavaScript and Flash only on trusted websites (your bank's webpage, or when you're renewing your FAFSA application). Not only is it widely lauded by everyone from PC World, to Edward Snowden, to the SANS Institute.

DO THIS ATTACK IN
CYBV 479

WIFI DEAUTHER 1/2

First making an appearance a few years ago from a small maker in China, this item circulated among hacking circles with little broad spread use. That is, until it began being noticed in certain circles on social media about a year ago, and a few months ago it received broad attention.

A deauther (deauthorizer) is a small device that exploits the IEEE 802.11 Wi-Fi protocol, a weakness that allows an unauthorized device to send deauthentication frames to a specific MAC address. This frame is sent to the access point and terminates the connection of the client device, and the MAC address can be found via wireless network sniffing. Once 'deauthed' or kicked off the network, the device continues to send out deauthentication frames for any desired period of time, preventing reconnection.

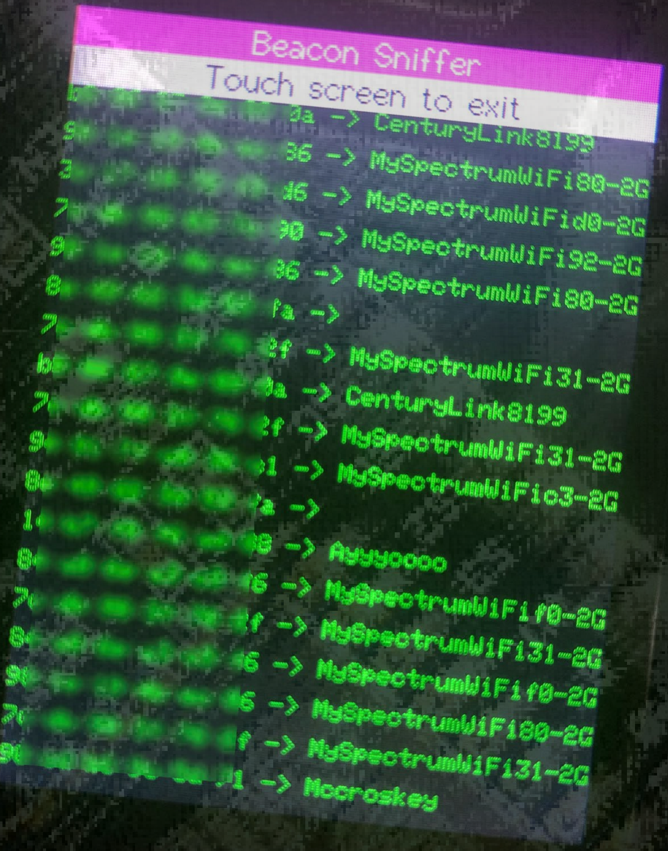
LOOK!

IF YOU ARE GOING TO DO ANY TYPE OF WIFI DEAUTHING OUT IN THE WILD YOU ARE OPENING YOURSELF UP TO LIABILITY. DO THESE TYPES OF ATTACKS ON YOUR OWN NETWORK THAT YOU CONTROL AS MESSING WITH A PUBLIC OR PRIVATE NETWORK WILL GET THE ATTENTION OF MANY GOVERNMENT AGENCIES AND THEY WILL MAKE YOUR LIFE DIFFICULT. LEARN AND UNDERSTAND BUT DON'T TOUCH!

BOLO LIST

WIFI DEAUTHER 2/2

This type of denial-of-service attack is not new. It can be easily performed in the Aircrack-ng suite. What is new - and what raises a concern - is this type of attack being proliferated in the form of a cheap and simple to use device.



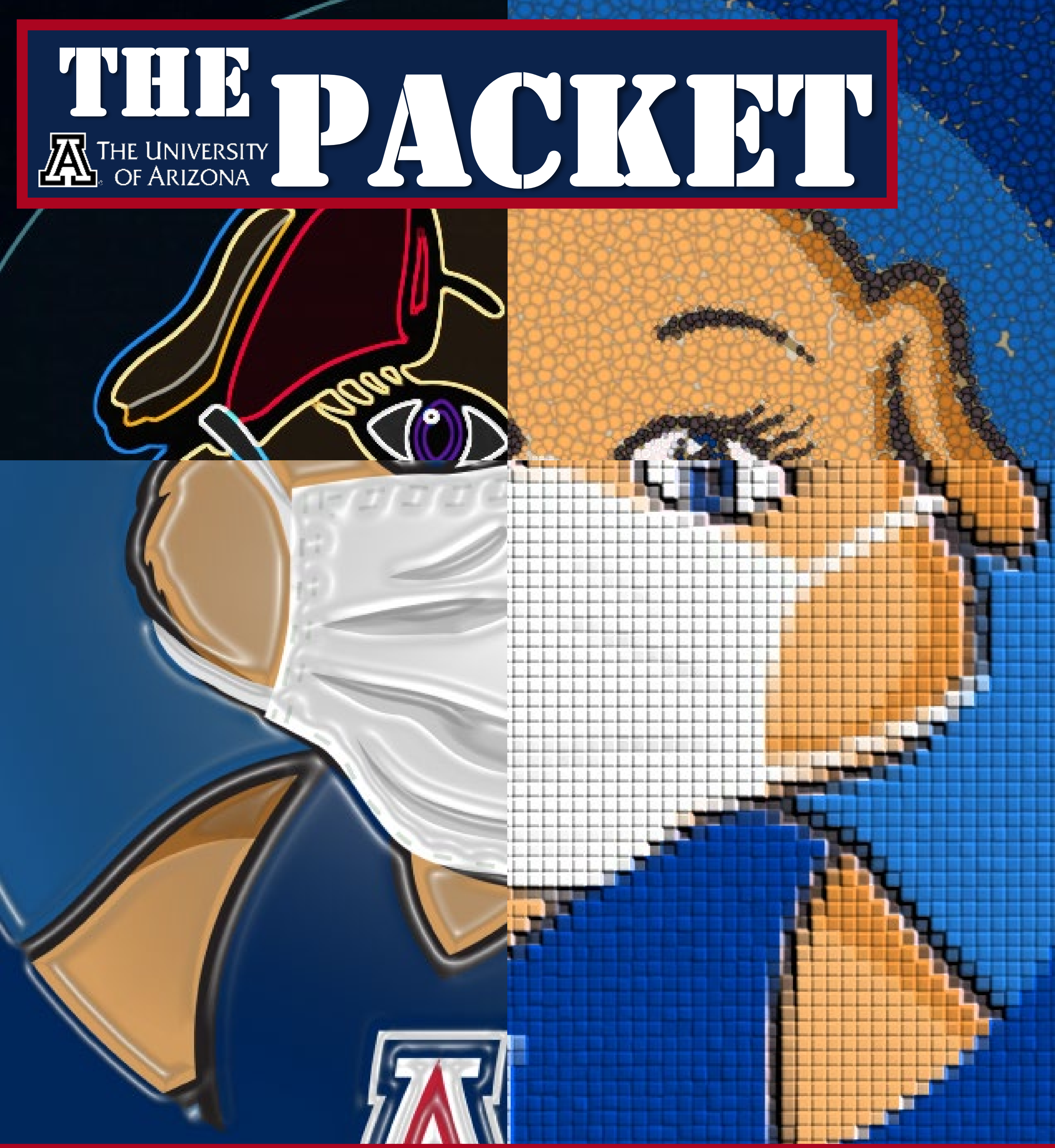
```
Beacon Sniffer
Touch screen to exit
a -> CenturyLink8199
36 -> MySpectrumWiFi80-2G
d6 -> MySpectrumWiFid0-2G
90 -> MySpectrumWiFi92-2G
36 -> MySpectrumWiFi80-2G
fa ->
2f -> MySpectrumWiFi31-2G
a -> CenturyLink8199
2f -> MySpectrumWiFi31-2G
1 -> MySpectrumWiFio3-2G
a ->
8 -> Ayyyoooo
6 -> MySpectrumWiFif0-2G
f -> MySpectrumWiFi31-2G
6 -> MySpectrumWiFif0-2G
6 -> MySpectrumWiFi80-2G
f -> MySpectrumWiFi31-2G
1 -> Mccroskey
```

Beyond the deauth attack, many of these devices are also capable of spamming beacon packets under the guise of Wi-Fi networks - even allowing for specification of network names under SSIDs - making it extremely difficult to sort through network lists and find the real network(s) in order to reconnect.

The security implication? Alarms, security cameras, and other IoT devices that depend on a stable Wi-Fi connection in order to fulfill their role are all vulnerable to this type of attack.

THE PACKET

THE UNIVERSITY OF ARIZONA



CONTACT US

CIIO@EMAIL.ARIZONA.EDU

1140 N. Colombo Ave. | Sierra Vista, AZ 85635

Phone: 520-458-8278 ext 2155

http://cyber-operations.azcast.arizona.edu/

THE UNIVERSITY OF ARIZONA