Security, the Internet, Failure to Learn Lessons, and Forming an Unstoppable Voltron of Bad Decisions

Mike Kershaw
mike@kismetwireless.net
Proving Sadness With Math

- Security is terrible
- The Internet is terrible
- People are terrible
- People use the Internet
- Everything is on the Internet now
- By the transitive property, everything is terrible.

- But we have funny pictures from the Internet to make you feel less bad about it.
- So... who remembers Voltron?
I Liked Transformers Tho...

- Voltron is a bunch of crummy lion robots
- (Look, it was the 80s, we had toys to sell here people.)
- The lions always get their butts kicked
- Then they team up to make Voltron, the unstoppable giant robot of doom that stomps the aliens
- I think we were supposed to learn teamwork is important?
- How about, when enough little problems gang up, they’re almost unbeatable?
How Does A Company Get Owned

- Maybe it’s a bug in their web app
- Is it in their own code? Were they just sloppy?
- Is it in Apache/Ngnx/IIS/Other core service?
- Is it a fundamental bug in PHP/Ruby/Etc?
- Is it in the database API?
- Is it in the *bash* interpreter?
- Is it in OpenSSL?
Maybe Not The Server At All

- Maybe an employee got infected on a bad Wi-Fi network
- Or visited an ... exciting ... site at work and got hit with a browser bug
- Maybe they’re important enough to be interesting to a foreign government looking to collect data and were hit with a targeted attack?
- Maybe they’re not important, but got owned anyhow because any data has value?
- Maybe it’s ransomware looking to extort money?
Maybe Email?

- Maybe it was a bulk phishing attempt
- Maybe it was a targeted phishing attempt
- Bug in PDF?
- Bug in Word?
- Bug in the browser via E-Mail?
- How do you even know?
- Or maybe one of their employees used the same password at work and on a public site
- Like a dating site
- Or a “dating” site
- And their work email
- How many .gov and .mil addresses were in the Ashley Madison dump?
- Look, people are dumb
- Some hacks are still curious kids exploring
- Not a bet you can make anymore
- There’s a lot of money in crime
- Calling it “cyber” crime and “cyber” theft doesn’t mean it’s not the same people behind it as, you know, crime.
Passwords for 32M Twitter accounts may have been hacked and leaked

Posted Jun 8, 2016 by Catherine Shu (@catherineshu), Kate Conger (@kateconger)
TeamViewer confirms number of abused user accounts is “significant”
Investigation continues to show external password breaches are cause, spokesman says.

by Dan Goodin - Jun 5, 2016 6:06pm EDT
Target will pay hack victims $10 million

by Charles Riley and Jose Pagliery  @CNNTech

March 19, 2015: 3:05 PM ET
Heartland Payment Systems, the sixth-largest payments processor in the U.S., announced Monday that its processing systems were breached in 2008, exposing an undetermined number of consumers to potential fraud. Meanwhile, Forcht Bank, one of the 10 largest banks in Kentucky, told its customers it would begin reissuing 8,500 debit cards after being informed by its own card processor of a possible breach.
Internet-connected Hello Barbie doll can be hacked

The iconic toy becomes a connected device, and promptly gets pegged for security issues.
Five Lessons On The 'Security Of Things' From The Jeep Cherokee Hack

Last week, Wired published an account describing how two security researchers, Charlie Miller and Chris Valasek, were able to wirelessly hack into a Jeep Cherokee, first taking control of the entertainment system and windshield wipers, and then disabling the accelerator. Andy Greenberg, the Wired writer who was at the wheel as the self-described “digital crash test dummy” explained what happened next:
How Did We Get Here

- How did things get this bad?
We Have A History

- We have a history of sucking at security.
- We sucked at it in the 80s
- We sucked at it in the 90s
- We sucked at it in the 00s? Naughties? Aughts? … The 2000s. We sucked at it then.
- Do you think we suddenly learned how to do security properly in 2016? Of course we didn’t. That’s a silly idea.
The 80’s

- We didn’t know security, but we knew how to rock.
- Encryption was computationally expensive, weakened by the government export rules
- Telnet was good enough for everyone
- RSH seemed like a real good idea. Just set what hostnames are allowed! That’s great! (hint: usually ‘*’)
- Shared-media Ethernet (or TokenRing if you were really special)
The 90’s

- Switched networks are a good thing
- Encryption is still difficult and regulated.
- Who remembers the export-legal versions of Netscape?
- SSL happens, sometimes
- SSH happens, sometimes
- Dial-up still sucks, but it sucks at 56k
- How many floppies is that update?
I tried to come up with something funny about the 2000s but failed.

TokenRing went away, mostly, unless you work at IBM.

Windows XP, the One True Windows version
- We understand encryption? I guess?
- Encryption is still really hard to do right. And we very often do it completely wrong.
- Now we’re starting a whole new war on regulating it
- Guess what Wi-Fi is? Shared media networking again.
- **Everything** is a computer.
- How do I update my light bulbs?
- *Why* do I have to update my light bulbs.
My Favorite Topic!

- You’ve probably heard this before
- You may have even heard me talk about this before
- Just because it’s old doesn’t mean we’ve gotten smarter
Wi-Fi Is Like Time Travel

- Using Wi-Fi is a lot like going back in time to the 80s
MEAN Time Travel

- Except it’s not hippy friendly time travel
- You get to bring back all the advanced modern attacks and weaponry
Shared Media

- Open Wi-Fi networks are shared media
- Like, an Ethernet hub.
- What protects you from your fellow users on Wi-Fi?
- **Basically Nothing**
- Sniffing, injecting, sequence number guessing, hijacking the router, ARP poisoning…
- Let's party like it's 1993!
Hijacking A Client The Old-School Way

- What protects a TCP connection from stream hijacking?
- Sequence and Ack numbers
- What can we see for every connection on open Wi-Fi?
- *Seq/Ack*
- What uses a lot of unencrypted connections and loads arbitrary content?
Hijack Browser

- Trivial to hijack the browser
- Inject malicious code into browser sessions while user is on open network
- Set cache controls to keep the hostile page saved forever
- Trigger exploit when victim goes back to their company and loads the page again
- All the corporate defenses are useless when the victim brings it in as a cached page
WEP - It’s Like Encryption, But Not

- Let’s make fun of WEP! (Again!) (Always!)
- It’s like they read how to misuse an algorithm
- And specifically implemented it to expose every possible flaw.
- So do we still have to talk about WEP?
- Yep. Because what uses WEP? Stuff that hasn’t been updated in the last decade.
- What doesn’t get updated?
You Can’t Fix Everything

- What can’t get updated?
- Stuff in planes. Probably bad.
- Power plants. Probably bad.
- Rando core infrastructure. Probably bad.
- Medical equipment. Really bad.
Worst Email I’ve Ever Gotten

“Customer needs assistance connecting an IV Drug Pump to a WEP network.”
But I’m fine”, I claim to hear you say, for the sake of a clever presentation. “MY coffee shop uses WPA!”

What do you need to know to impersonate a network?
1. The SSID
2. The WPA key

Where could we ever find the WPA key?

Oh right. That wall over there has it.

This even happens at hard-core security conferences, and it’s hilarious to me.
Open Wi-Fi?

- Open Wi-Fi is a cesspool of other people’s infected machines
- WPA with a public key is basically Open Wi-Fi
- In the *best* case
- Worst case? Actively hostile network attempts to compromise your traffic and your system
- Especially at airports (where business people travel), conferences (where people take work laptops), etc
- How about in-flight Wi-Fi?
But Who Would Use Open Wi-Fi

- But who would blindly use open Wi-Fi at this point?
- Your phone
- All the time
- *All* the time
- More than happy to connect to any open Wi-Fi network with a name you’ve connected to before
- Sometimes even networks you’ve never used deliberately (pre-loaded like ATTWifi)
Impersonating Networks

- Same fun attack as a decade ago
- Wi-Fi never changes
- “Karma” attack
- Probe contains network you want to join
- “Yes, of course I’m that network. I’m also that network over there, and that one, and the fourth one, too. Please talk to me. I’m so lonely.”
No Way To Know

- Not entirely the clients fault
- How do you know what’s legit?
- A network is a name (ESSID)
- And the encryption options (usually Open)
- Any network with the same ESSID is considered to be the same network
Now I Control Your Traffic

- Once someone gets you to connect to their AP…
- They control your routing
- They control your DNS
- They control your ports
- They see all unencrypted traffic
- They see encrypted traffic, and you hope they can’t do anything about that
- They are, basically, your ISP
What’s So Bad?

- Your phone is an embedded computer
- “Embedded.” Android is Linux. You can put bash on it. It’s a Linux PC that’s always online. iOS is based on BSD.
- And it knows where you are
- And who you talk to
- And shows you content (like ads) …
  … From random sources and networks.
Let’s Make Fun Of Phones!

- I used to work for a company making Android phones
- My preferred platform is Android
- I still love to make fun of Android
- Android vs Apple is a political argument
- That said, Apple probably does more things right for security right now, if you had to pick on that alone
Vulnerabilities Gonna Vuln

- Everyone is going to have vulnerabilities
- Everyone
- Everyone is going to have high profile device killing and crippling vulnerabilities
- The real question is, what happens when the poop hits the fan
How Do You Fix It

- So someone just found a crippling vulnerability in your phone OS
- Let’s say, one that you can trigger with manipulated traffic
- Examples:
  IOS: root from web (rootmyiphone.com)
  Android: Arbitrary code execution from JS, Stagefright
Doing It Right

- Apple releases updates universally to all iPhone devices (unless your device is too old. Of course you have $800 burning a hole in your pocket, right?)
- Google releases updates to the Nexus phones worldwide
- Google releases fixes to partner companies
- Finally, Google updates the AOSP source code repo if the exploit is in public code
Doing It Wrong

- Every Android vendor has to patch their own device
- Every vendor typically makes 4 to 10 devices per year
- Each device typically has a 200 person team
- Each device has custom kernel and userspace modifications on top of stock Android
- Plus vendors love to re-skin the entire device to encourage user lock-in
- Do you think they keep 1000-2000 developers around for the 2-4 year lifespan of 15-40 devices?
- No, they don’t
- Which means they have to go take people off a new phone dev cycle
- Find the old code
- Find the old build environment
- Backport the fixes
- Decide this is all worth losing money by not telling the user to just buy new HW
- At least it’s fixed!
Now Wait Another 6 Months

- Basically any phone sold direct from a carrier (except iPhone, because Apple is a pretty pretty princess with a really big baseball bat with nails in it) has carrier-controlled firmware
- Carrier controls OTAs
- Stocks their adware and crapware and custom apps
- Have their own homologation and approval process
- Can take 6 months or more
So a critical bug, like say, sending someone a malicious SMS can execute code (like, Stagefright?) hits
- Public patches land showing exactly how to execute it (nothing better for reversing an exploit than a patch)
- 6 months later, some phones get an update. The rest might in another 2 or 3 months.
- Most phones see one or two updates, ever
- Even fewer see an upgrade to the latest OS revision
Baby Steps

- Google knows this is a terrible problem
- Fixing it by taking power away from carriers and phone vendors, naming and shaming, and splitting up the codebase
- Android 5 makes web browser core updateable, Android 6 revamps permissions and makes other core components updateable
- Too bad only about 8% of devices have Android 6 after almost a year.
Who Has The June Update?

- Google just dropped the June update last week
- Who has it yet?
- How important is it?
<table>
<thead>
<tr>
<th>Issue</th>
<th>CVE</th>
<th>Severity</th>
<th>Affects Nexus?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Code Execution Vulnerability in Mediaserver</td>
<td>CVE-2016-2463</td>
<td>Critical</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Code Execution Vulnerabilities in libwebm</td>
<td>CVE-2016-2464</td>
<td>Critical</td>
<td>Yes</td>
</tr>
<tr>
<td>Elevation of Privilege Vulnerability in Qualcomm Video Driver</td>
<td>CVE-2016-2465</td>
<td>Critical</td>
<td>Yes</td>
</tr>
<tr>
<td>Elevation of Privilege Vulnerability in Qualcomm Sound Driver</td>
<td>CVE-2016-2466 CVE-2016-2467</td>
<td>Critical</td>
<td>Yes</td>
</tr>
<tr>
<td>Elevation of Privilege Vulnerability in Qualcomm GPU Driver</td>
<td>CVE-2016-2468 CVE-2016-2062</td>
<td>Critical</td>
<td>Yes</td>
</tr>
<tr>
<td>Elevation of Privilege Vulnerability in Qualcomm Wi-Fi Driver</td>
<td>CVE-2016-2474</td>
<td>Critical</td>
<td>Yes</td>
</tr>
<tr>
<td>Elevation of Privilege Vulnerability in Broadcom Wi-Fi Driver</td>
<td>CVE-2016-2475</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td>Elevation of Privilege Vulnerability in Qualcomm Sound Driver</td>
<td>CVE-2016-2066 CVE-2016-2469</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td>Elevation of Privilege Vulnerability in Mediaserver</td>
<td>CVE-2016-2476 CVE-2016-2477</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td>Vulnerability Description</td>
<td>CVE Numbers</td>
<td>Severity</td>
<td>Detected</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>----------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>Elevation of Privilege Vulnerability in Qualcomm Camera Driver</td>
<td>CVE-2016-2061</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CVE-2016-2488</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Elevation of Privilege Vulnerability in Qualcomm Video Driver</td>
<td>CVE-2016-2489</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td>Elevation of Privilege Vulnerability in NVIDIA Camera Driver</td>
<td>CVE-2016-2490</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CVE-2016-2491</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Elevation of Privilege Vulnerability in Qualcomm Wi-Fi Driver</td>
<td>CVE-2016-2470</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CVE-2016-2471</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-2472</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-2473</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Elevation of Privilege Vulnerability in MediaTek Power Management Driver</td>
<td>CVE-2016-2492</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td>Elevation of Privilege Vulnerability in SD Card Emulation Layer</td>
<td>CVE-2016-2494</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td>Elevation of Privilege Vulnerability in Broadcom Wi-Fi Driver</td>
<td>CVE-2016-2493</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Denial of Service Vulnerability in Mediaserver</td>
<td>CVE-2016-2495</td>
<td>High</td>
<td>Yes</td>
</tr>
</tbody>
</table>
And This Isn’t Even The Problem

- This isn’t even the real problem
- You’re going to have vulns
- These are the ones that were reported and fixed
- Never mind the ones that aren’t disclosed
- The real problem is that everyone in the room doesn’t have this fix already
- And a significant percentage never will
- If you don’t have a Nexus or this years flagship, you may never see these fixes. Or next months. Etc.
What Else Can We Do To Phones?

- Ads use webviews because it’s easy
- Webviews can connect javascript and native java
- Ads turn on the JS/Java bridge so they can scrape more info out of your phone. Because ad companies are lovely like that.
- Java has introspection
- Java can run native commands via System.exec()
- See where we’re going?
- Hijack an ad, run a command.
Open Wi-Fi

- So still think open Wi-Fi injecting malicious code into phones isn’t a big deal?
- Hard to tell how many malicious networks are actually out there
- Can snag a phone with a few packets
- Can poison existing HTTP sessions with a few packets
- Trivial to intercept an ad and wrap it in hostile JS
- Maybe some apps are fixed, but are all your apps fixed?
Updates Are Hard, Yo

- Yeah, I get it, updates are hard
- Not like a phone is by nature always online
- … Oh. But it is.
- It’s so bad that Congress is interviewing phone companies about their update processes
- Good thing we don’t have any other products which are online but even harder to update…
You Can’t Have A Nice Internet Of Things

- So, let's make fun of the Internet Of Things!
- This is why you can’t have nice things, ever
The low hanging easy targets are the nonsense products like IOT egg crates. Why does the Internet need to know how many eggs I have? Light bulbs are a little more interesting. But have you tried to buy a TV that doesn’t listen to the whole room? Why does a fridge run Android? How do you update this nonsense anyhow?
Security Bugs? In *My TV*?

- It’s more likely than you think!
- Smart TVs are just Android with a big screen, usually
- Android that doesn’t get a lot of updates
- And is always online
- And records what you say to try to listen to voice commands
- And sends it… somewhere… on the Internet
- All. The. Time.
Be careful what you say in front of your Samsung TV. It's listening to you.

Many Samsung "SmartTVs" come equipped with voice recognition, which allows you to bark commands at your TV. Since the television is always listening for your voice, Samsung has warned its SmartTV customers that every word is being captured and sent over the Internet.

"Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition," Samsung posted in its SmartTV privacy policy.
LAS VEGAS — The next time you watch something on your Smart TV, beware, the television might be watching you too.

As in turns out, just like smartphones, Smart TVs can be hacked and compromised. On Thursday, at the Black Hat security conference, researchers Aaron Grattafiori and Josh Yavor demonstrated how they found vulnerabilities in different 2012 models of Samsung Smart TVs that allowed them to turn on the camera, take control of social media apps like Facebook or Skype, and access files and basically any app on the set.

SEE ALSO: How Hackers Can Turn Your Android Into A SpyPhone

“Because the TV only has a single user,” Grattafiori explained to Mashable, “any type of compromise into an application or into Smart Hub, which is the operating system — the smarts of the TV — has the same permission as every user, which is, you can do everything and anything.”
This Could Be You

- Think you’re not a target?
- Work for a tech company?
- Have a government clearance?
- Everyone with a clearance already has had all their info stolen via the OPM hack
- Ever bring work home?
- Maybe it’s a real threat. Maybe it’s time for a tin foil hat. Don’t use aluminum. That’s how they get you. Has to be tin.
But Back To IOT

- Sorry, we were making fun of IOT.
- Wi-Fi is hard
  - More expensive to talk to
  - Requires more processing
  - Requires more battery
  - Harder to set up
- So we’ll use our own protocol!
- Now we have z-wave. And zigbee. And wink. And brillo. And apple home. And random ISM radio. And…
- And then they bridge to Wi-Fi anyhow!
No-One Wants To Interoperate

- The IOT market is a bunch of balkanized one-offs
- Nothing works with anything else
- Deliberately - why have a way for someone to pick something that isn’t your product and accessories?
- No central repository of expertise
- No institutional understanding of security, and no institution to understand it
- Developing hardware like it’s a website with fast integration, only, it’s hardware, so it isn’t.
Race To The Bottom

- Consumer gadgets are cheap
- A $0.005 vs $0.01 component actually matters
- Do you think they’re going to do a very good job on security when they’re pumping these things out?
- Who wrote the software to connect to your phone/pc/fridge/child/dog
- Did they know what they were doing?
- Many companies getting into “Internet All The Things” aren’t tech companies at all
I’d Like To Wi-Fi My Car, Please?

```python
>>> def sendit(payload):
...     c=crc(payload)
...     s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
...     s.connect(("192.168.8.46",8080))
...     s.send(payload+c)
...     s.close()
...     time.sleep(10)
...
>>> alarmoff()
```

Internet of Shit @internetofshit · 3h
open wifi on a car
and this
bbc.com/news/technology...
Michel Jansen
@dawuss

The manufacturer performed a software update on my engine. It has a bug. There is no fix yet.
#welcometotheffuture
Defending Against Physical

- Another problem is defending from physical attackers
- If you store your key in your device, someone will find it, eventually
- Things like gaming consoles use expensive dedicated TPM devices to protect signing keys to authenticate data
- Your lightbulb wasn’t designed by Microsoft or Sony.

- 9F 55 95 F1 02 57 C8 A4 69 CB F4 2B C9 3F EE 31
Consumer Un-Friendly

- IOT is so new it’s mostly young companies
- Who have a habit of not sticking around
- How often do you change major appliances in your house?
- Tech moves fast. Appliances and cars do not.
- So what happens in 3 years if WPA gets cracked and your dishwasher, fridge, and toilet have to be replaced?
- Or the company shuts down the servers required to use them because it’s no longer profitable?
Nest is permanently disabling the Revolv smart home hub

Starting May 15th, the Revolv hub and app won't work

By Nick Statt on April 4, 2016 03:40 pm  Email  @nickstatt
DMCA To The Non-Rescue

- Maybe someone will hack a custom firmware
- Not that this helps anyone but the geeks
- Except you can’t, because it’s all locked behind DRM
- And the DMCA says you can’t hack that even when the company goes out of business
- So we’re stuck with insecure stuff, in our houses, on the Internet.
- Well, until it stops working.
- Great!
More Than Home

- Let’s be honest, messing with the lights in someone's home is obnoxious
- But it’s probably not the end of the world
- … Unless, of course, someone figures out how to make a worm that shuts down the heat in every house using some popular home thermostat… err…
- But, do you think that industrial systems are any more secure?
The Worst Of All Options

- Industrial control systems don’t typically update
- Power plants still run Win 3.1. Or 95. Or XP. Whatever was around when they were built.
- Would you be willing to explain why the metropolitan power grid went down when you updated Win2k?
- Assuming it’s even possible to update the systems and they aren’t linked to specific behavior of deprecated platforms!
But They’re Not Online

- But it’s fine! They’re not online!
- Until someone decides they need to add Wi-Fi to display something on a tablet
- Or the new cabling guys come in and neaten up the old network and consolidate
- Or they just set up VNC on the control PCs
- Or they’re just ignorant / lazy / dumb
There’s A Search Engine

- There’s a search engine for control systems
- And webcams
- And security systems
- And baby monitors
- And elevators
- http://shodan.io
The Internet Of Industry
Bad People Doing Bad Things

- Bad people wanting to do bad things don’t even need a password for some critical systems.
- Bored people looking to troll don’t even need a password.
- So how easy is it for a targeted attacker who wants to cause some malicious trouble?
- This can’t be good.
Infinite Monkeys, Typewriters, Etc

- Municipal control gear
- Smart meters
- Smart power grid controls
- All of this stuff sits outside a building somewhere
- Or on a customer’s property
- Nearly infinite time to attack the devices because no-one is watching them
The Problem With Trust

- When you have no power and can’t be online all the time, how do you know who to trust?
- There’s a lot of wrong ways to do it, that’s for sure
Lets Make Fun Of Parking Meters

- Smart card parking meters are a good example of doing it wrong
- Parking meter has no idea what’s going on
- All the trust is in the card.
- The card the user takes home and can poke at
- The card that the meter can’t validate because it doesn’t have a live connection
Look At The Protocol

Meter: What is your region?
Card: “Oh, I’m region 1234.”
Meter: Great, what’s your ID?
Card: “ABCDE”
Meter: Fantastic! Is “abracadabra” your password?
Card: “Sure is, pal! And I’ve got $1000”
Meter: You should take away $0.50
Card: “I’ll get right on that, sure. No worries. Absolutely.”
- This means all the trust is in the card
- The card is expected to compute the password
- This means the attacker controls the entire mechanism of verification
- Don’t even have to know what the password algorithm is, just always say yes
- There are/were thousands of meters using the same protocol across the US
Well, Let's Just Use Crypto

- OK. Sure.
- What crypto?
- How do you provision keys?
- Who controls your root of trust?
- How long is a key/cert valid for?
- How do you update a key later?
- If you’re not online, how do you validate that trust?
- How do you revoke trust if something goes wrong?
Randomness

- Basically two ways to connect a device to a network
  1. Embed the key in the device at manufacture.
  2. Create a process where a new key is negotiated as a device joins the network
- Neither is without flaws
- Both require random data to build a session key
- Being random is hard
Embedded Keys

- Many ways to extract embedded keys
- Access any standard flash chips, SD cards, etc that may be in the device
- Disassemble firmware update
- Glitch CPU to image firmware and disassemble
- Snoop physical connection between CPU and Radio
Isn’t That Hard?

- Isn’t sniffing hardware... hard to do?
- Well, even if it was, would that really stop someone?
- But it isn’t.
- $30 in hardware, free software
- Documentation for nearly all microcontrollers readily available
Sniffing SPI data with Bus Pirate

Posted on Sunday, February 12th, 2012 in Bus Pirate, how-to, MSP430 by the machinegeek

Greg Whitmore at Four-Three-Oh forum has written a quick how-to post on using the Bus Pirate to sniff SPI data on the MSP430. We’re reproducing the post here in its entirety with Greg’s permission.
Crypto relies on there being a source of randomness which is unguessable.

- Often provided on a PC by user input, disk I/O, and RNG in the CPU.
- Your lightbulb and toothbrush won’t have these, neither will industrial control gear or lightweight sensors.
- Maybe sample some sort of sensor to generate randomness?
- So maybe we can sample the radio for power levels. That’s kind of random, right?
- What happens if you put it inside a faraday cage with no radio signals?
- Make your random seed 0?
- Predictable crypto keys
- Can expose comms, allow control of network, etc
All Of This Has Happened Before

- This isn’t even far fetched
- In 2006 Debian made some changes to the OpenSSL code because it looked like it was using uninitialized memory
- This meant the entire source of randomness for nearly all crypto options was the process id
- ie 1-32767
- It was discovered in 2008. Two years later.
In The Meantime...

- Every SSL key generated by a Debian or Ubuntu system was guessable
- Every SSH server key
- Every SSH user key
- Session keys
- Usually in seconds
- It was so non-random it was possible to pre-compute every possible key the system would generate for SSH ahead of time
And The Beat Goes On

- Since session keys are guessable
- All data saved from those two years could be retroactively decrypted
- Good thing no-one was doing bulk data collection in the 2000s, right?
- All because of commenting out one line of code because it produced an error in a memory analysis tool
Can You Trust Your HW?

- But say you have a HW random number generator
- Can you even trust it?
- Where was the CPU made? Where is it used?
- If there’s money in attacking it, it’s being attacked
- Research shows it’s possible to remove nearly all entropy from a hardware RNG by manipulating the CPU manufacturing mask
- Long after validation, when no-one can see it
- Uh oh.
I Have The Power

- When you control the physical system all sorts of other things become available
- Closely monitor the CPU power consumption & use that to derive the encryption keys
- Or, just image the firmware off the chip by controlling the power
Yes? No.

- CPU boots
- Ask CPU for firmware access
- CPU says no
- This is controlled by setting a register
- What happens if you under-volt the CPU, at just the right time, so much that it can’t, electrically, lock the register?
- “Can I read the firmware?” “Yes”.

SharkFest ‘16 • Computer History Museum • June 13-16, 2016
- What if there is no flashable firmware, and it’s just in ROM?
- That can be even easier
- Decap the chip with nitric acid
- Photograph it under a microscope
- *Literally read the code from the transistors*
- People do this.
- For fun.
Not Just Fairy Tales

- Not just a tin foil hat fairy tale
- DECT cordless phone encryption cracked by imaging the ROM chips from a phone
- Extracted hard-coded encryption keys & the code for the encryption algorithm
Just A Matter Of Time

- If someone can control the entire environment of a device, cracking it is just a matter of determination and time.
- Resources help.
- Is it worth cracking a lightbulb? It is if you’re making a competing product or cloning it.
- Is it worth cracking a power meter network? That’s a good question.
Where Does All This Go, Anyhow?

- Wait... almost none of these things install a server in your house...
- So where does all your configuration data end up, anyhow?
- (And your power usage, times you're home, info about your TV shows, how often you brush your teeth, where in the yard your dog is...)
- I guess it goes in the cloud?
- Everyone loves The Cloud!
- The cloud is magical! It’s where Netflix lives! It’s got infinite capacity and processing!
- But really, it’s just computers
- Other peoples computers
- Somewhere else
- So...
Cloud + Security

- Anything you do in the cloud is only as trustworthy as the people owning the computers
- And their company
- And their government

- And their security.
- Hypervisors are great
- And as we’ve learned, security is *real easy* right?
- Of course there are bugs in the virtualization space
- Bugs in VMs can be really bad since they hit more than one server
I See What You’re Doing There

- Lets accept for the sake of argument that the hypervisor is good enough that client “A” can’t look at what client “B” is doing
- The hypervisor still can
- So… your crypto keys, your SSL private keys, your customer data, your database passwords, anything you compute/operate on in memory
- This doesn’t even need a bug, just a bad operator
- Boy that’s a lot of trust for $15/mo…
Physical Attacks - Again!

- Latest “fun” is the Row Hammer attack
- Attacks the physical architecture of DDR4 RAM allowing processes to gain admin/root
- From a physical flaw in how RAM functions.

... FROM JAVASCRIPT
Ram Is Tiny

- RAM is rows and columns addressed as a matrix
- Memory is really tiny and packed really close
- By flipping the contents of RAM rapidly it’s possible to cause errors to occur in adjacent rows due to electrical fluctuations
- Possible to tune these errors to cause RAM to change in areas completely outside of your program’s normal control
- Actually proven to work. It’s amazing.
ECC? We Don’t Need No ECC

- But servers use error-correcting RAM, don’t they?
- Yep, but it doesn’t solve the problem
- Attacks proven against ECC, too
- It gets even worse on virtual machines!
- To save memory, hypervisors perform page de-duplication
- If two (or more) pages of RAM are identical, they’re compressed into a single page and referenced from multiple locations
- Things like glibc, kernel memory, etc end up in de-duped pages
One Page To Rule Them All

- Normally de-duped pages are read-only
- By finding de-duped pages via timing and page faults, specifically target pages of memory which are shared
- Modify a non-writeable page by corrupting it via attacks on adjacent rows
- Modify all VMs sharing that page
- ... Uh oh.
Can You Solve A Physical Bug?

- Some attempts remove the instructions in the JS VM that perform the rowhammer
- Try to profile memory access and stop programs that are exploiting it
- BIOS updates that change how memory refreshes are performed
- Hope there isn’t a new variant that bypasses these stopgap fixes once millions of machines are (maybe) updated
We’ll Just Use Open Source

- But most virtual hosting systems run Linux
- And Linux is open source
- And open source prevents security bugs, right?
Even Open Source Has Bugs

- The lesson here: *Everything has bugs*
- What matters is *being able to respond to them*
- Open source *may* be better at responding to them
- ...
- But not always
- There’s many layers between an update and end users
- Servers can still be out of date
- Bugs may go unreported or (publicly) undiscovered
Bugs Have Value

- Part of the problem is vulns have value now
- There are marketplaces for vulns
- Buyers can be criminals, or governments, or both
- Vulnerabilities can be worth thousands or even millions of dollars
- That’s a lot of incentive to keep and sell it privately
Somebody Just Claimed a $1 Million Bounty for Hacking the iPhone

November 2, 2015 // 01:36 PM EST

Apple devices are widely considered extremely secure and hard to hack. But as the internet adage says, everything can be hacked—even the new iPhone.

Over the weekend, somebody claimed the $1 million bounty set by the new startup Zerodium, according to its founder Chaouki Bekrar, a notorious merchant of unknown, or zero-day, vulnerabilities.
Why Are They Worth Money?

- Valuable to criminals for installing malware
- Valuable to governments for the same reason (or if you want to be charitable, for accessing devices legally)
- Valuable to security companies who use them during break-in tests or when reselling their services to companies or governments
It’s A Big Market

- It’s a big market
- Bigger than most people realize
- Escape from Chrome sandbox? $300k - $500k
- Still use Flash? $200k-$500k
- Windows remote exploit? $500k-$1m
- There’s real money out there changing hands for exploits that likely impact everything you do on the Internet
Why So Valuable?

- So you should be asking: Why are these so valuable
- What are the buyers doing with them?
- iOS jailbreak sold for $1m to Chinese firm
- Jailbreak software installed an alternate marketplace for Apps on every phone it was used on
- Presumably there was at least a million in revenue captured by selling apps outside of Apple
FBI paid more than $1.3 million to break into San Bernardino iPhone
The line between “project” and “product” is rapidly blurring
- OpenSSL is a project until recently maintained by one or two people
- But used in millions of *products* worldwide
Isn’t This Regulated, Somehow?

- Yes and no
- Legal regulations move slow
- And paint with a broad brush
- And are often fairly toothless
What’s An Exploit?

- Even if you think it should be regulated
- What’s an exploit?
- What’s research?
- Do laws stop criminals from doing something illegal, anyhow?
- Better to support finding flaws and fix them than not know the risks
Research, Research, Research

- There’s too much money for people to ignore vulnerabilities
- They’re going to be found
- And sold
- And used
- The ones you hear about which make it into patches are the success stories
- Someone, somewhere, just lost a lot of money when that got fixed
Have We Learned *Anything*?

- Have we managed to learn *ANYTHING*?
- Well, sort of...
Good: We’re A Little Less Afraid Of Bugs

- We’ve gotten a bit better about understanding that bugs happen
- Hackers aren’t *always* demonized for reporting bugs
- Many major companies have bug bounty programs and public vulnerability reporting
Bad: We suck at updating

- We’re still terrible at updates
- We’re networking devices for no reason
- There’s a lot of contention between security and government
- The 1980s crypto wars are upon us again
Bad: Stunt Hacking

- There seems to be a culture of “stunt hacking”
- High-profile bugs demonstrated in high-profile ways
- Don’t demonstrate hacking cars on a public highway
- Not every bug needs a cute name and logo
- You don’t need to hire a PR company for your bugs
Stunts Hurt Everyone

- Stunt hacking isn’t just obnoxious
- Everyone wants to make headlines
- Unfortunately headlines convince people that something Must Be Done
- And that Something may not be well considered
Legal Quagmire

- Govt wants access to data and devices
- People generally don’t want the government to access their data
- Government may or may not be accessing devices legally
- What defines legally?
- Whose government?
Doors Don’t Care

- Doors don’t care who opens them
- Put a hole in the system and anyone who finds it can use it
- This weakens it for everyone
- Many governments want back doors into all crypto systems
- But governments are so good at keeping secrets!
- And never get hacked, right?
First on CNN: Newly discovered hack has U.S. fearing foreign infiltration

By Evan Perez and Shimon Prokupecz, CNN

Updated 10:09 AM ET, Sat December 19, 2015
Hacking of Government Computers Exposed 21.5 Million People

By JULIE HIRSCHFELD DAVIS   JULY 9, 2015
Why the IRS Was Hacked Again and What the Feds Can Do About It

How can U.S. government agencies be better prepared to protect their sensitive data?

By The Conversation | Contributor Feb. 16, 2016, at 11:46 a.m.
FBI Says a Mysterious Hacking Group Has Had Access to US Govt Files for Years

April 4, 2016 // 03:43 PM EST

The feds warned that “a group of malicious cyber actors,” whom security experts believe to be the government-sponsored hacking group known as APT6, “have been using cyber tools that stem from the Chinese government to target U.S. government and critical U.S. infrastructure sectors.”
US government hack stole fingerprints of 5.6 million federal employees

Office of Personnel Management hack, which US believes China is responsible for, originally thought to have compromised prints of only 1.1 million workers.
- Clearly, these are the right people to decide to backdoor what security we have.
- It’s good.
- We’ve got this covered.
So...

- Security is hard
- We don’t really know how to do it
- No-one can stop products from being insecure
- Back-room dealing will always put preferred devices into play regardless of security
- We’re actively trying to make it worse
- We’re going to be stuck with bad security indefinitely
- Get off my lawn with your lightbulbs and your car updates and your... zzz...