Cyber Security Threats and Myths

Jay C. Daniel, CISSP – KG4DCI

TN ARRL ASM – Information Technology and Security

Traditional Attack Vectors

- Computer Viruses
- Worms
- 619 Email Scams
- Identity Theft
- Credit Card Numbers
- Man-in-the-Middle
- Malware
- Distributed Denial of Service (DDoS)
- Phishing Attacks

Traditional Protective Measures

- Anti-virus software
- Firewalls
- Software Signing
- UAC/Active Directory
- Passwords
- SSL/TLS
- Spam Filtering
- EV SSL Certs

The ‘Good Old Days’

If you think the Internet was the wild west before – look at where we’re at today.

Spear Phishing

- Much more targeted
- From your friends
- Subject and body look legit
- Masked or modified URL and links to familiar websites
- Clicking the link is all it takes
- Can fool even experienced users
- Spam filtering rarely works against these types of attacks

Look what I found – USB Drive

- Gifts on the ground? You bet!
- This works almost every time
- What's the worse that can happen? Bad, very bad - and about to get worse

Stuxnet – June 2010

- Can't put the genie back in the bottle
  - Used USB drives
  - Was supposed to be limited to certain networks
  - Escaped into the wild
- What did it target?
  - Targeted Windows computers
  - Siemens Step 7 Software
  - SCADA and PLC controlers
- What did it do?
  - Targeted Iran's Nuclear Program
    - Caused wild shifts in centrifuge motors while reading normal
    - Caused physical damage
    - Spread over the network, was hard to detect and remove
- Design Flaw
  - Escaped Iran
  - Decoded, code is now in the wild
  - Others are using the code

Heartbleed – April 2014

- SSL/TLS Private Keys compromised
- Passwords, and other private data also exposed
- Lots of stuff vulnerable – Windows, Linux, MacOS, Android, firewalls, VPN's, embedded devices
- OpenSSL is everywhere used in many different applications
- Client systems at risk if they visit a malicious web server
- Private keys are gold to hackers
- Costs a lot to replace, many haven't replaced their keys, have you?

Shellshock – September 2014

- Effects Linux and MacOS
- Remote arbitrage code exploit – very bad
- Lots of systems vulnerable
  - Consumer devices will never be fixed
  - Routers, Cable Modems, etc
- Web, SSH, DHCP, Email all vulnerable
- Very good chance this effects you, did you know?

You ain’t seen nothing yet

Be afraid, be very afraid… it gets much worse

BadUSB

- Every USB device has a micro controller – think Arduino
- Bad guys can modify the firmware on the USB device
- USB thumb drive that attaches virus code on the fly to every file you open
- USB device that pretends to be a keyboard and capture all your passwords
- Endless possibilities on bad things an attacker can do
- Defcon 2014 – researches did us a favor and released the code to the hackers ☺

BadBIOS – yes it is much worse

- What is a BIOS?
- So bad many people thought it was a hoax
- Blended threat that targets the operating system, BIOS, and USB devices
- Uses wireless, bluetooth, and when all else fails audio to jump air gaps
- Can't get rid of it… might as well toss the laptop

Ok, I'm scared. Now what?

How these types of threats are being used in the real world to attack systems today.

JP Morgan Chase attack

- 83 million households compromised
- Russian hackers with links to Putin's government
- Cyber warfare over Ukraine
- 10 other major financial firms also attacked
- Had access to systems for weeks or months
- Email addresses, usernames and passwords compromised – these will be used for follow on identify theft and spear phishing

China is constantly probing

- Military backed hackers attacking everyday
- Not limited to corporate networks, also targeting government and emergency services
- Placing backdoors in targeted equipment purchases
- Fake networking gear with special backdoors
- Risk to cell phone and other communication systems

Even Road Signs are Hackable

Cell Phones aren't safe either

- Fake towers all over the country
  - 18+ in Washington, DC alone
  - Others spread all over the country
  - Some could be government ran, but others clearly aren't
- Can monitor calls, text messages, and Internet usage
- Could be used to hack cell phones and compromise them long term
- Hackers can build this type of device for less than $1500

A look into the future

How hackers, terrorists and foreign governments can leverage these threats to attack us in the future.

Predicition

The first Internet murder will happen in the next 18 months – if it hasn't already happened.

Son of Stuxnet?

- Moving from cyber annoyance to kinetic threats
  - Power Plants & Grid – Don't forget nuclear
    - Already seeing attacks today – MetCal for example
  - Water treatment and flow control
  - Rail, airplanes, stop lights and electronic signs
    - Zombies?
  - Phone switches, and E911
    - SWATing - DDoS style
  - Hospital and healthcare
- People don't understand just how many vulnerable SCADA controllers are out there…

So what can we do?

The goal should be to mitigate threats, and segregate systems.

Bring your own device

- iPads, phones, tablets, oh my…
- People want to bring they own devices to work…
- No control… could be a major threat…
- How many people carry thumbs drives into the building everyday? Remember BadBIOS?
- If you're going to allow them, to keep separate from critical systems, don't allow them unfettered access

Keep things separate

- Backup communication systems shouldn't be on your production network
- Wifi should be separate from servers and work stations…
- BYOD should be kept separate from everything else

Buying it doesn’t solve the problem

- Buying cool toys, firewalls, IDS, centralized anti-virus… are all great
- All these tools need to be monitored and alerts need to be followed up every time
- Remember outbound traffic is just as import as inbound traffic

Home user – what can I do?

- Make sure all your embedded devices are up to date
- Think about splitting critical function… good firewalls don't come with wifi built it
- Virtual Machines are you friend – hardware is cheap today
  - VM for banking
- Think before you download please
- Got "always on" remote control? Get rid of it
  - Teamviewer, etc.

Cyber Security is easy…

But getting people to do the right thing is hard- it takes extra time, and is an inconvenience Resist the urge to cut corners.

Questions?