CMSC 426
Principles of Computer Security

Lecture 14

Ethics and Computer Security

Last Class We Covered

- Cryptanalytic attacks
  - Attack methods
  - Attack types
- Attack types
  - Ciphertext only
  - Known plaintext
  - Chosen plaintext
- Pseudorandom numbers

Any Questions from Last Time?

Today's Topics

- "Big" ethics questions and ideas

- Case studies
  - Let's Encrypt
  - Marcus Hutchins (WannaCry)
  - Hacking back
  - Responsible disclosure
    - Gray hat hacking
  - Apple encryption

Ethical Topics

"Big" Ethical Questions

- What do "right" and "wrong" mean?
- Who gets to decide what's right and wrong?
- How do/should those decisions be made?
- What should we do about things that are wrong?

- We won't be answering these today!

Based on slides by Dr. Cynthia Matuszek

Basic Ideas of Right and Wrong

- It's wrong to harm people
  - Physically, emotionally, financially…
- It's wrong to discriminate against people
- It's wrong to steal from people
- It's wrong to invade people's privacy
- It's wrong to be unfair to people

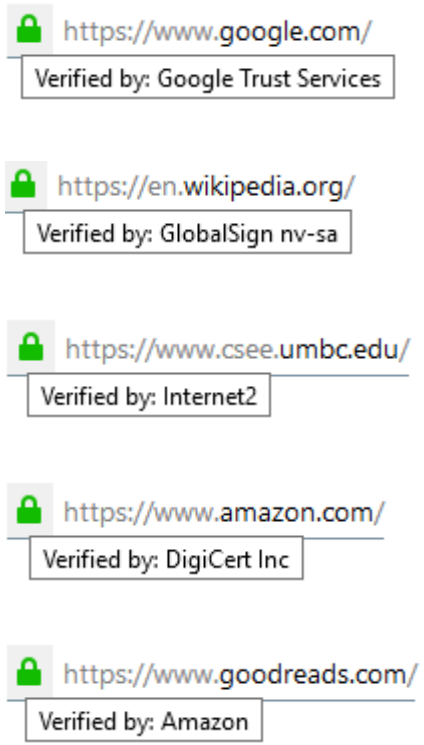
- We'll assume that these things are true…
  - Barring extenuating circumstances
  - And remembering that there's sometimes no "right" answer

Based on slides by Dr. Cynthia Matuszek

Let's Encrypt

Certificate Authorities

- Certificate authorities charge money to issue certificates used in Transport Layer Security (TLS)
  - Sometimes also called Secure Sockets Layer (SSL)
  - Prices vary, but typically $100 or more a year
- SSL/TLS certificates are used to enable secure HTTPS connections
  - Seems that if more websites could use HTTPS, the Web would be a safer place overall, right?



Let's Encrypt

- Let's Encrypt is a CA that issues free, renewable 90-day TLS/SSL certificates for Domain Validation (DV)
  - Guess who took advantage of these?

- In December 2015, criminals
  - Used issued certificates to…
  - Disguise malicious traffic to a website that…
  - Ran an exploit kit to…
  - Download a banking Trojan onto the user's computer

Information taken from https://blog.trendmicro.com/trendlabs-security-intelligence/lets-encrypt-now-being-abused-by-malvertisers/

Revocation of Certificates

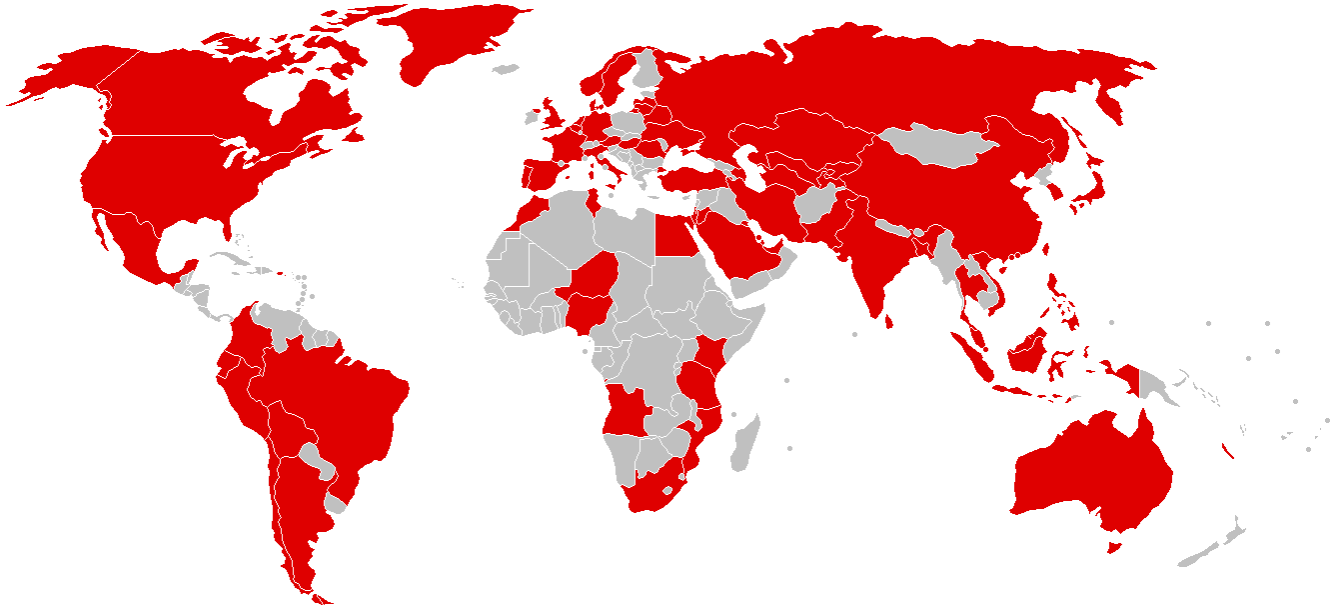
- Let's Encrypt does not revoke certificates for malicious sites
  - "A DV certificate […] says nothing about a site's content or who runs it"
  - "Users are much better informed and protected when browsers include anti-phishing and anti-malware features"
  - "On a philosophical and moral level, mistakes will mean censorship, since CAs would be gatekeepers for online speech and presence"
  - "CAs are not well positioned to operate anti-phishing and anti-malware operations – or to police content more generally"
  - "For the time being, Let's Encrypt is going to check with the Google Safe Browsing API before issuing certificates"

Information taken from https://letsencrypt.org/2015/10/29/phishing-and-malware.html

Marcus Hutchins (WannaCry)

Recap on WannaCry

- Propagated and spread as a worm (not a Trojan)
- Uses a leaked NSA-developed exploit to propagate
  - Exploit called “EternalBlue,” leaked by the Shadow Brokers
  - Windows released a patch in March 2017
- WannaCry was released worldwide in May 2017
  - Caused billions of dollars in losses and damages



Marcus's Exploits

- Authors the cybersecurity blog MalwareTech
- Discovered a "kill switch" for WannaCry after it struck in 2017
  - Code in WannaCry was linked to an unregistered domain name
  - Marcus registered it, and this stopped the worm from spreading

- Alleged to have created the Kronos malware in 2014
  - Kronos was sold via a darknet market for $7,000 in 2015

- How should past and current actions be weighed?

Information taken from https://krebsonsecurity.com/2017/09/who-is-marcus-hutchins/

Hacking Back

What is "Hacking Back"?

- Essentially, "attacking back" the computers/people that are currently or recently attacked a person or company
- Measures taken within the boundaries of one's own network are not normally counted as hacking back
  - Monitoring traffic patterns, encrypting data, using authentication
- Natural to want to "defend" yourself
  - Especially since law enforcement can't/won't help with malware
  - "Pay the ransom" is common advice

Information taken from http://www.slate.com/articles/technology/future_tense/2017/10/hacking_back_the_worst_idea_in_cybersecurity_rises_again.html

ACDC Legislation

- Stands for Active Cyber Defense Certainty Act
  - Introduced to House, referred to subcommittee in November 2017

- Would grant authorized entities the legal authority to venture outside their computer networks to
  1. Establish attribution (*i.e.*, nature, cause, source) of an attack
  2. Disrupt cyberattacks (without damaging other computer systems)
  3. Retrieve and destroy any files stolen during the course of an attack
  4. Monitor the behavior of an attacker
  5. Use “beaconing” technology

Information taken from https://www.cyberisk.biz/active-cyber-defense-certainty-act/

ACDC Legislation Breakdown

- "Only allows retaliatory action against computers based in U.S. territory"
  - Does this present any problems or limitations?
- Establish attribution (i.e., nature, cause, source) of an attack
  - How easy and/or accurate is it to do this?
- Disrupt cyberattacks (without damaging other computer systems)
  - How to prevent collateral damage caught in the crossfire?
- Retrieve and destroy any files stolen during the course of an attack
  - May taint forensic evidence at the scene of an attack
- Use "beaconing" technology
  - How is this meaningfully different from "creepware"?

Information taken from https://www.cyberisk.biz/active-cyber-defense-certainty-act/

Responsible Disclosure

Vulnerability Disclosure

- When white hat hackers or security researchers discover a vulnerability, what responsibilities do they have?

- Disclose the issue to the public so they know about it
  - "The public has a right to know"
  - Forces the vendor to address the issue
- Alert the vendor of the issue so they can fix it
  - But then the vendor is getting free security consultations
  - Is it ethical to expect/demand payment?
    - Some vendors offer "bug bounties" to incentivize detection and reporting

Responsible Disclosure

- Compromise between alerting the public and alerting the vendor
- Vendor is alerted first, and is given a period of time in which to fix and/or patch the vulnerability
  - Time that is granted is often negotiated, and depends on the possible impact, difficulty of fixing the issue, etc.
- After this time period, the vulnerability is released to the public
  - Including people who would take advantage of it

Google's Project Zero

- Project Zero is a full-time team dedicated to find zero-day vulnerabilities, including in non-Google products
  - Vulnerability is released after patch, or after a strict 90 days
  - To help with patching, a Proof of Concept is often provided to vendor

- Disclosed a Windows vulnerability two days before patch released
  - Patch was already scheduled for "Patch Tuesday"
  - Google released the PoC in code and executable form
  - Windows is one of Google's competitors
  - "Don't use vulnerable software" doesn't work for things like the Windows OS

Information taken from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2624411

Gray Hat Hacking

Mirai and Hajime Worms

- Mirai worm infects networked devices to added them to a botnet
  - Very widespread, infects things like routers and surveillance cameras

- Hajime is a more advanced worm in how it spreads, how it hides itself, and in how difficult it is to combat
  - Blocks access to ports 23, 5358, 5555, and 7547
  - Fetches and displays a statement on the terminal
  - Once infected, a system is… secured against Mirai infections

Information taken from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2624411

Analyzing Hajime Worm

- Spreads itself onto computers without permission
- Author can open a shell script to any infected machine in the network at any time
  - Hides its processes and files from the system
- Blocks access to ports
  - Closes ports vulnerable to the Mirai worm
- Doesn't perform DDoS or similar attacks (but could)

Apple Encryption

Background: San Bernardino Attack

- December 2015, a married couple perpetrated a terrorist attack consisting of a mass shooting and an attempted bombing

- Terrorists were killed in a shootout with the police
  - Personal phones were destroyed
- FBI recovered an iPhone used for work by one of the terrorists
  - Employee of San Bernardino, so phone actually owned by county
  - Unable to unlock the phone – would wipe data after 10 attempts
  - Requested help for NSA – unable to crack the phone

Information taken from https://en.wikipedia.org/wiki/2015_San_Bernardino_attack

Backdoor to Apple Security

- FBI requested Apple create software that would allow them to
  - Attempt multiple passwords with no added delay
  - Prevent the automatic deletion of data

- Apple declined, citing its policy to never undermine the security features of its products
  - FBI appealed: Apple could install the software in person, FBI would remote hack, then Apple could remove/destroy software
  - Request withdrawn after FBI paid a third party over 1 million dollars for use of a tool to bypass the ten-try limit

Information taken from https://en.wikipedia.org/wiki/FBI–Apple_encryption_dispute

Image Sources

- White hat:
  - https://pixabay.com/en/hat-white-fashion-male-man-308778/
- Black hat:
  - https://pixabay.com/en/fedora-hat-black-headwear-297371/
- Gray hat (adapted from):
  - https://pixabay.com/en/hat-red-fashion-male-man-308779/