Lecture 27: Wrap Up
Wrap Up
- Case studies
  * Authentication: OPM Hack
  * Transport: Poodle
  * Platform: PS3
  * Software: WannaCry
  * Privacy: U.S. Census

- What's next?

Logistics
* Final exam
  → Open laptop
  → No network

* Course evaluations

* Intro to Math Prog
* Efficient Deep Learning Computing
* Fields, Forces, & Flows
Plan for this class

- Five case studies, one from each module of the course

- Goals
  1. To show you that you really have learned something this semester?
  2. To show how class topics intersect with real world.
  3. To entertain you. 😊
Let's start off with an authentication failure...

Office of Personnel Mgmt. Hack: History

* To get sec clearance to see classified USG docs, fill out SF86
  - 136-page PDF!
  - Info on relationships, mental health, drug use, $, etc.
  - VERY invasive - one ostensible goal: understand blackmail risk
  - Does apparently happen!

* Roughly 2.8m have sec clearance, 1.6m cong/sec, 1.2m TS (CNN)

* Records stored in mainframe computer at OPM
  - "USG's HR dept."

June 2015: OPM announced that 520m background-check records breached
  - NYT and others attribute to PRC govt.

* Big problem for USG for two reasons:
  1. Blackmail info leaked
  2. CIA records NOT stored in OPM database
OPM Hack: What Happened

Actually, two hacks — OPM discovered one, missed the second.

1. Attacker got contractor's credentials.
   Likely paths:
   - R/W all files, etc.

2. Compromise root acct on local machine.
   - Easy if old version of Windows

3. Work up to compromise of top admin credentials.
   - Exfiltrate data
   "Pass the hash attack"

---

STEP 1: Get user credentials
- Not clear how. Could be spam-phishing, etc.
- No 2FA, smart card
  - 1% of OPM users
  Why? Old systems
  Expensive to upgrade
STEP 2: Privilege escalation
- After compromise user acc, how to get root access?

```
  at 16:05 /interactive "cmd.exe"
```

"at" is like a cronjob on Linux
- Run job at specified time. Runs as "system"!
  (apparently only on very old versions of Windows)
- Lots of other equally simple tricks.
  Some not as simple

STEP 3a: Getting OPM admin password
- Once you have root (SYSTEM) privileges on local machine, need to get admin access on another
- Idea: Steal credentials of other logged in users
- Windows stores (user, Hash(password)) pairs of all logged in users... like Kerberos.

If admin is logged in, you can get their hashed password!
STEP 3b: "Pass the hash"

NTLM Authentication protocol...

Problem: Client doesn't need cleartext pw to log in.
→ Compromising local machine allows lateral movement

→ Not super-clear how to defend against these while keeping backwards compatibility...
Lessons?

- Passwords are a terrible form of authentication
  → Ideally, ONLY used to auth user to their phone/laptop
- Always use 2FA
- Use signatures whenever possible

Also...

- Backwards compatibility is enemy of security
  → Isolation (e.g. CI scanners running XP)
- Audit logging could have made cleanup easier
Transport: POODLE

Ex of "Downgrade attack" - very subtle protocol bug

Many versions of TLS...

| SSL 2 | 1995 |
| SSL 3 | 1996 |
| TLS 1.0 | 1994 |
| 1.1 | 2006 |
| 1.2 | 2008 |
| 1.3 | 2018 |

New versions fix serious & vulns in prior ones.

But millions of out-of-date clients & servers (e.g. IoT)

Need backwards compatibility

Old servers might send garbage when they don't understand protocol version... retry w/ lower version
Transport: POODLE
Should negotiate TLS 1.2...

Client (TLS 1.2)

Server (TLS 1.2)

Once they're speaking, attackers can use 25 yrs of attacks to recover plaintext. L Uses CBC padding oracle attack MAC-then-enc instead of enc-then-MAC

Not an easy attack to pull off: Net access + JS to get cookies from browser

How to prevent?

* Disable SSL 3 support on both sides
* "Anti-pooldle record splitting" (!)
  L Re-jigger data bytes to make underlying SSL 3 harder to exploit
* New TLS extension
Poodle Mitigations

TLS-Fallback, SCSV: Client signals when falling back (TLS 1.2)

Client (TLS 1.2) --

TLS 1.2

garbage

TLS 1.1 Fallback

ERROR

Server (TLS 1.2) -- My version > Client's version

TLS 1.3 has a slightly fancier trick:
- Server signals to client that it is falling back
- If client is TLS 1.3, will halt

[Maybe protects against a REALLY bad bug in older TLS versions that could submit SCSV]

Many downgrade attacks on TLS
- FREAK - Downgrade to export RSA (512 bits)
- SLOTH - "..." old hash algs

Plan for things to break?
CBC Padding oracle

CT1

CT2

Decrypt

+2

IS last byte is ≠ 2, fail.

Attack idea: * Copy CT1 over CT2, can learn last byte of CT2,
* Repeat many times to get cookie, etc.
Platform: Sony PS3 Hack

- Sony PS3 originally could boot Linux/Windows
- Theory: avoid taint
  * Popular in pre-GPU era for cheap HPC (dlog)
- Later on, Sony shipped update that disabled ability to run custom OS
  * Used secureboot, much like iPhone
  * Only boots Sony-signed OS

Sony used EC-DSA... morally equivalent to:

\[
\sigma = (g^r, r + \text{Hash}(pk || g^r || m) \cdot sk) \pmod{q}
\]

\[
\sigma' = (g^r, r + \text{Hash}(pk || g^r || m') \cdot sk)
\]

\[
\Rightarrow \text{Sony's signatures leak their secret key.}
\]

* Has happened to cryptocurrency wallets
* Also embedded devices
* Can also be: \(r = \text{Hash(time())}\)
Software: WannaCry Ransomware

Platform & Software sec failures

- Affected 100ks of computers
  - Hospitals
  - Manufacturing (TSMC, Nissan, etc)
  - Universities
  - Telcos

- Encrypts all juicy-looking files on all HDS (docx, pptx, etc.)
- Shows box demanding ransom paid in Bitcoin with "countdown" timer

Is Caused lots of damage ($4bn?)

⇒ Didn’t raise much $$$ (maybe $300K)

⇒ Hit mostly big enterprises

⇒ Shoddy payment infrastructure (1 static Bitcoin address)
WannaCry: History

- Starts with NSA TAO (?)
  * Developed an exploit "EternalBlue" in MSFT SMB server
  * Combination of three bugs not reported to MSFT
    1) Invalid cast of struct
    2) Parser bug
    3) Allocation bug
  * Attacker can overflow net - get RCE on windows machines
  * Possibly used for years (Five years - unpatched)
  * Key component used to spread WannaCry

⇒ Software bug

- How did EternalBlue get out?

  * NSA contractor (Harold Martin) took TBs of NSA data home with him... motivation

⇒ Platform problem - least privilege?

  * WSJ reports: Martin ran Kaspersky AV on computer with NSA data
  * AV ships suspicious files home for analysis
  * WSJ reports: likely way exploit leaked
WannaCry: History (cont'd)

- After theft, Microsoft (March 14, 2017) issued patches for supported Windows versions.
  - Older Windows unpatched for 2 months.

Platform security - updates

- Shadow Brokers dump many exploits (including 0days) online - GitHub repo

  *Dump April 14, 2017

- Shows up in WannaCry May 12, 2017

  *Suspected to be N. Korea. (why?)
WannaCry: Mechanics

1. Connects to website at random-looking addr
   → Extre if succeeds ("kill switch")
   * Potentially used to check whether running in VM
   * Used to help mitigate

2. Installs Tor, uses to connect to C2 infrastructure
   * C2 hosted at onion address

3. Encrypts all files that have fixed set of extensions.
   → Uses RSA + AES
   * Often source of bugs: Power Vorm - didn't save key
     * Key reuse across users
   * Malware also updates itself!

4. Demands ransom be paid to one of four static Bitcoin addr
   * $300 then $600
   * Problem: No automated way to match payment to machine/IP/peer → No scale
   * Problem: Spreading via SMB meant that if hit mostly enterprises - no better backups

5. Spreads itself
   * Tries to connect to port 445 (SMB) on all IPs
   → Random, IPs on internet
What can we learn?

- That you should fill out your course evals?
- Less software \(\Rightarrow\) fewer bugs
  - Do you really need an SMB server?
- Any bug is a security bug?
  - Not obvious that a parser bug could cause such chaos

- Design for fast updates
  - Most machines affected were old (XP?)
  - Many didn't get patch in time
  - Most secure s/w (e.g., Chrome) has a very aggressive update plan — not an accident

- Having a recovery plan (backup) is as important as trying to prevent attack.
Privacy: U.S. Census

- Performed every 10 years
  - Data used to allocate House seats
  - Used for redistricting

  13 USC 99: Census Bureau may not “make any publication... whereby the data furnished by... any individual under this title may be identified.”

- In 2020 census, bureau used D.P. to protect released data from de-identification
  - Used $\epsilon = 19.61$

  $\Rightarrow$ If a bad event $B$ was going to happen to you absent data release
  - \[ \Pr[p] \leq e^{\epsilon} \Pr[p] \]
  - \[ \leq 1,000,000 \Pr[\text{struck by lightning}] \]

  This $\epsilon$ ignores some non-private data releases (e.g. State pop)

- Still, amazing to see sophisticated privacy tech used in practice

- Alabama sued in March 2021 over use of D.P.
  - Dropped... still may come up again
Lessons?

* Cryptography can help in many places
  * Publishing data sets might not be one of them
    * Tough trade-offs

* Though, I worry less about intentionally published datasets and more about unintentionally published ones (data breaches, etc.)
  * Therefore, secure systems-building tools + cryptography can help?
What's next for you?

If you're interested in learning more...

- Course evaluations

This class

- Security
  - 6.5660 (6.858)
  - Nicola

- Applied crypto
  - 6.5610 (6.857)
  - me & Yael

- Theory of crypto
  - 6.5620J (6.875)

+ Lots of offerings at Harvard on privacy & security policy.
  + OS, randomized algs, ...

- Charles River Crypto Day
- CIS seminar (F 10:30am)
- Security seminar (W 4pm)

Research! Feel free to ping us