Lecture 27: Wrap Up

Fall 2023 - MIT
6.1600
LG & Zuldarsh

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. DDD

* 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 w/ real world.
  3. To entertain you. 

Let's start off with an authentication failure...

2014 - 2015

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 conf/sec, 1.2m TS (CNN)
* Records stored in mainframe computer at OPM
  - "USG's HR dept"

June 2015: OPM announced that ≈20m background-check records breached

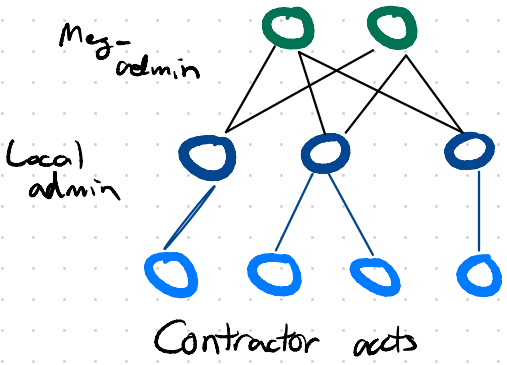
↳ NYT and others attribute to PRC govt

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

OPM Hack: What Happened

[Various - Duo Blog, CS 558 write-up]

Actually two hacks — OPM discovered one, missed the second



1. Attacker got contractor's credentials.

Likely path...

2. Compromise root acct on local machine. ← R/W all files, etc.
   - ↳ 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 spear-phishing, etc.
- ↳ No 2FA, smart card ~ 1% of OPM users
  - Why? Old systems. Expensive to upgrade

OPM Hack: Technical Details

STEP 2: Privilege escalation

- After compromise user acct, 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 with more access

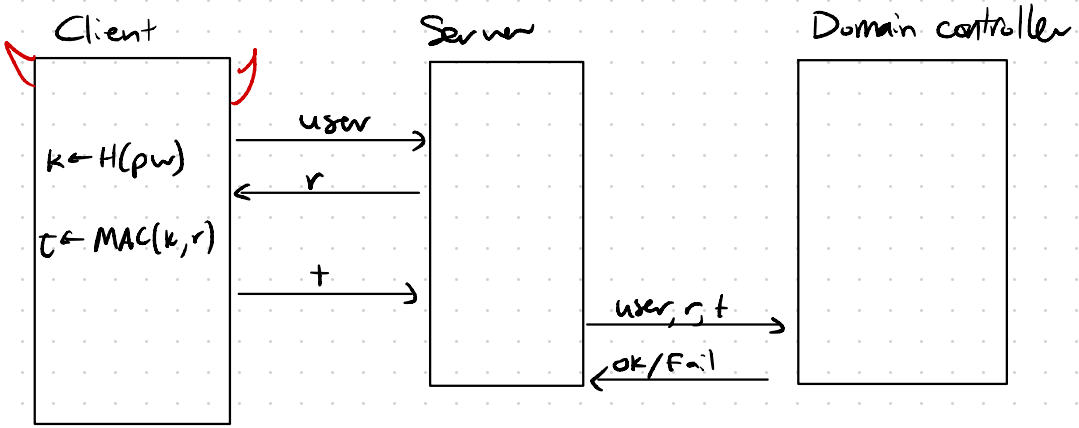
- Windows stores (user, Hash(password)) pairs of all logged-in users... like Kerberos.

↳ If admin is logged in, you can get their hashed password!!

STEP 3b: "Pass the hash"

(See CSS58 blog post, many other NTLM)

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. CT scanners running XP)
- Audit logging could have made cleanup easier

Transport: POODLE

[Möller, Duong, Kotowicz 2014]

Ex of "Downgrade attack" - very subtle protocol bug

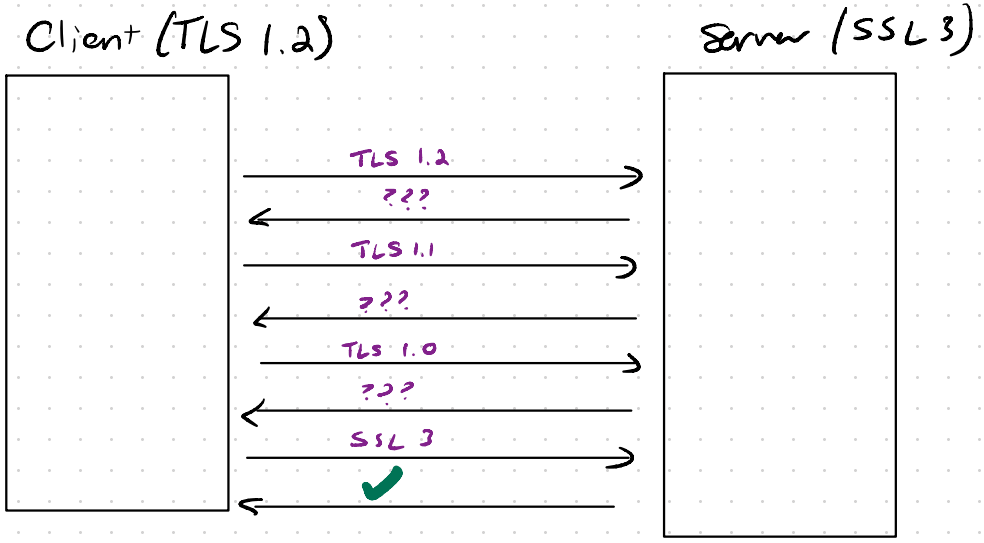
Many versions of TLS...

SSL	2	1995
	3	1996
TLS	1.0	1999
	1.1	2006
	1.2	2008
	1.3	2018

New versions fix serious sec vulns in prior ones.

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

↳ Need backwards compatibility

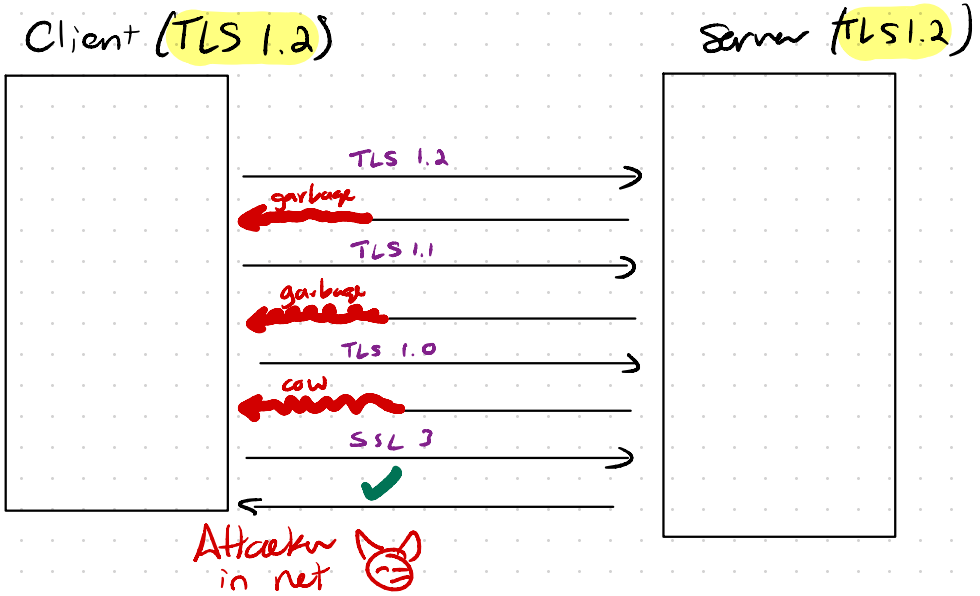


Old servers might send garbage when they don't understand protocol version... retry w/ lower version

Transport: POODLE

[See Langley's Blog post]

Should negotiate TLS 1.2....



Once they're speaking, attacker can use 25 yrs of attacks to recover plaintext.

↳ Uses CBC padding oracle attack
MAC-then-enc ✗ instead of enc-then-MAC ✓

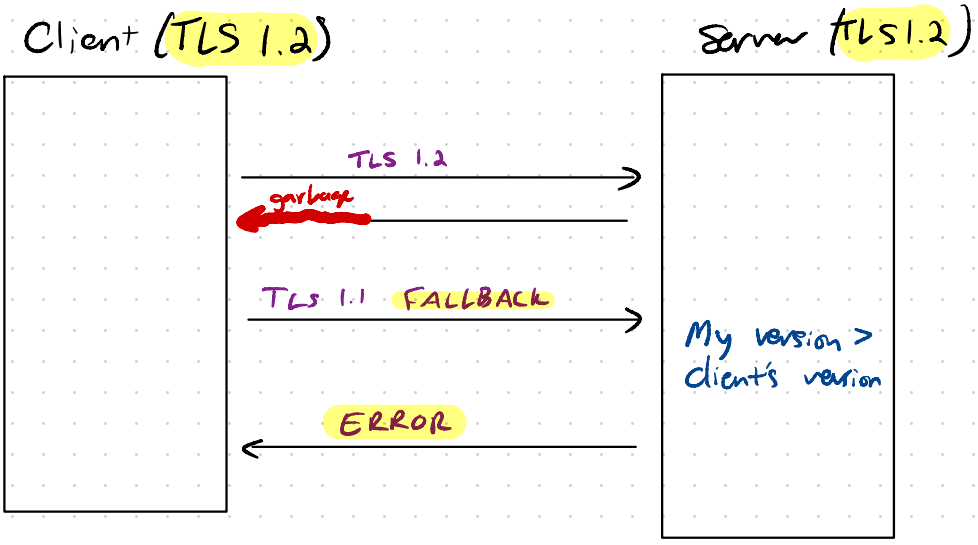
Not an easy attack to pull off: Net access + JS to get cookies from browser

How to prevent?

* Disable SSL 3 support on both sides
* "Anti-poodle record splitting" (!)
  ↳ Rejigger data bytes to make underlying SSLv3 buggy harder to exploit
* New TLS extension

POODLE Mitigations

TLS-FALLBACK_SCSV: Client signals when falling back [TLS 1.2]



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

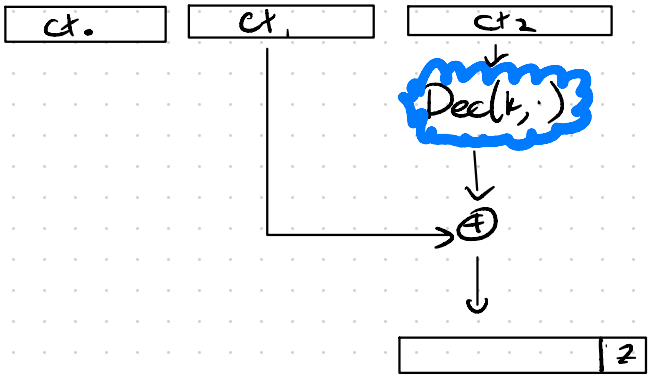
[Maybe protects against a REALLY bad bug in older TLS versions that could subvert SCSV]

MANY downgrade attacks on TLS

* FREAK - Downgrade to export RSA (512 bits)
* SLOTH - " " old hash algs
* ...

Plan for things to break!

CBC Padding oracle



IF last byte is $\neq 7$, fail.

Attack idea: * Copy ct_0 over ct_2, can learn last byte of ct_0.

* Repeat many times to get cookie, etc.

Platform: Sony PS3 Hack [fail0verflow 27C3 talk]

Software bug / crypto implementation failure → Platform sec failure

- Sony PS3 originally could boot Linux/windows
  - ↳ Theory: avoid tariffs
  - * 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:

Should be a random long #

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

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

⇒ Sony's signatures leak their secret key.

- * Has happened to cryptocurrency wallets
- * Also embedded devices
- * Can also be if $r \leftarrow \text{Hash}(\text{time}())$

Software: WannaCry Ransomware

[Many articles in popular press]

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 payment in Bitcoin with "countdown" timer

↳ Caused LOTS of damage ($4bn?)
  ↳ Didn't raise much $$$ (maybe $300k) ← Possible to know b/c Bitcoin
    - * Hit mostly big enterprises
    - * Shoddy payment infrastructure (1 static Bitcoin addrs)

WannaCry: History

* Much speculation / unattributed sources

[See Checkpoint]

- Starts with NSA TAO (?)
  - * Developed an exploit "EternalBlue" in MSFT SMB server (used for file sharing)
    - * Combination of three bugs not reported to MSFT
      1) Invalid cast of struct
      2) Parser bug
      3) Allocation bug

      (see Checkpoint blog post ... Not at all trivial)
  - * Attacker can – over net – get RCE on Windows machines
  - * Possibly used for years (five years – report)
  - * Key component used to spread WannaCry

  ⇒ Software bug

- How did EternalBlue get out?

  [WSJ articles]

  - * 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

(Logrhythm post)

1. Connects to website at random-looking addr
   - ↳ Exits 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 Worm - didn't save key
       - * Key reuse across users
     - ↳ Malware also updates itself!

4. Demands ransom be paid to one of four static Bitcoin addrs
   - * $300 then $600
   - * Problem: No automated way to match payment to machine/payer → No scale
   - * Problem: Spreading via SMB meant that it hit mostly enterprises — w/ better backups

5. Spreads itself
   - * Tries to connect to port 445 (SMB) on all IPs in local net (/24)
     - ↳ Random IPs on internet

What can we learn?

- That you should fill out your course evals?
- Less software => 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 allocated House seats
  - ↳ Used for redistricting

  13 USC §9: 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 $\varepsilon = 19.61$.

  ⇒ If a bad event B was going to happen to you absent data release w.p. p, it will now happen w.p. $\leq e^{19.61} \cdot p$

$$\Pr[\text{Bad in world with data included}] \leq e^{19.61} \Pr[\text{Bad in world w/o data included}]$$

$e^{19.61} \approx 1{,}000{,}000$

$\Pr[\text{Bad in world w/o data included}] \leq \Pr[\text{struck by lightning next yr}] \approx 2^{-19}$

This ε 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

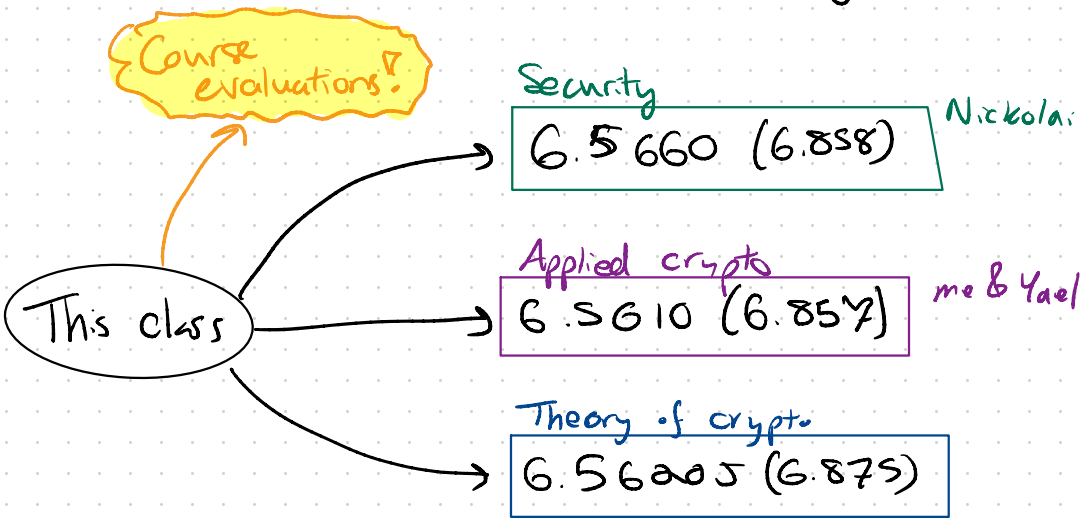
Lessons?

* 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.)
  ↳ There, secure systems-building tools + cryptography can help!

What's next for you?

If you're interested in learning more...



+ 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