Why Software Still Stinks

…and what you can do about it!

SECURITY INNOVATION

About Security Innovation

- Securing software *and* its ecosystem for two decades

- Helping clients get smarter about software security
  - **Assessments:** understand gaps
  - **Standards:** establish repeatable practices
  - **Training:** enable good decisions

Over **3.5 Million** Users

Authored **18** Books

Gartner MQ **6x** **Security Training**

intel Disney PNC BANK TARGET DISCOVER charles SCHWAB RoyalCaribbean INTERNATIONAL Nasdaq DELTA 3M Allstate facebook airbnb PayPal amazon hp

SECURITY INNOVATION

Attack Example #1: *SQL Injection*

- Apps are dumb; they do as they're told
- A login field sends a message to the database

```
SELECT * FROM USERS WHERE
Username = 'Ed' AND Password = 'Adams';
```

- But… humans know logic
  - What if you give it something it can't argue with?
  - Maybe something that's always true?
  - Will the dumb app be fooled?

DEMO TIME!

Example #2: *Cross-site Scripting*

- Apps execute code commands
- JavaScript has many such commands

- Some humans are not nice
  - They might feed apps harmful commands
  - Can the dumb app be fooled again?

DEMO TIME!

Example #3: *Escalation of Privilege*

- Get into an easy to open door
- Explore and exploit once inside
- Do damage and extract goods

- Did I mention some humans are not nice?
  - They will mess with “safe” areas

DEMO TIME!

Example #3: *Escalation of Privilege*

I want in here

I can get in here

What's in a house?

- TV
- Computers
- Electronics
- Money


What’s in a shed?
• Ladders
• Bolt cutters
• Spare keys
• Drills & Saws

Start Here

Go Here

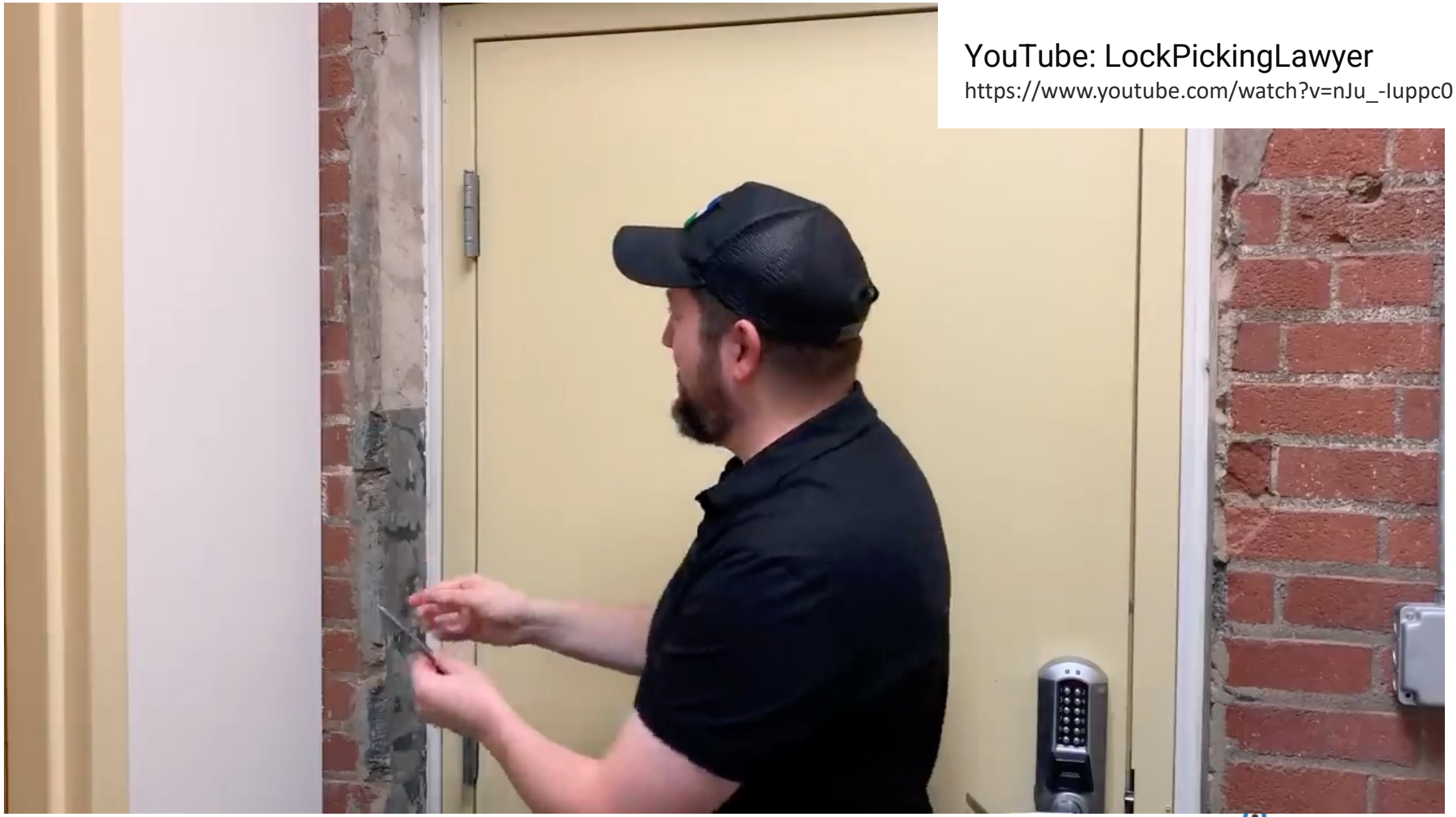
Examples #4, 5, and 6

- Time permitting, we'll also look at:
- Parameter Tampering
- Fuzzing Inputs
- Cloud Service Misconfiguration

DEMO TIME!

YouTube: LockPickingLawyer

https://www.youtube.com/watch?v=nJu_-Iuppc0



Thank You

eadams@securityinnovation.com

www.edtalks.io

Ponemon INSTITUTE

Security Training Benchmarks

getsec.in/PonemonReport

SECURITY INNOVATION