CIS 447/544: Computer and Network Security

Anys Bacha

Slides from U. Shankar, M. Hicks, K. Du, D. Boneh, N. Zeldovich, A. Rahmati

Law and Ethics

- Don’t be evil
  - Respect privacy and property of others
  - Violations in code of conduct will result in **failure of the course**
- Respect the law (federal/state)
  - Computer intrusion and wiretapping are illegal
  - You can go to jail
- Respect university policies
  - Do not tamper with campus systems
  - You can be expelled
- Ask TA or instructor when in doubt

Introduction

What is Security

- Normal users care about program correctness
  - Workaround buggy software
  - Never see all bugs
- Adversaries seek out undesirable behavior
  - Your adversary is not a typical user
  - Exercise corner cases to produce undesirable behavior
- Security is about achieving some goal in the presence of an adversary
  - Prevent undesirable behavior in a program

The Security Problem

Buggy Software

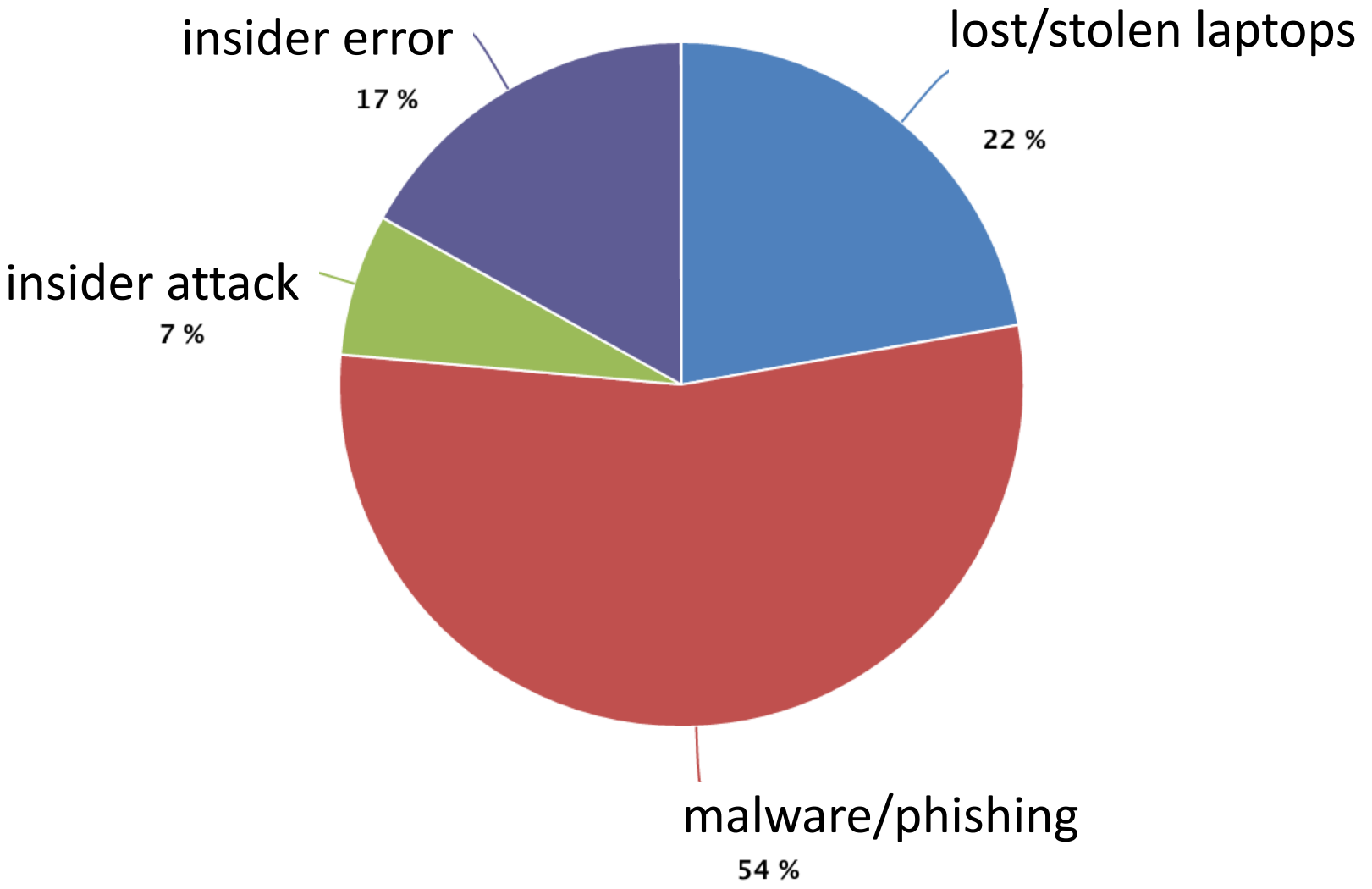
- Released software contains a lot of defects
  - Agile development is inherently a buggy process (feature = bug)
  - Time to market creates aggressive schedules
  - Some bugs too expensive to fix (bad design choices early on in project)

- Developers and validation engineers are not normal users
  - Rely on lab modes to gain full access to system details
  - Normal users don’t use the system this way
  - Leaves lots of corner cases to be exploited

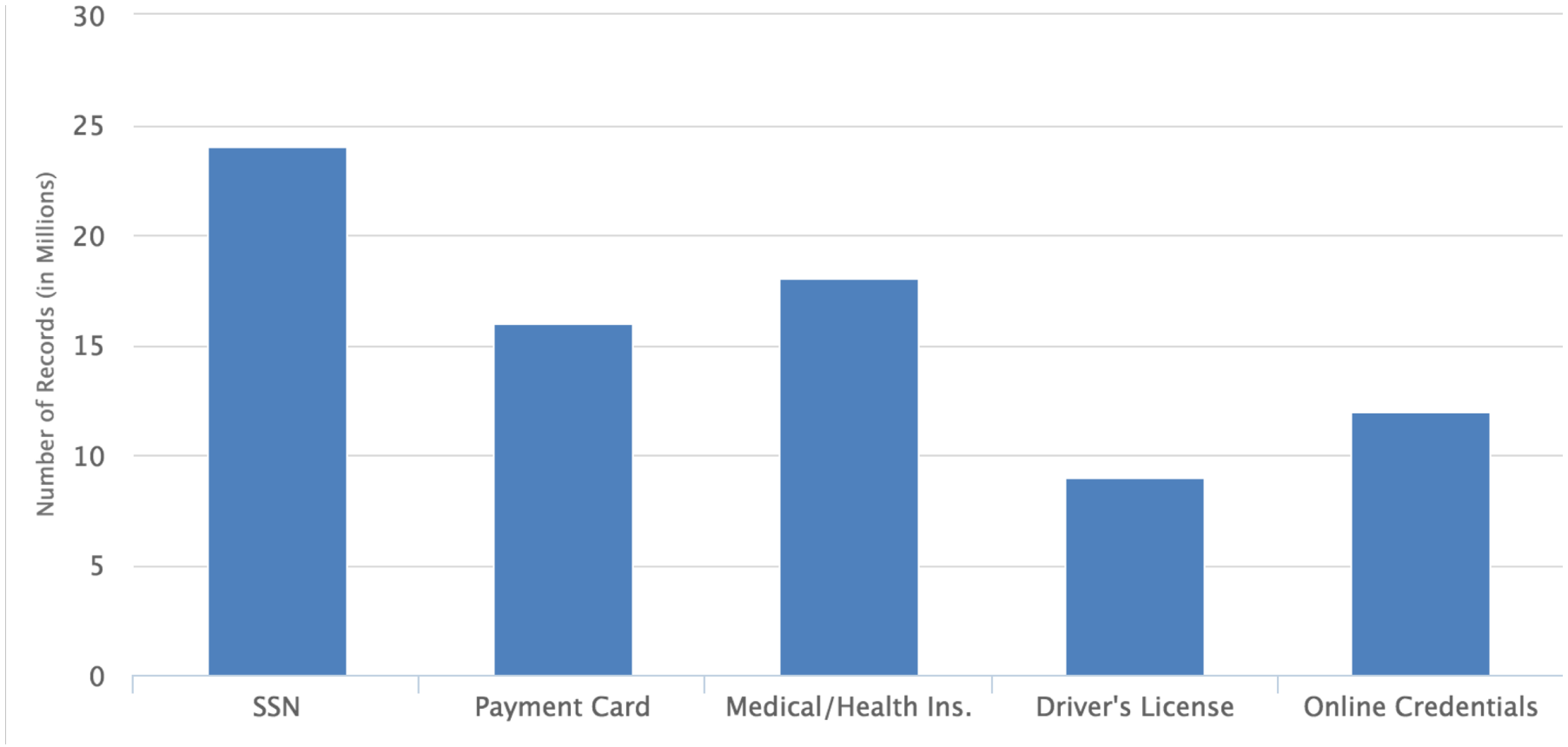
Social Engineering

- Social engineering is effective
  - Trick people into breaking standard security practices
    - Baiting
      - malware infected device (USB drive) user will find and install
    - Phishing
      - fraudulent communications (email, impersonating trusted source) to steal personal, financial, or business information
    - Tailgating
      - Unauthorized individual follows authorized users into restricted and secure locations where they can launch attack

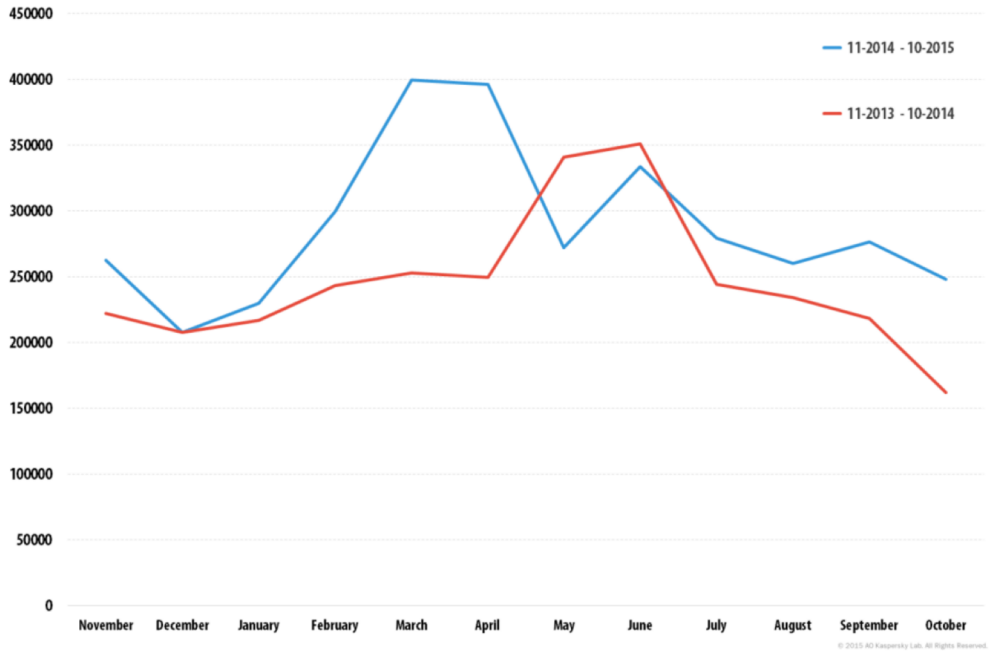
How Companies Lose Data



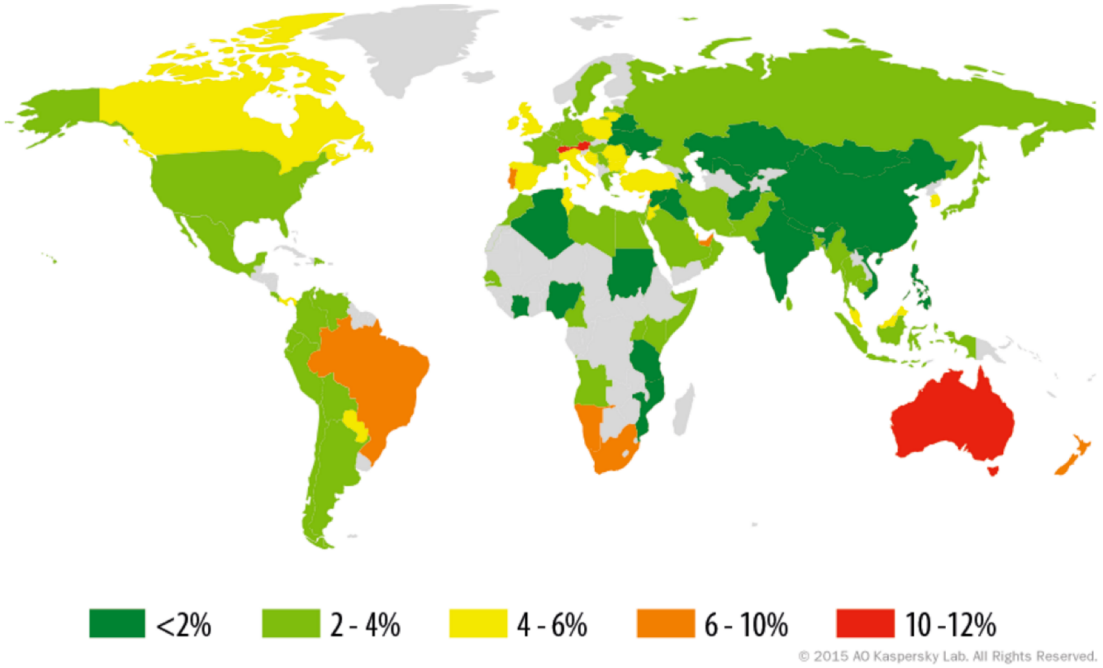
Types of Data Stolen



Distribution of Attacks Across the World

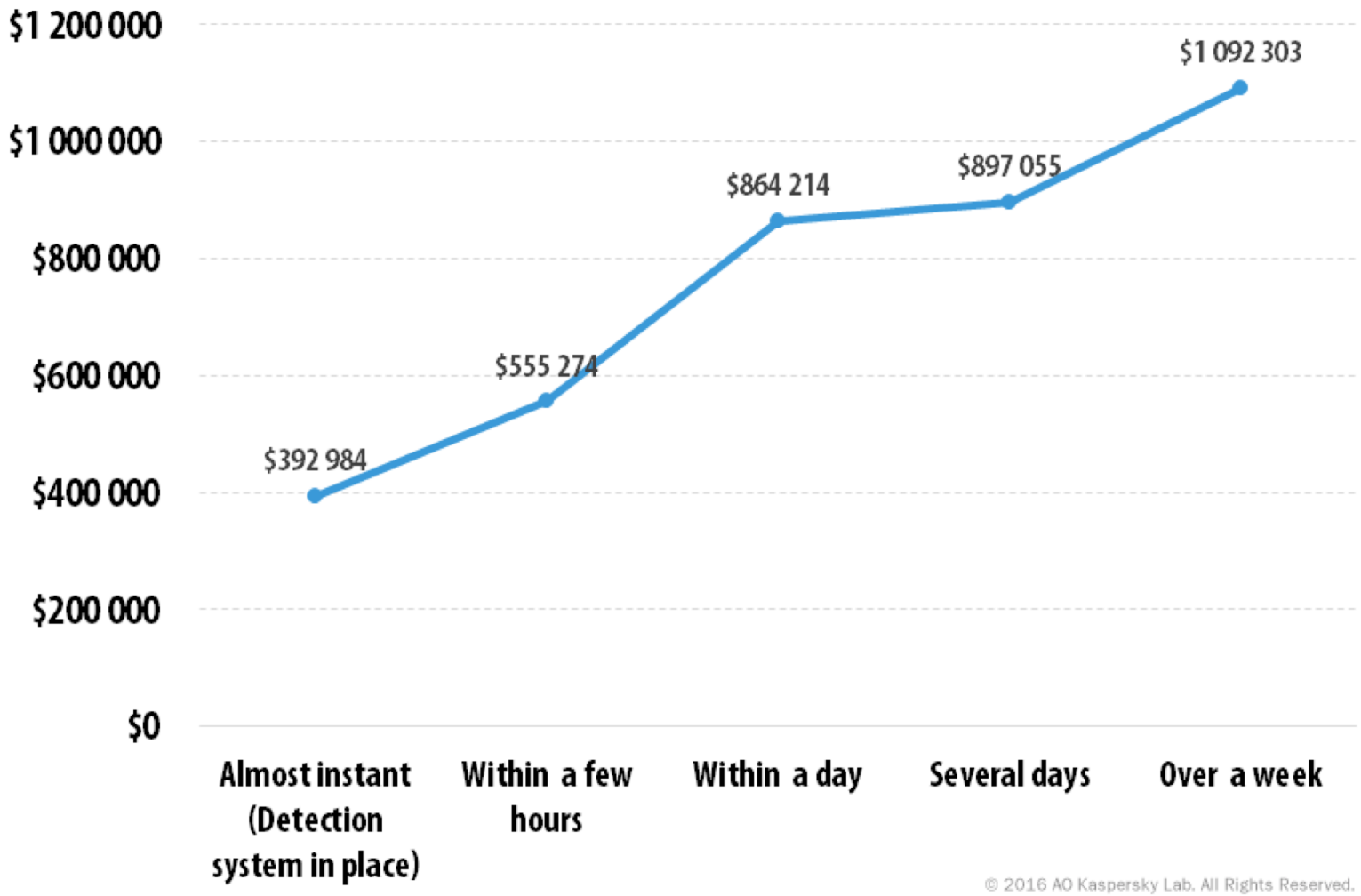


≈ 300,000 users/month worldwide



A worldwide problem

Cost of Not Fixing Vulnerabilities



Marketplace for Vulnerabilities

- Marketplace for finding and exploiting vulnerabilities
  - bug bounty programs
    - Google Vulnerability Reward Program: up to $31,337
    - Microsoft Bounty Program: up to $100K
    - Apple Bug Bounty program: up to $200K (secure boot firmware)
    - Pwn2Own competition: $15K
- Zero day initiative (ZDI), iDefense (accenture): up to $25K
- Zerodium: $1.5M for iOS10, $200K for Android 7 (Sep. 2016)

Vulnerability Disclosures

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Mac Os X	Apple	OS	385
2	Iphone Os	Apple	OS	376
3	Flash Player	Adobe	Application	313
4	Air Sdk	Adobe	Application	246
5	AIR	Adobe	Application	246
6	Air Sdk & Compiler	Adobe	Application	246
7	Internet Explorer	Microsoft	Application	231
8	Chrome	Google	Application	187
9	Firefox	Mozilla	Application	178
10	Windows Server 2012	Microsoft	OS	155
11	Ubuntu Linux	Canonical	OS	152
12	Windows 8.1	Microsoft	OS	151

How to Think about Security

Components of Security

- Policy: the goal you want to achieve, e.g. only Alice should read file F
  - Confidentiality: info users wish to hide must not be revealed, e.g. corporate secrets
  - Integrity: Information or functionality must not be modified, e.g. disallow deleting files or changing data in flight
  - Availability: System must remain available at all time, e.g. site must withstand denial of service attacks

Components of Security

- Threat model: assumptions about what adversary would do
  - e.g. assume adversary can guess passwords
  - Be conservative with assumptions

- Mechanism: knobs your system provides to enforce the policy, e.g. user accounts, passwords, access controls, encryption, etc.

- End goal: adversary must not be able to compromise the policy while within the threat model

Case Studies

Issues with Policies

- Account recovery questions are widely used for resetting passwords
  - List of questions that only account owner knows
  - Email link to reset password
  - What if dealing with email provider?

- Yahoo weakened the policy by providing a path to accessing the account through questions

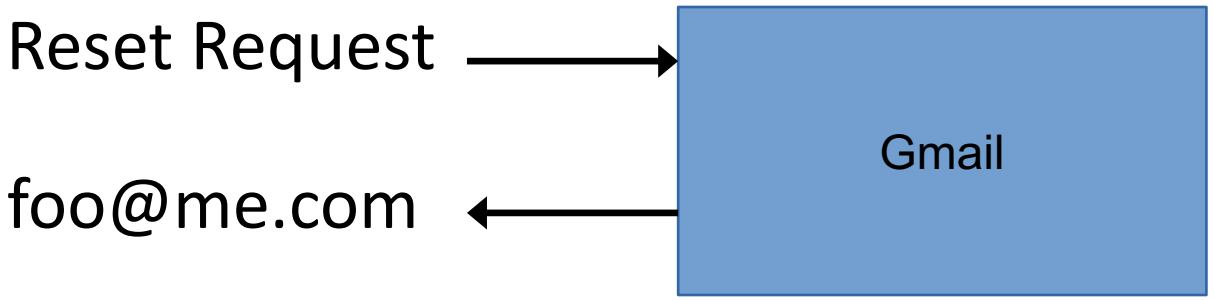
- Some adversary guessed Sarah Palin's high school, birthday, etc.
  - All info was on wikipedia

Issues with Policies

- Interaction between multiple accounts (Amazon, Apple, Google, etc.)
- All accounts had strong policies individually
  - Weakness when combined together
- Digital life of Mat Honan from wired.com dissolved within an hour
  - Google account taken over then deleted
  - Twitter account compromised and used as platform for broadcasting info
  - AppleID broken into (erased data on iPhone, iPad, and MacBook)

Mat Honan

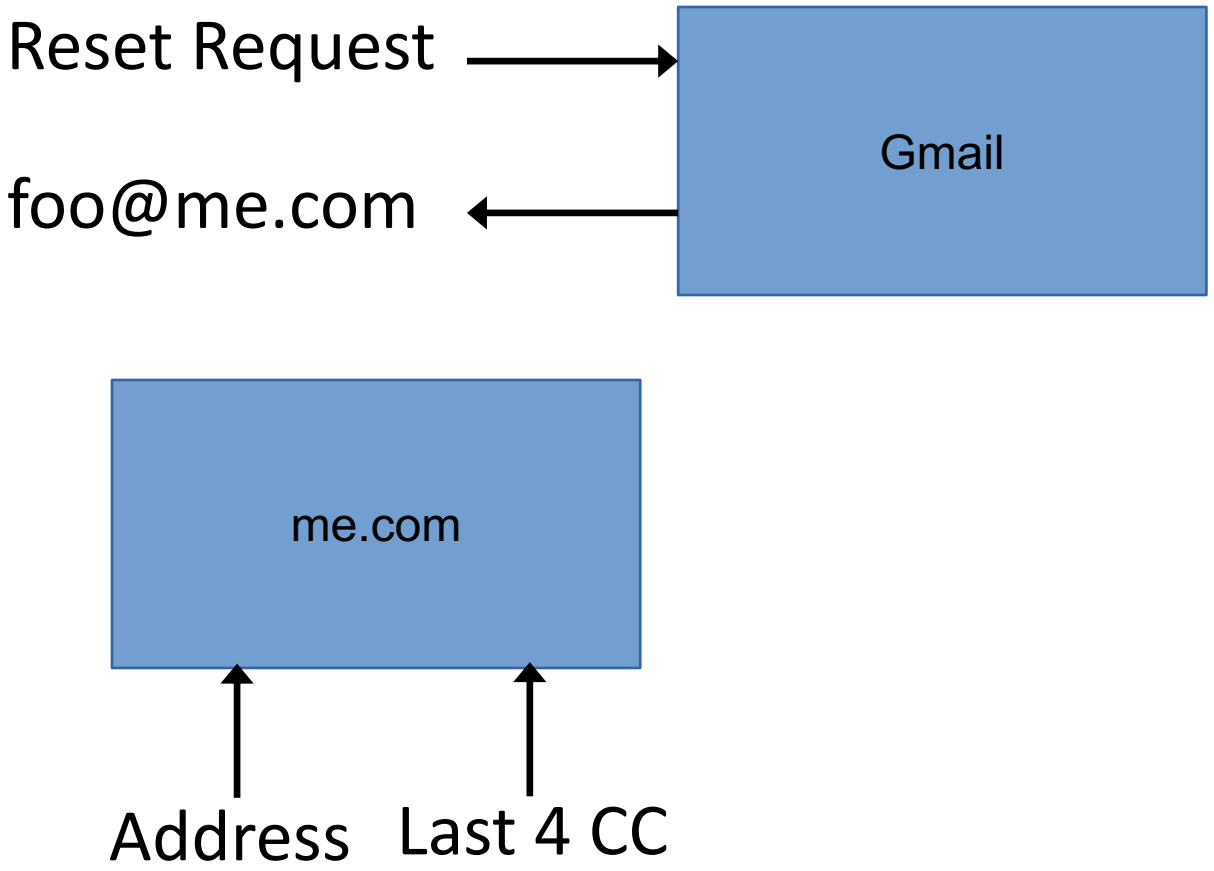
Issues with Policies



Gmail allows password reset

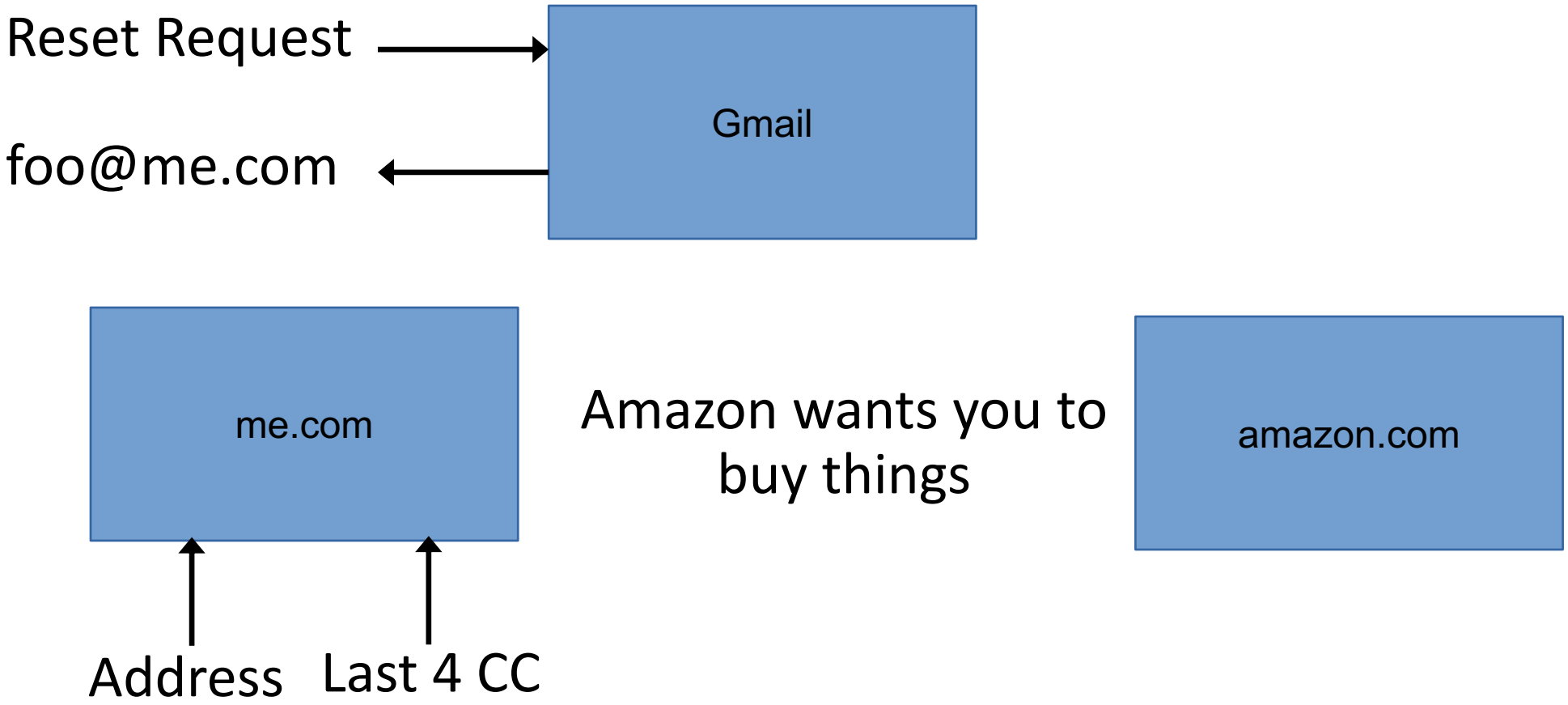
How to access foo@me.com?

Issues with Policies

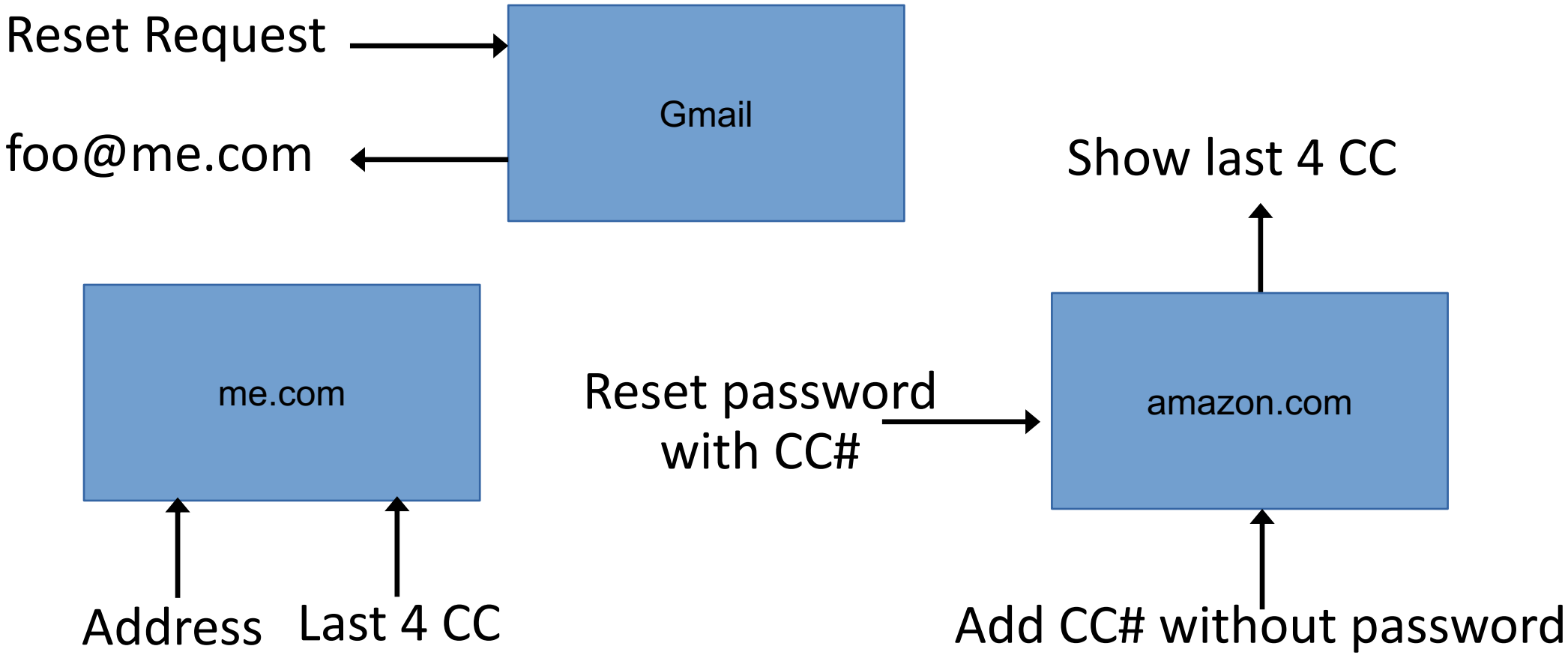


How to get last 4 CC?

Issues with Policies



Issues with Policies



Issues with Threat Model

- Issues with threat model sometimes involves computational assumptions changing over time

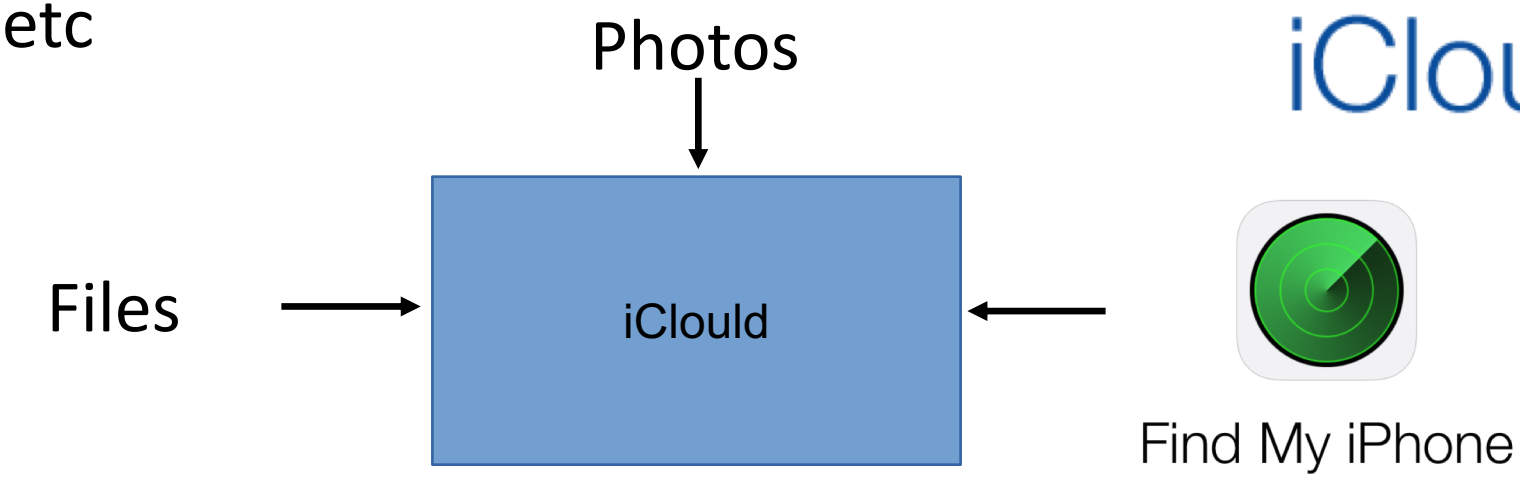
- MIT's Kerberos system used 56-bit DES keys
  - In 1980's adversary couldn't check all 2^56 keys
  - Student project at MIT showed that key could be obtained in a day

- DARPA wanted to build secure operating system
  - Got red team to break into the OS
  - The OS was secure, however source code of OS was stored on machine kept in someone's office
  - Red team broke into the server and inserted backdoor
  - OS was compromised when developers built a new OS

Issues with Mechanism

- Most issues tend to be with mechanism due to complicated software, hardware, and different system-level interactions

- Apple iCloud provides many services including storage, locating device, etc



Multiple APIs

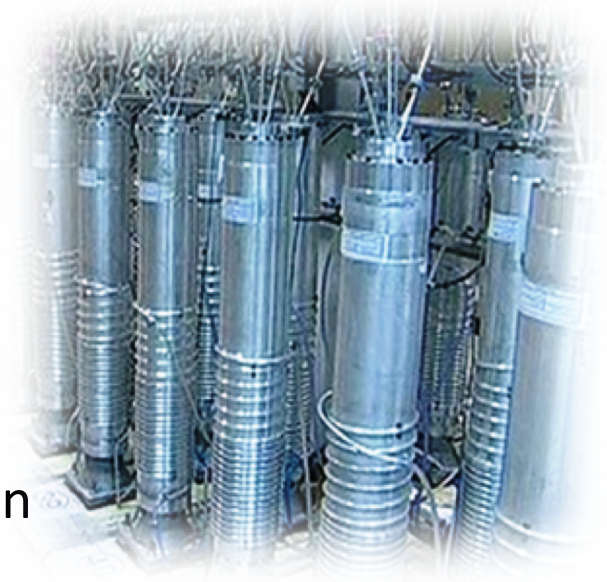
Issues with Mechanism

- Human passwords are relatively easy to crack using GPUs (<1day)
- Mechanism should only allow limited number of incorrect attempts and implement some exponential backoff
- Find iPhone interface forgot a check on the number of incorrect login attempts allowing adversary to make unlimited guesses of password
- Many accounts were compromised as a result

Other Case Studies

Stuxnet

- First worm known to attack supervisory control and data acquisition (SCADA) systems that control wide range of machinery
  - Cyberweapon used to target Iran's centrifuges at nuclear facilities
- Typically spread via USB flash drive
  - Installs kernel mode rootkits using digitally signed certificates stolen from Realtek and Jmicron
- Worm then propagates itself across a private network and scans for Siemens Step 7 software (used for programming PLCs)



Centrifuge

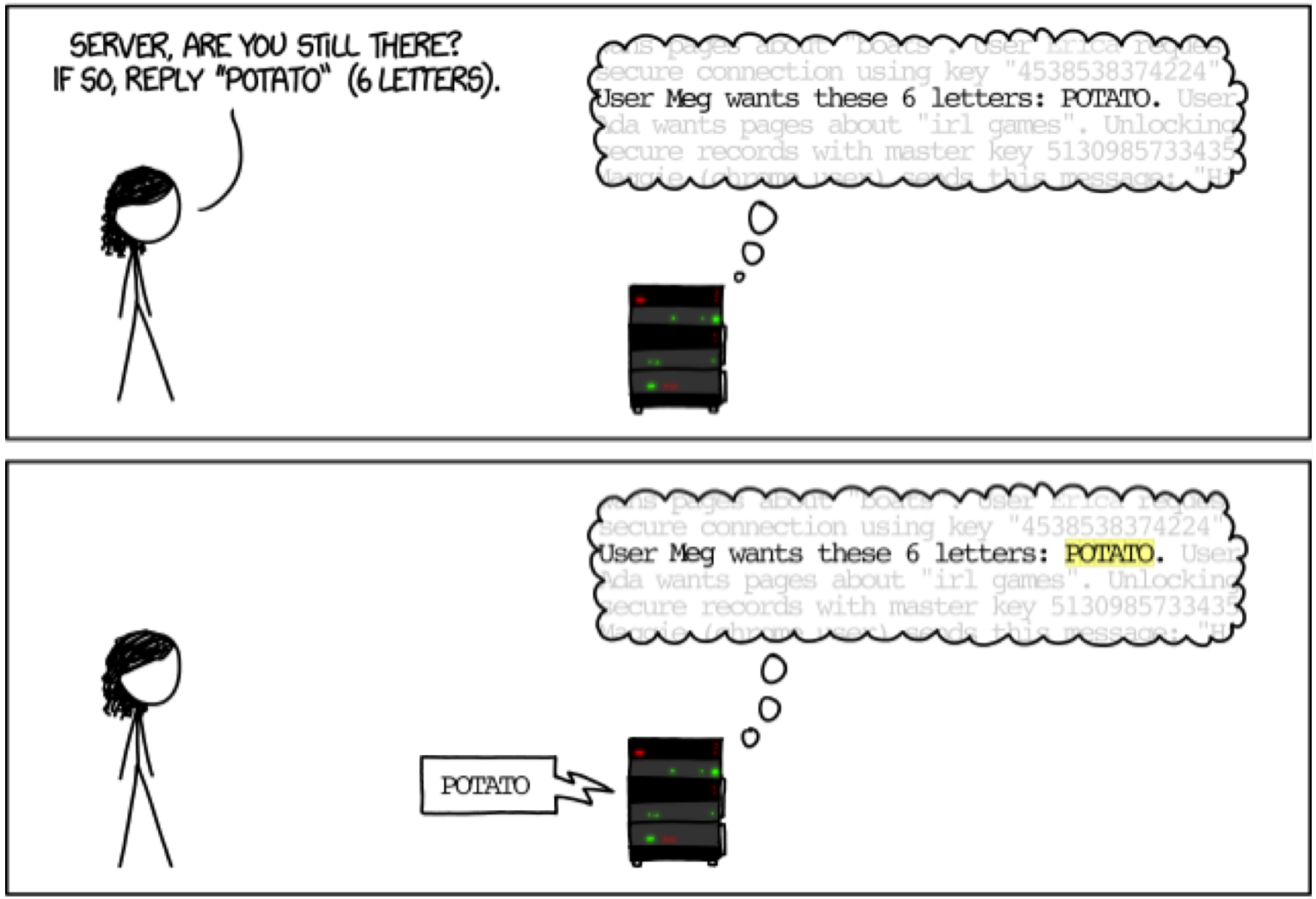
Stuxnet

- Once software is connected to PLC device, Stuxnet infects the PLC
- Malicious code injected into PLC ramps up and down the velocity of centrifuges (used for uranium enrichment) in an attempt to destroy them
  - Maintaining rotor speed of centrifuges is critical
  - Stuxnet had the ability to report false feedback to the monitoring system
- 984 centrifuges were destroyed during this process

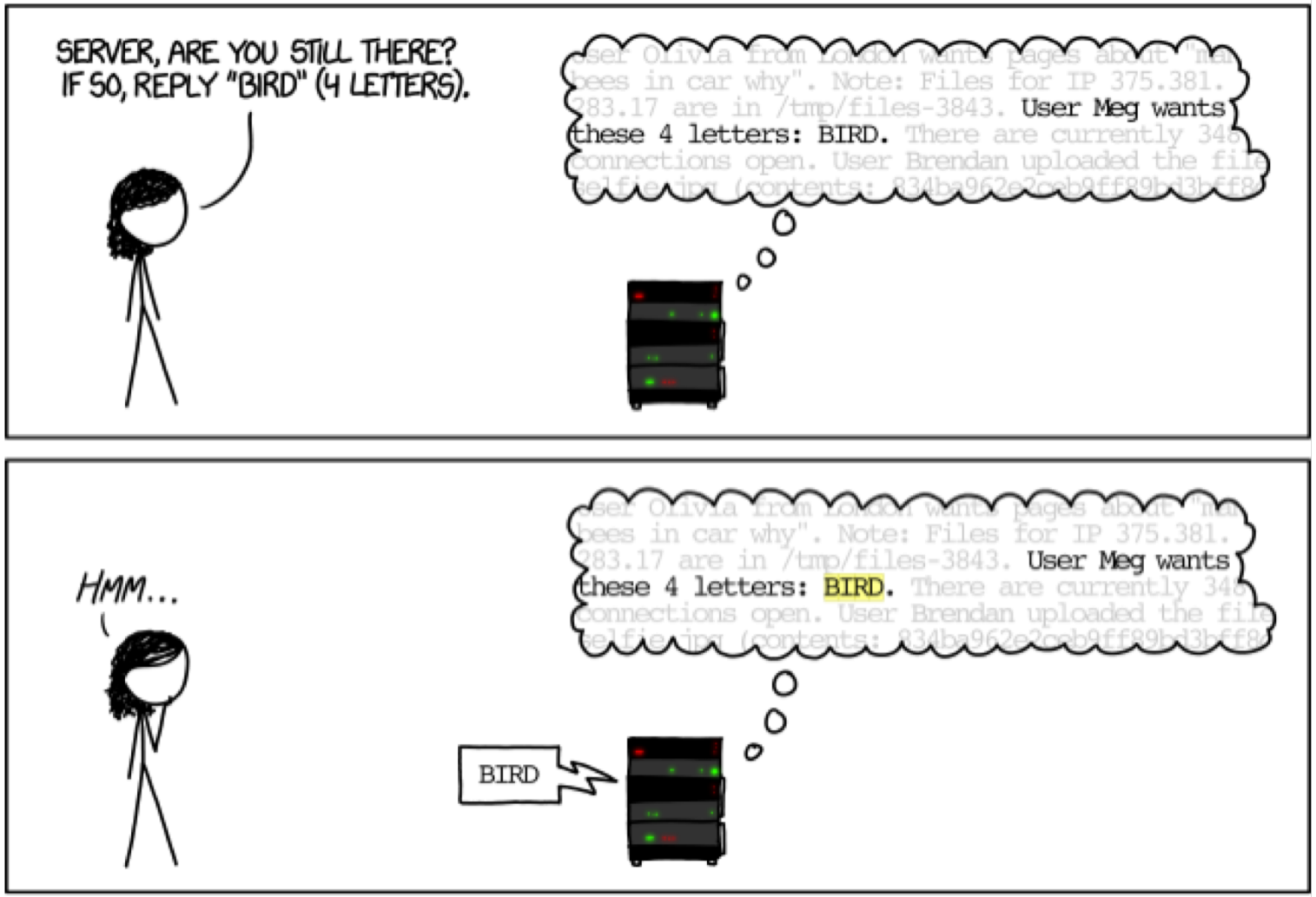
Heartbleed

- SSL/TLS was extended to implement a heartbeat
- Heartbeat used to test and keep alive a secure communication link without the need to renegotiate the connection every time
- Bug allowed attacker to send a maliciously crafted packet that would prompt the server to return more data (buffer over-read)
- Server blindly copied memory (up to 64KB) according to the payload size specified by the user which typically contains usernames, passwords, and keys

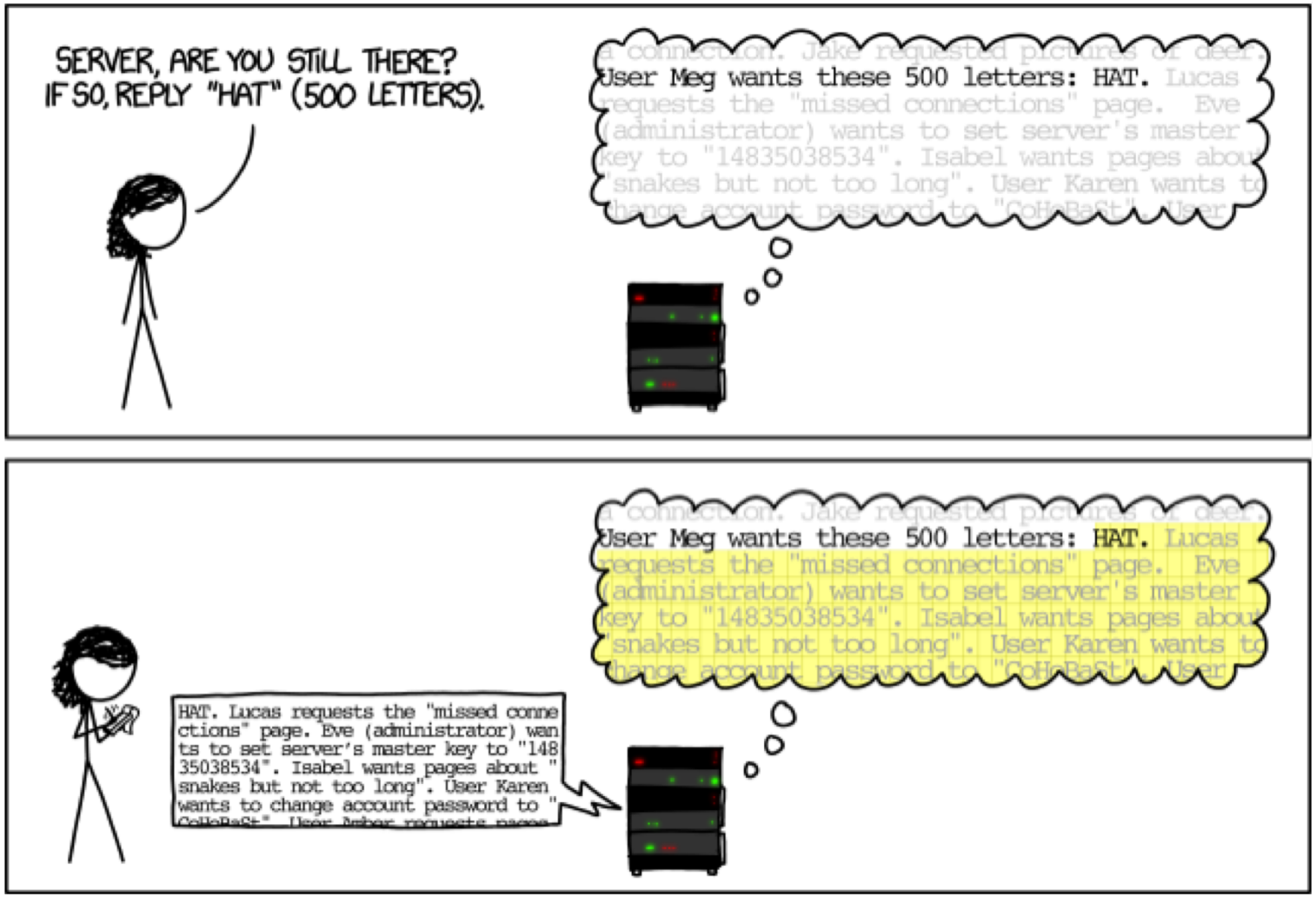
Heartbleed


SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).
User Meg wants these 6 letters: POTATO.
POTATO

Heartbleed


SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).
User Olivia from London wants pages about "ma
bees in car why". Note: Files for IP 375.381.
283.17 are in /tmp/files-3843. User Meg wants
these 4 letters: BIRD. There are currently 348
connections open. User Brendan uploaded the file
selfie.jpg (contents: 834ba962e2eab9ff89bd3bff8
HMM...
User Olivia from London wants pages about "ma
bees in car why". Note: Files for IP 375.381.
283.17 are in /tmp/files-3843. User Meg wants
these 4 letters: BIRD. There are currently 348
connections open. User Brendan uploaded the file
selfie.jpg (contents: 834ba962e2eab9ff89bd3bff8
BIRD

Heartbleed

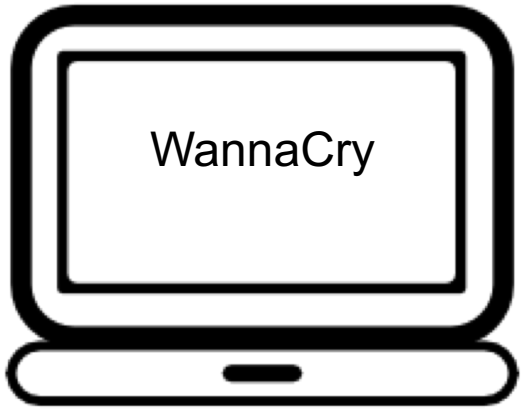

SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoRaSt". User
User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoRaSt". User
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "

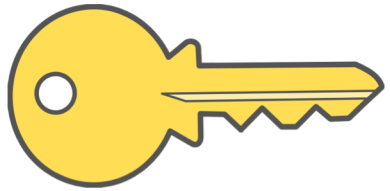
WannaCry

- Ransomware attack that targets systems running the Windows operating system, encrypts data files, and demands $300 in bitcoins within 3 days (or $600 in 7 days)
- Ransomware affected more than 230K systems across the world including the UK's National Health Service (NHS) prompting them to run services on an emergency-only basis
- Propagates itself using EternalBlue, a Windows exploit associated with Server Message Block (SMB) which is used for file and printer sharing
  - Attackers could send a crafted packet to allow code execution on target

WannaCry

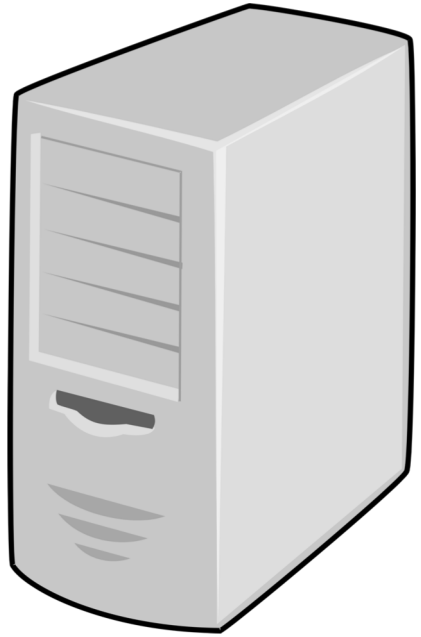
Client

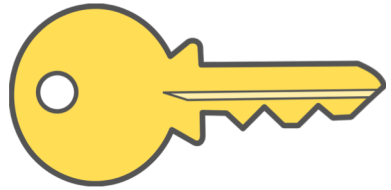




S_pub

Server

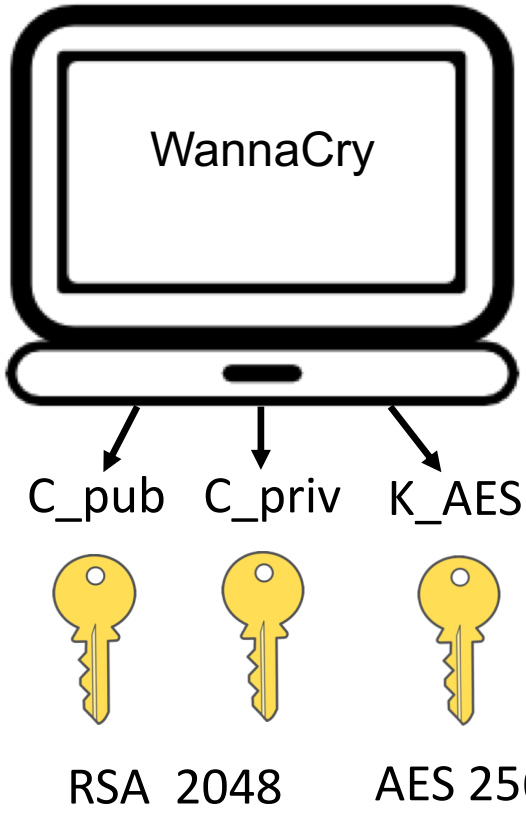


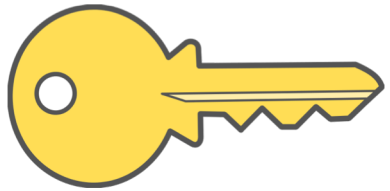


S_priv

WannaCry

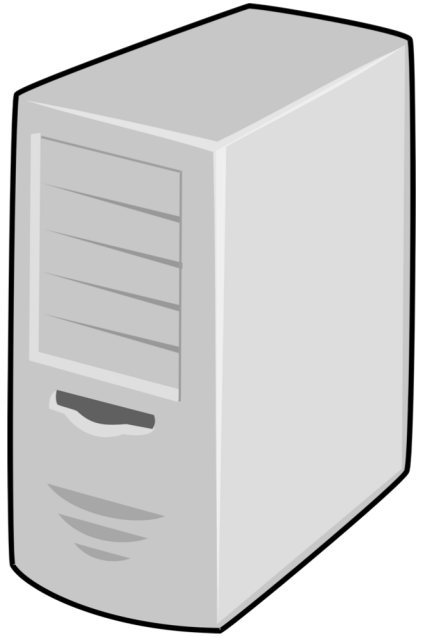
Client

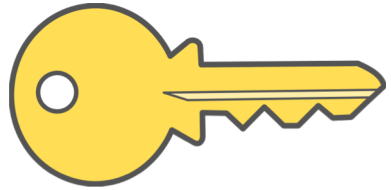




S_pub

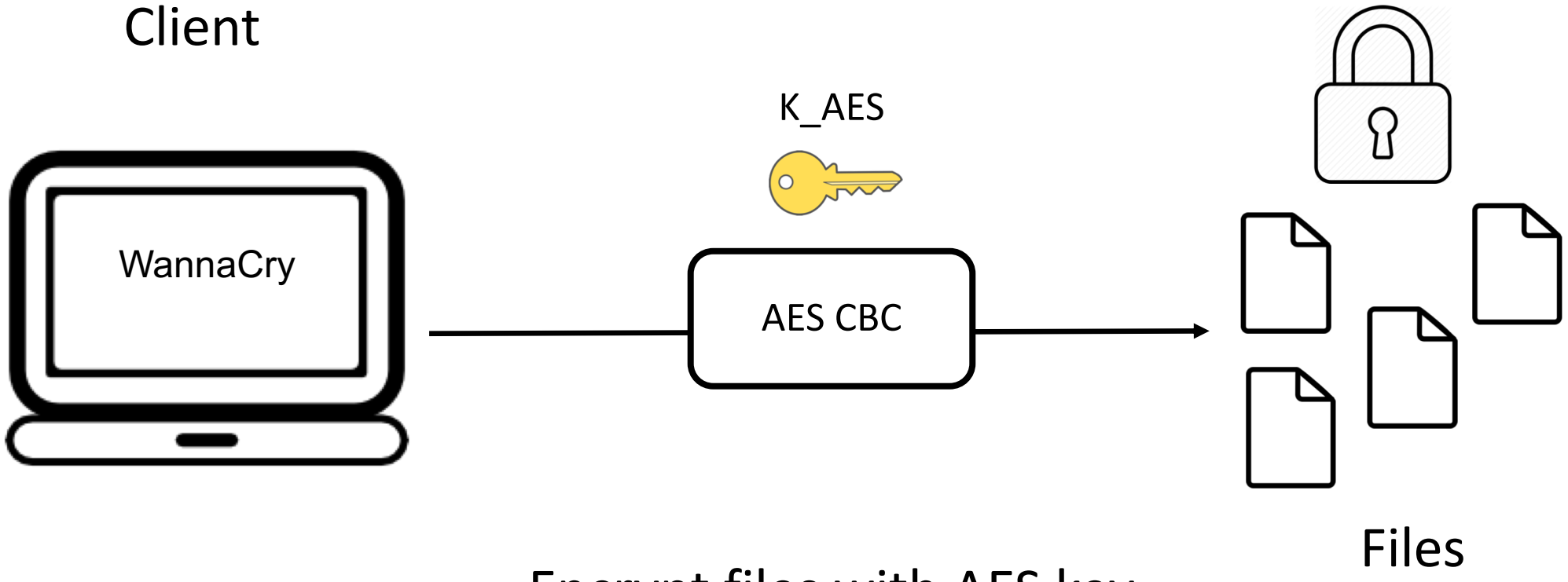
Server





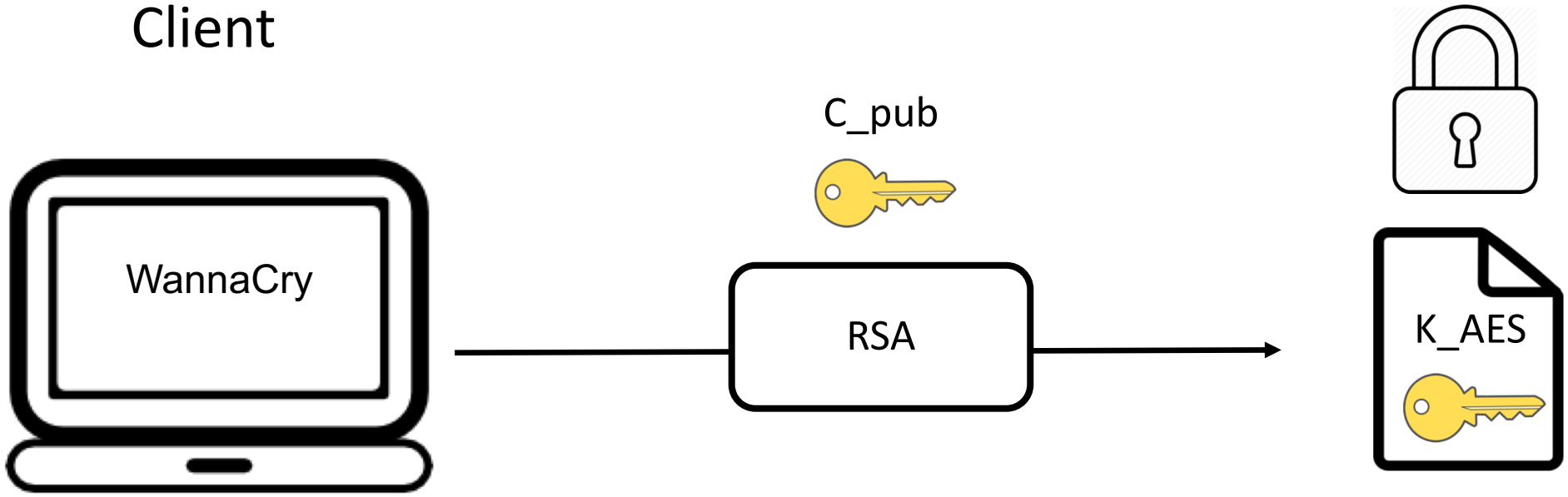
S_priv

WannaCry



Encrypt files with AES key

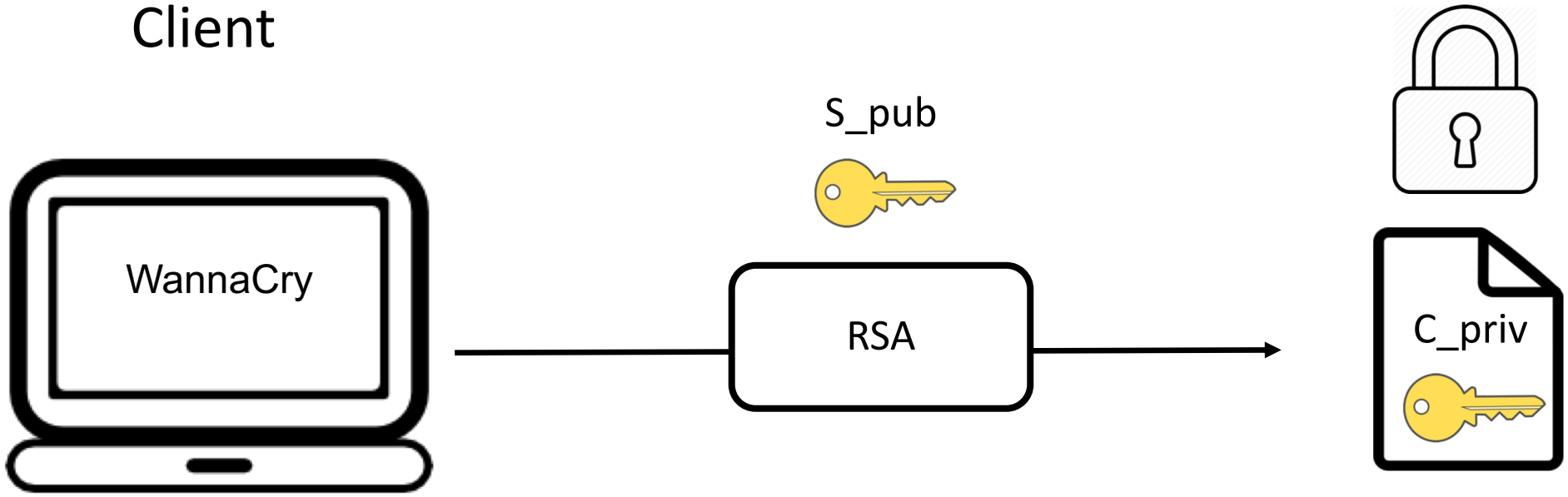
WannaCry



Encrypt AES key with asymmetric client’s public key

C_pub{K_AES}

WannaCry



Encrypt client's private key with server's public key and send to server

S_pub{C_priv}