Introduction to Security

Instructor: Khaled Diab

On Wednesday…

- ❑ Read the “how to read a paper”
- ❑ Read the “project startup document”
- ❑ Read and understand the syllabus
- ❑ Sign the Ethics form
- ❑ Get to know your classmates, and form project groups
- ❑ Start thinking about project ideas
- ❑ Prepare an answer for “What do you think security is?”

What is Security?

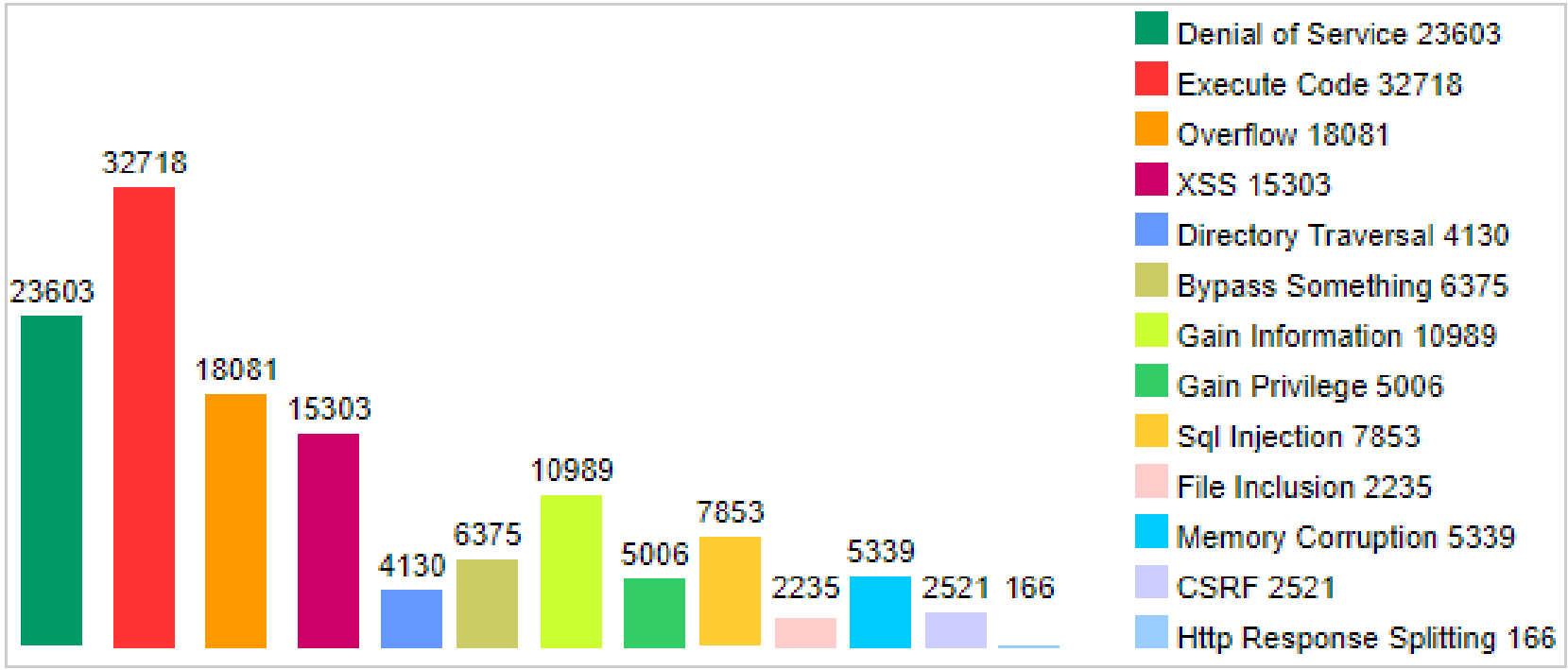
What is Security?

“Managing a malicious adversary [and] guaranteeing **properties** even if a malicious adversary tries to attack” – Adrian Perrig

Security is Hard

1. Lack of security-driven designs
   - For many software systems and network protocols
   - Focusing on functionality not security!
2. Finding vulnerability has become a business
3. Side-channel attacks
4. Too many threats
5. …

Lack of security-driven designs



https://www.cvedetails.com/vulnerabilities-by-types.php

Lack of security-driven designs

Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2019

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 All Time Leaders

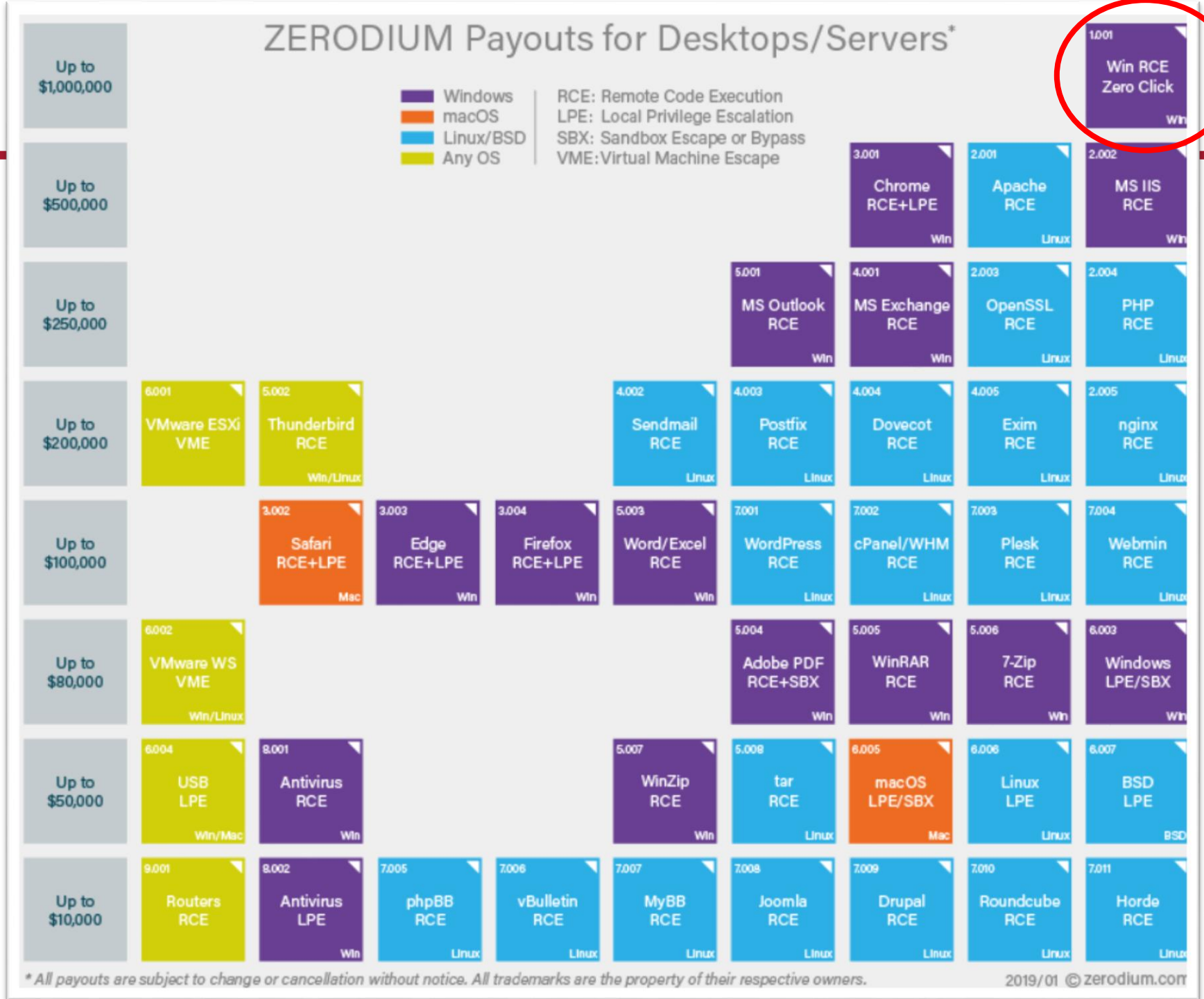
	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	414
2	Debian Linux	Debian	OS	360
3	Windows Server 2016	Microsoft	OS	357
4	Windows 10	Microsoft	OS	357
5	Windows Server 2019	Microsoft	OS	351
6	Acrobat Reader Dc	Adobe	Application	342
7	Acrobat Dc	Adobe	Application	342
8	Cpanel	Cpanel	Application	321
9	Windows 7	Microsoft	OS	250
10	Windows Server 2008	Microsoft	OS	248

https://www.cvedetails.com/top-50-products.php?year=2019

Finding vulnerability has become a business

- 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)

- Acquiring vulnerabilities
  - Zerodium: up to $2M for iOS, $500K for Android

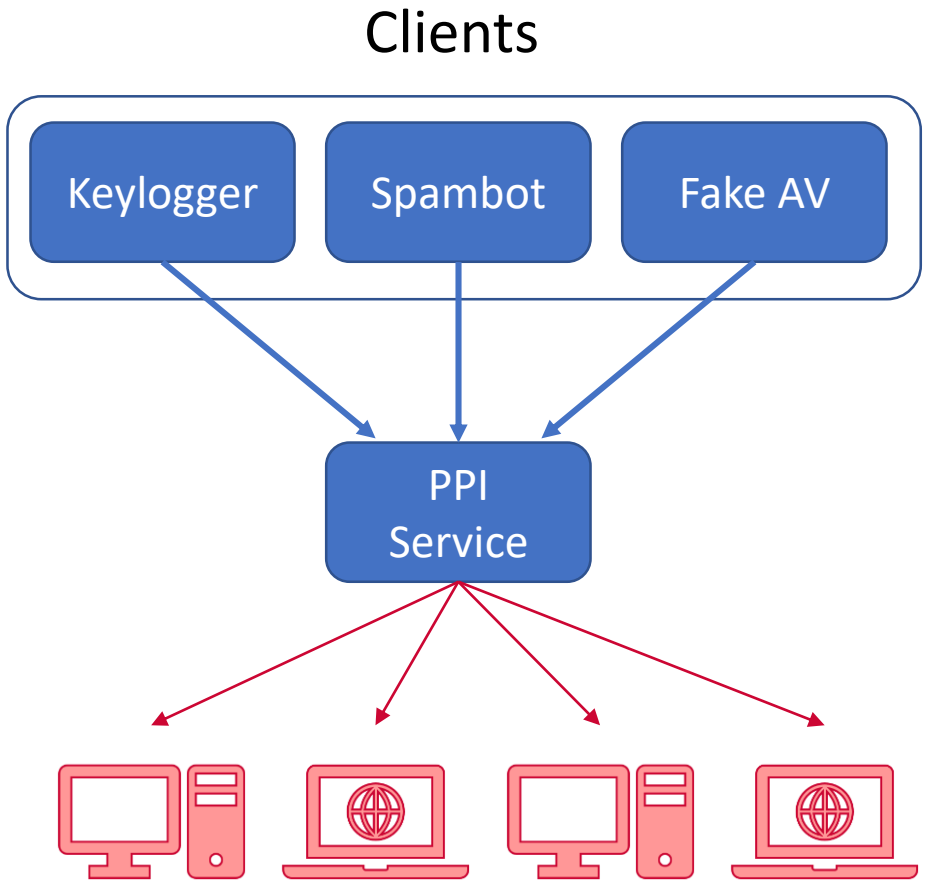

ZERODIUM Payouts for Desktops/Servers*
Windows
macOS
Linux/BSD
Any OS
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape
Up to $1,000,000
1.001 Win RCE Zero Click Win
Up to $500,000
3.001 Chrome RCE+LPE Win
2.001 Apache RCE Linux
2.002 MS IIS RCE Win
Up to $250,000
5.001 MS Outlook RCE Win
4.001 MS Exchange RCE Win
2.003 OpenSSL RCE Linux
2.004 PHP RCE Linux
Up to $200,000
6.001 VMware ESXi VME
5.002 Thunderbird RCE Win/Linux
4.002 Sendmail RCE Linux
4.003 Postfix RCE Linux
4.004 Dovecot RCE Linux
4.005 Exim RCE Linux
2.005 nginx RCE Linux
Up to $100,000
3.002 Safari RCE+LPE Mac
3.003 Edge RCE+LPE Win
3.004 Firefox RCE+LPE Win
5.003 Word/Excel RCE Win
7.001 WordPress RCE Linux
7.002 cPanel/WHM RCE Linux
7.003 Plesk RCE Linux
7.004 Webmin RCE Linux
Up to $80,000
6.002 VMware WS VME Win/Linux
5.004 Adobe PDF RCE+SBX Win
5.005 WinRAR RCE Win
5.006 7-Zip RCE Win
6.003 Windows LPE/SBX Win
Up to $50,000
6.004 USB LPE Win/Mac
8.001 Antivirus RCE Win
5.007 WinZip RCE Win
5.008 tar RCE Linux
6.005 macOS LPE/SBX Mac
6.006 Linux LPE Linux
6.007 BSD LPE BSD
Up to $10,000
9.001 Routers RCE
8.002 Antivirus LPE Win
7.005 phpBB RCE Linux
7.006 vBulletin RCE Linux
7.007 MyBB RCE Linux
7.008 Joomla RCE Linux
7.009 Drupal RCE Linux
7.010 Roundcube RCE Linux
7.011 Horde RCE Linux
* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.
2019/01 © zerodium.com

…or even worse: A Marketplace for owned machines

- Pay-per-install (PPI) services

- PPI operation:

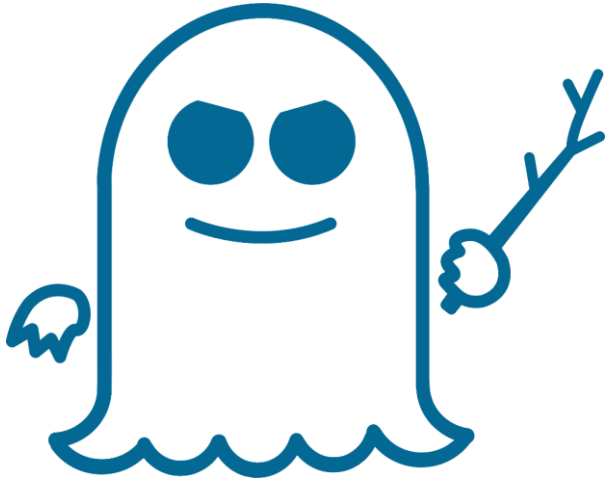
1. Own victim machine
2. Download and install client program
3. Charge client



Cabalerro et al. (www.icir.org/vern/papers/ppi-usesec11.pdf)

Side-channel attacks

- Attacks that are based on implementation of a system
  - Timing attacks
  - Power analysis attacks
  - Electromagnetic attacks
  - Caching attacks



Too many threats…

- Consider the Internet
  - Every host, router, middlebox is a potential threat
  - Esp. when they become Zombies

Threat Modelling

- There is no such thing as perfect security!
  - Risk management is a critical activity in security.

- Defining security per context; identify:
  - assets,
  - adversaries and motivations,
  - threats,
  - vulnerabilities,
  - risk, and
  - possible defenses.

Threat Modelling

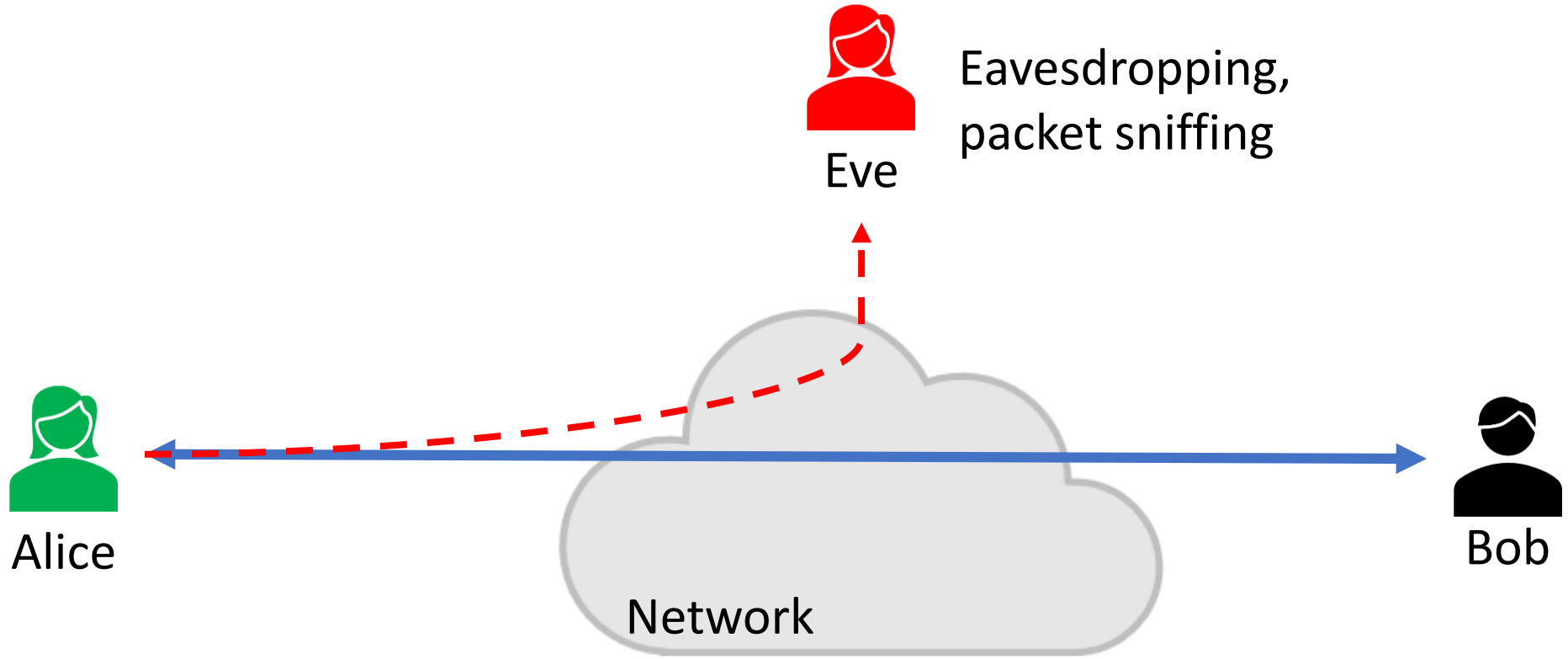
- Assets:
  - What are we trying to protect? How valuable are those assets?
- Adversaries:
  - Who might try to attack, and why?
- Vulnerabilities:
  - How might the system be weak?
- Threats:
  - What actions might an adversary take to exploit vulnerabilities?
- Risk:
  - How important are assets? How likely is exploit?
- Possible Defenses

Security Goals

- Common general security goals: “CIA”
  - **C**onfidentiality
  - **I**ntegrity
  - **A**uthenticity
  - Availability

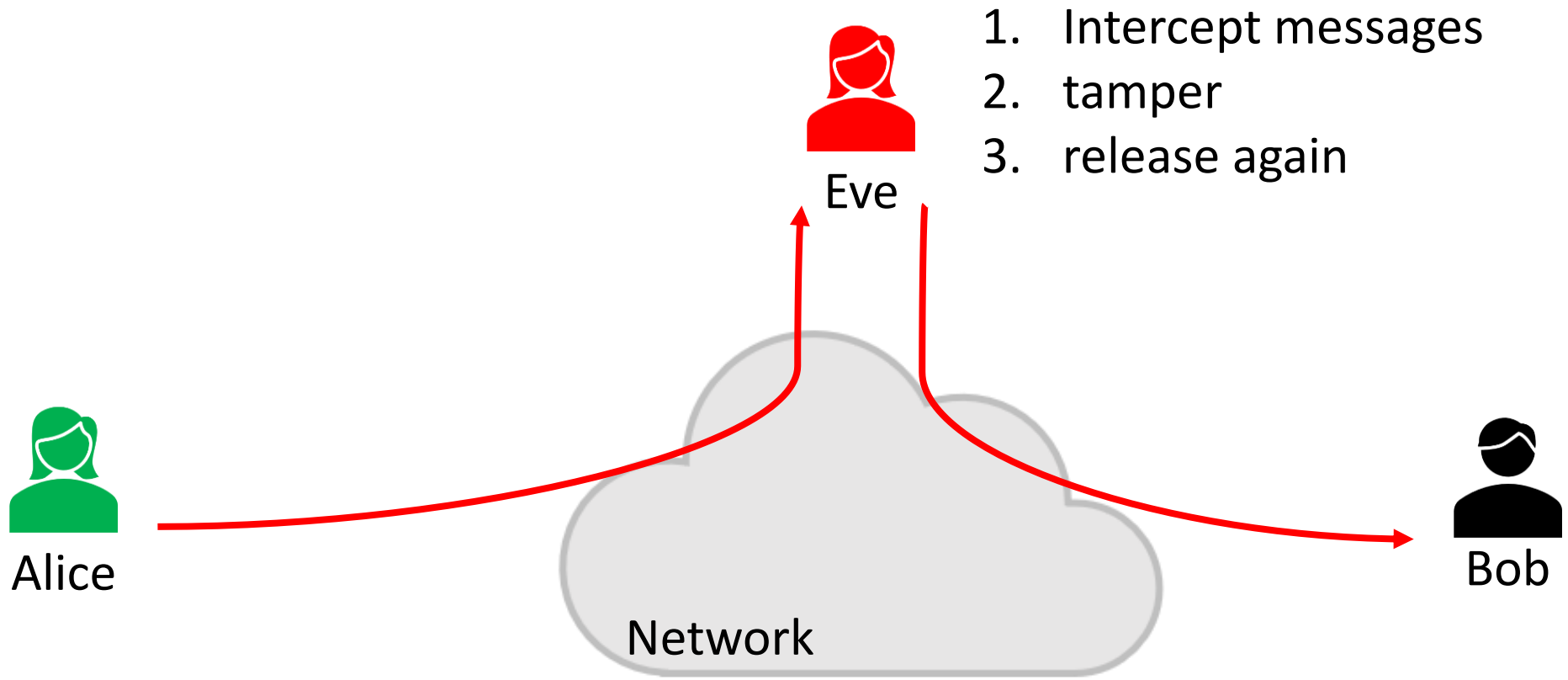
Confidentiality (Privacy)

- Confidentiality is **concealment of information**.



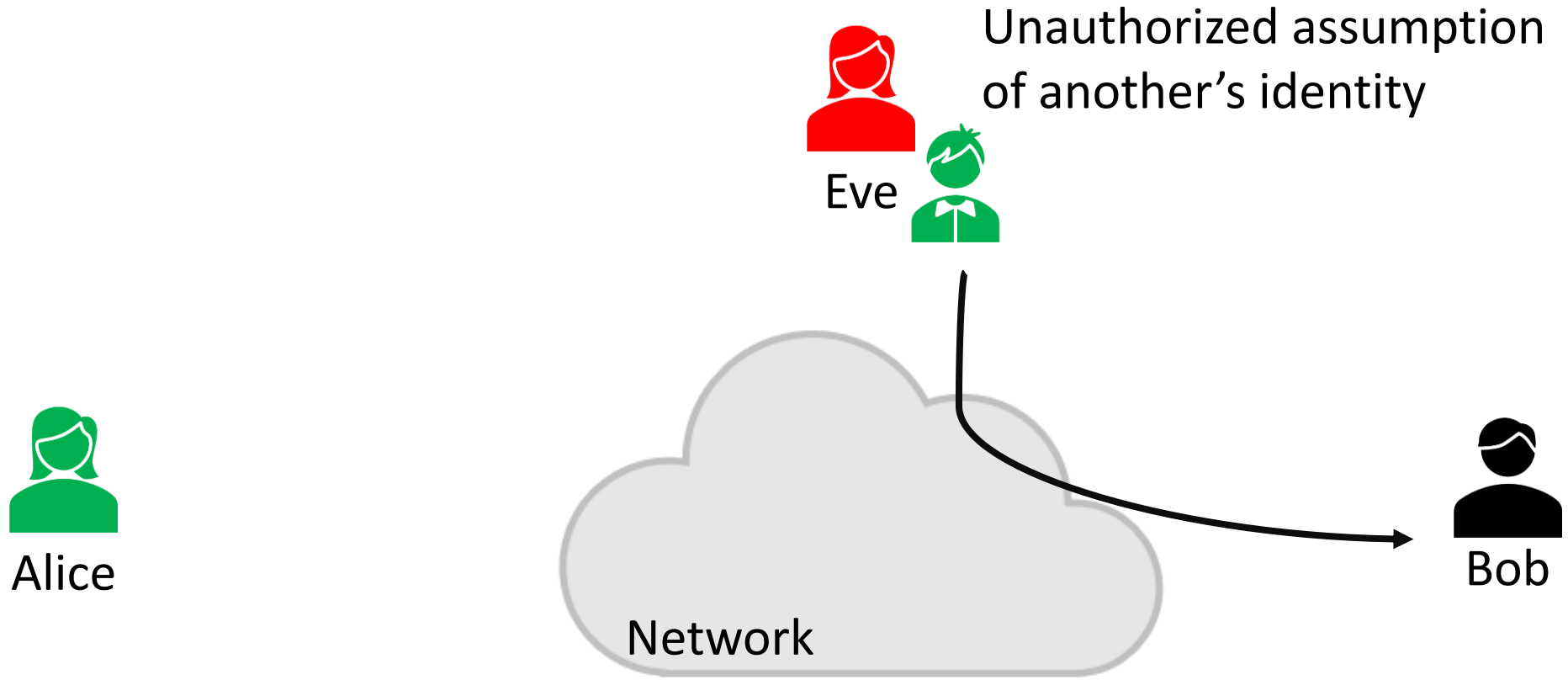
Integrity

- Integrity is **prevention of unauthorized changes.**



Authenticity

- Authenticity is **knowing who you are talking to.**

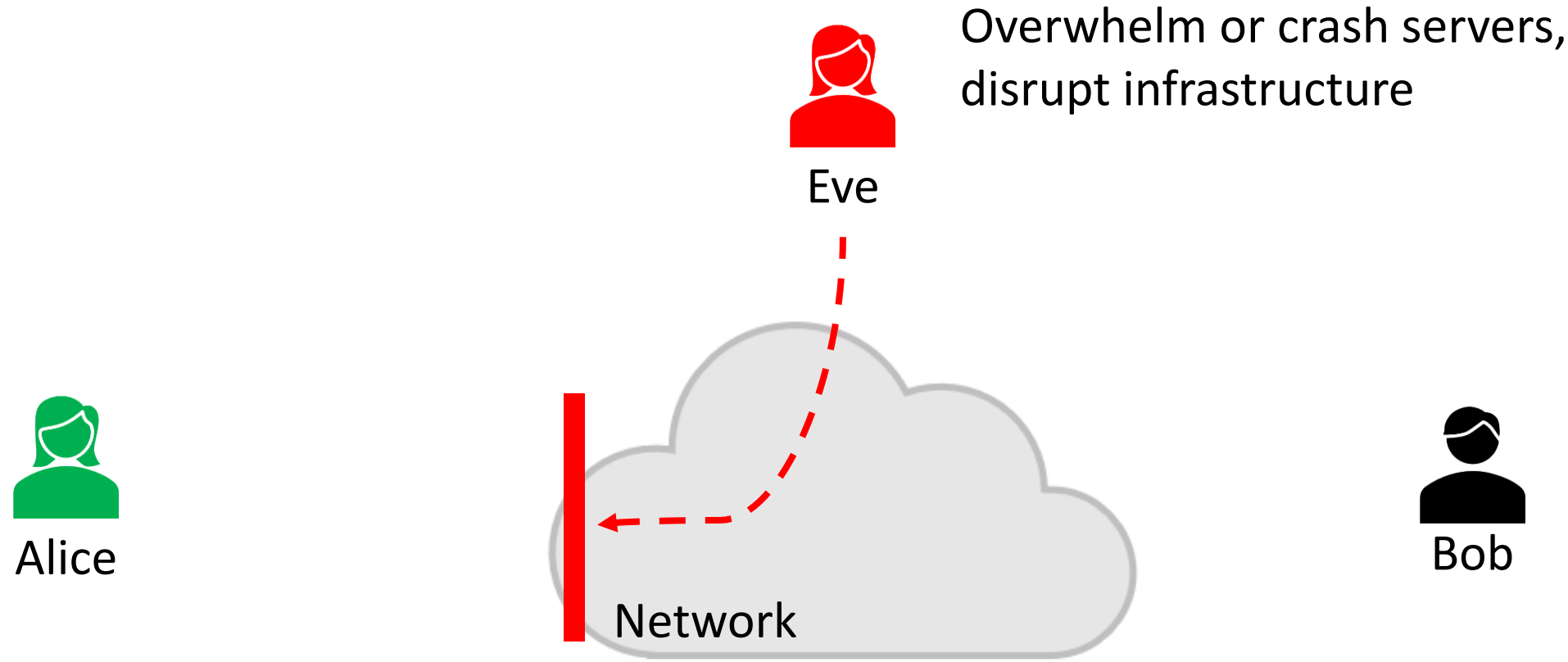


Authenticity

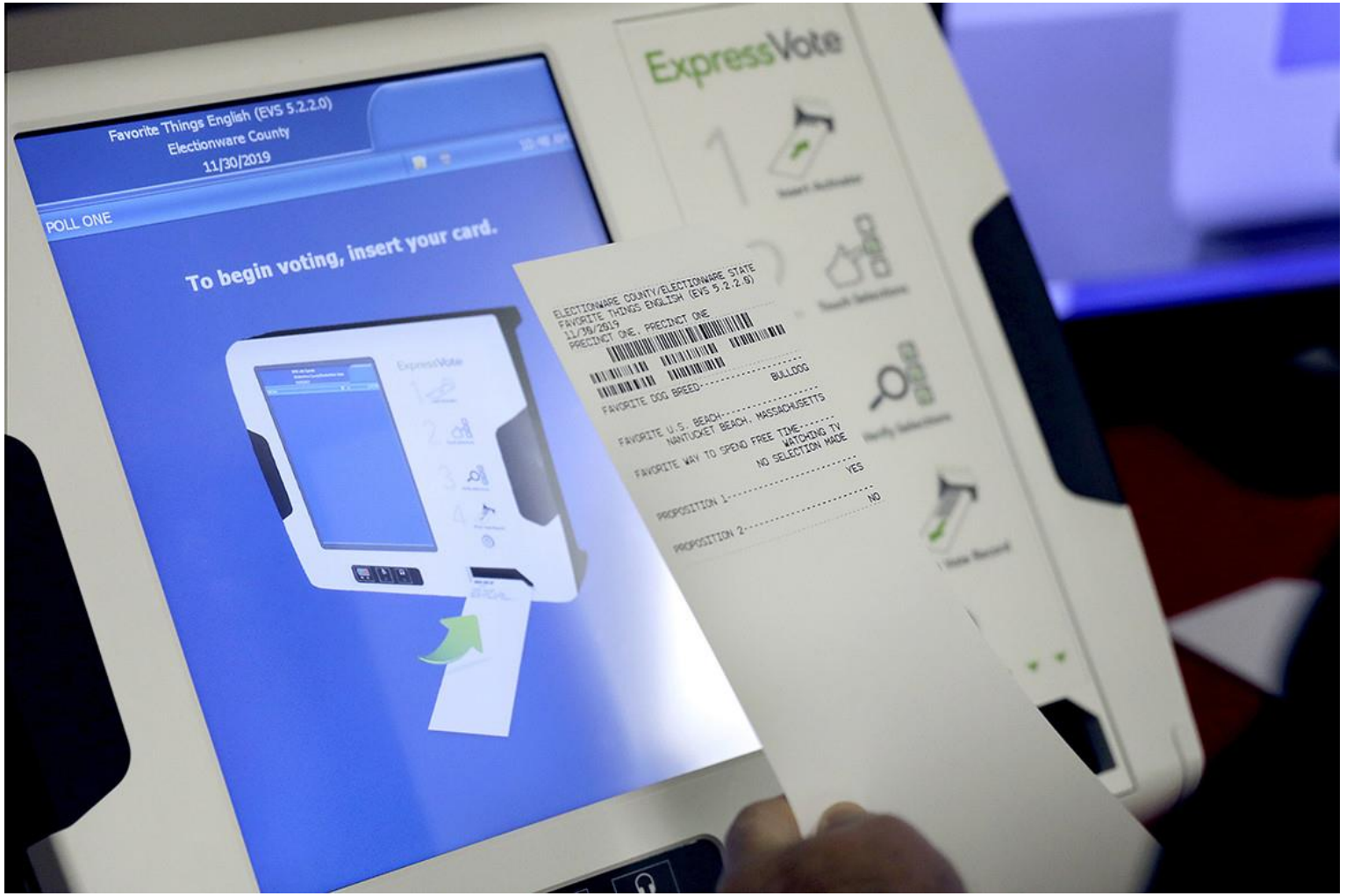
"On the Internet, nobody knows you're a dog."

Availability

- Availability is **ability to use information or resources.**



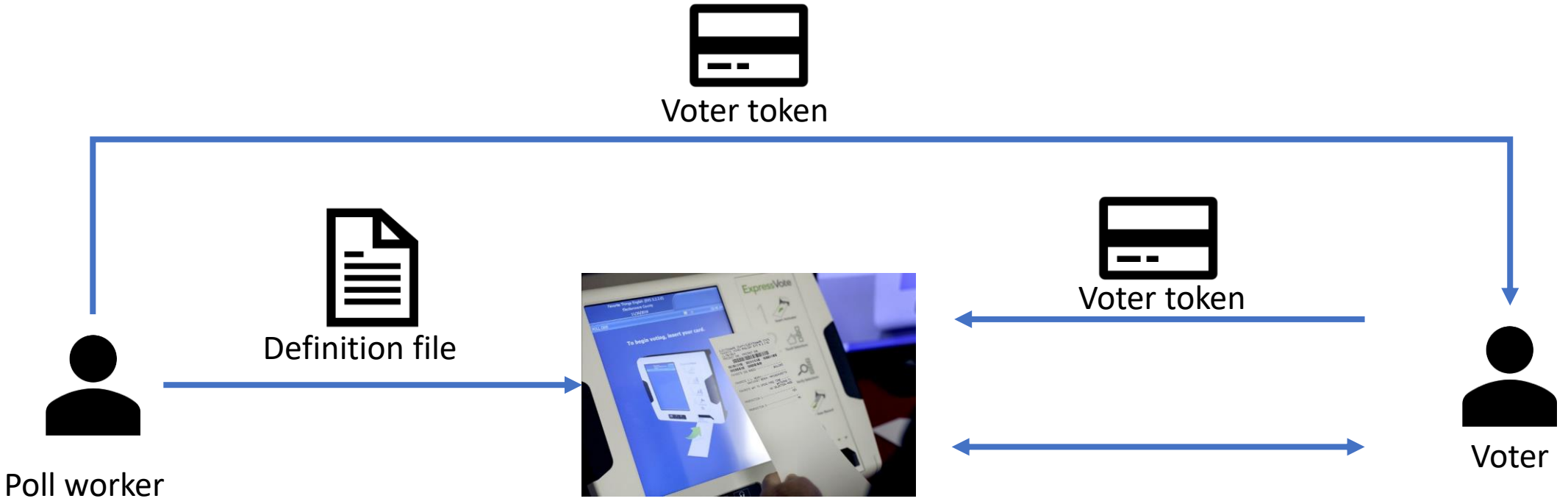
Threat Modeling Example: Electronic Voting



Pre-Election

Pre-election: Poll workers load “ballot definition files” on voting machine.

Active Voting

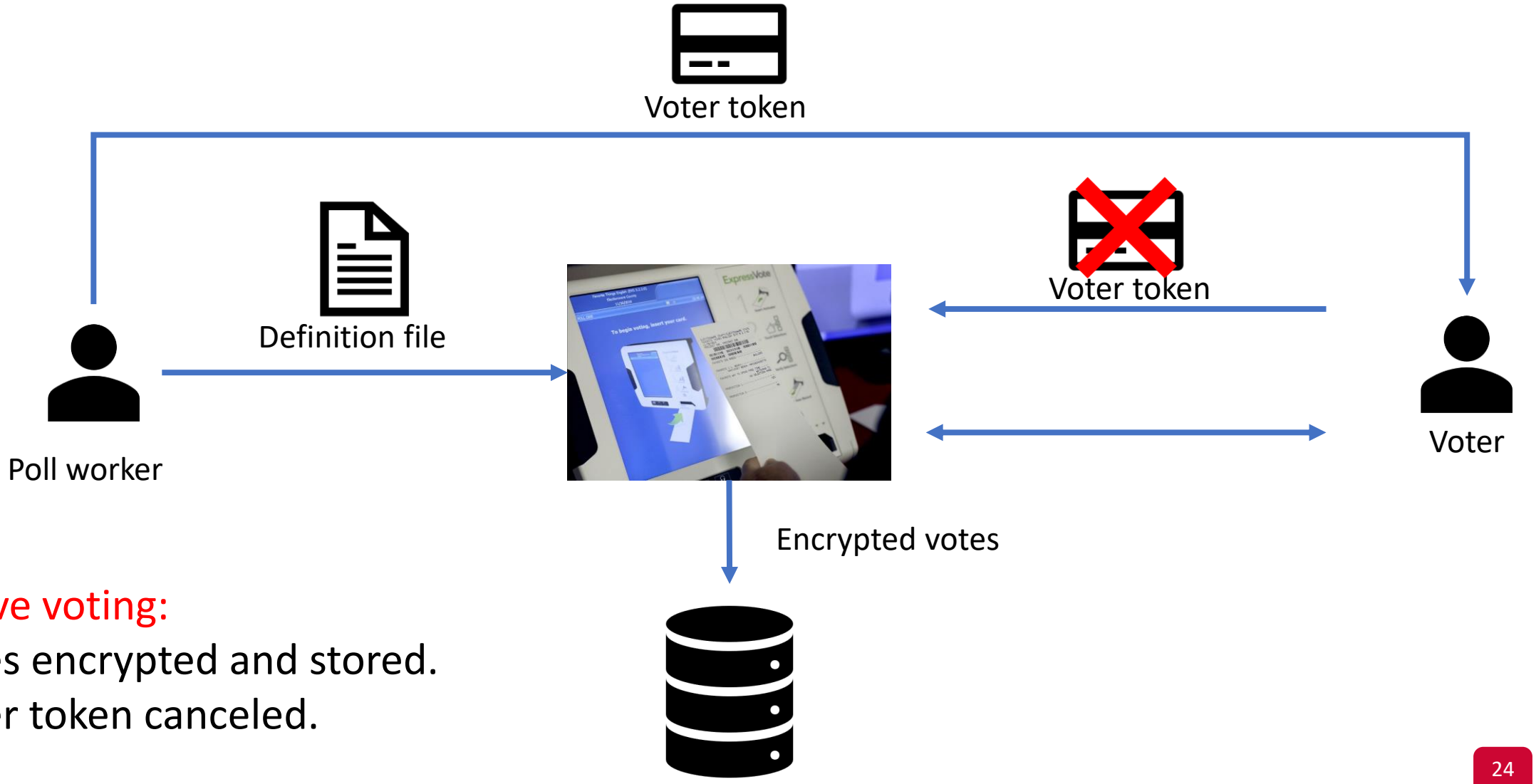


Active voting:

Voters obtain **single-use** tokens from poll workers.

Voters use tokens to activate machines and vote.

Active Voting

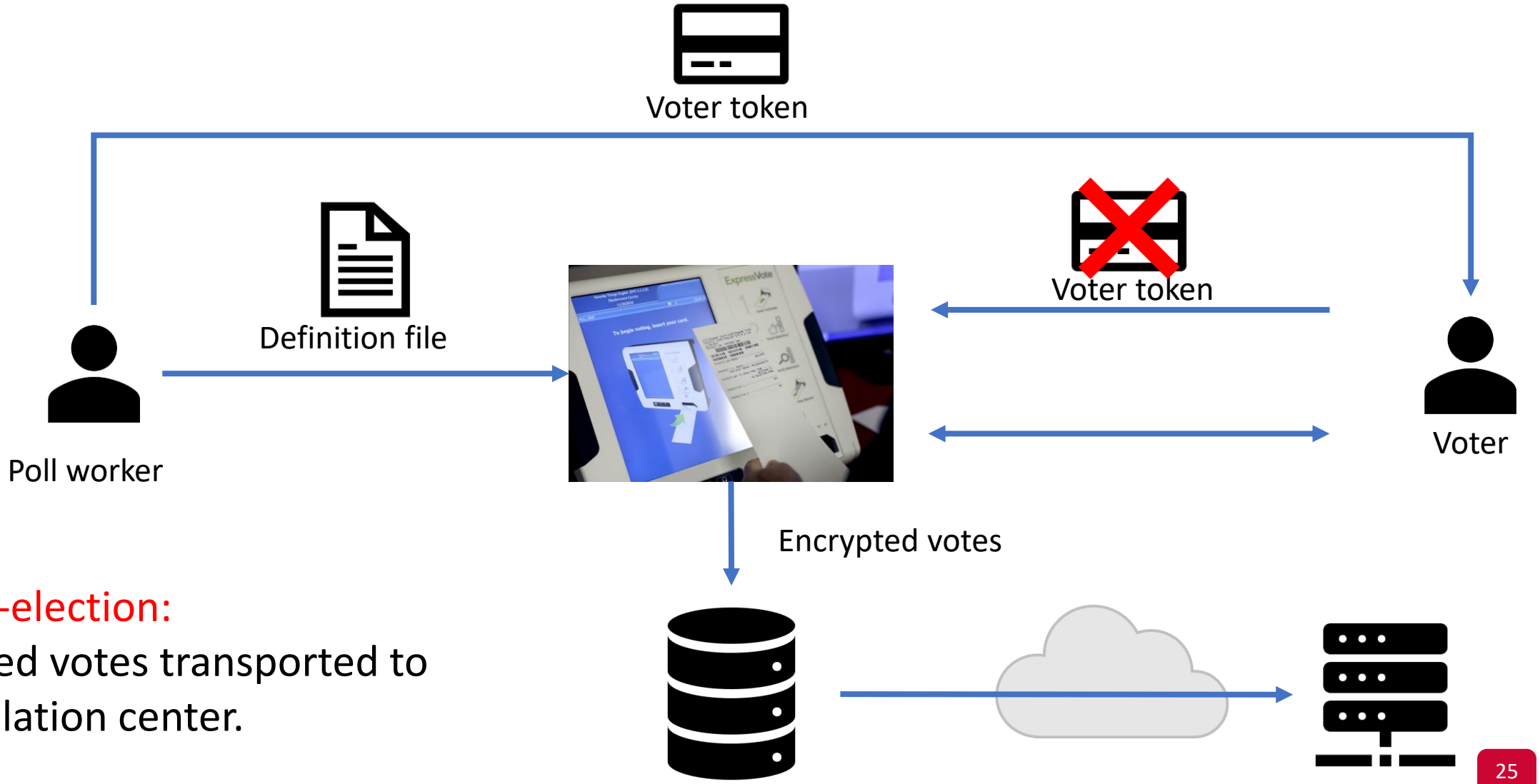


Active voting:

Votes encrypted and stored.

Voter token canceled.

Post-Election



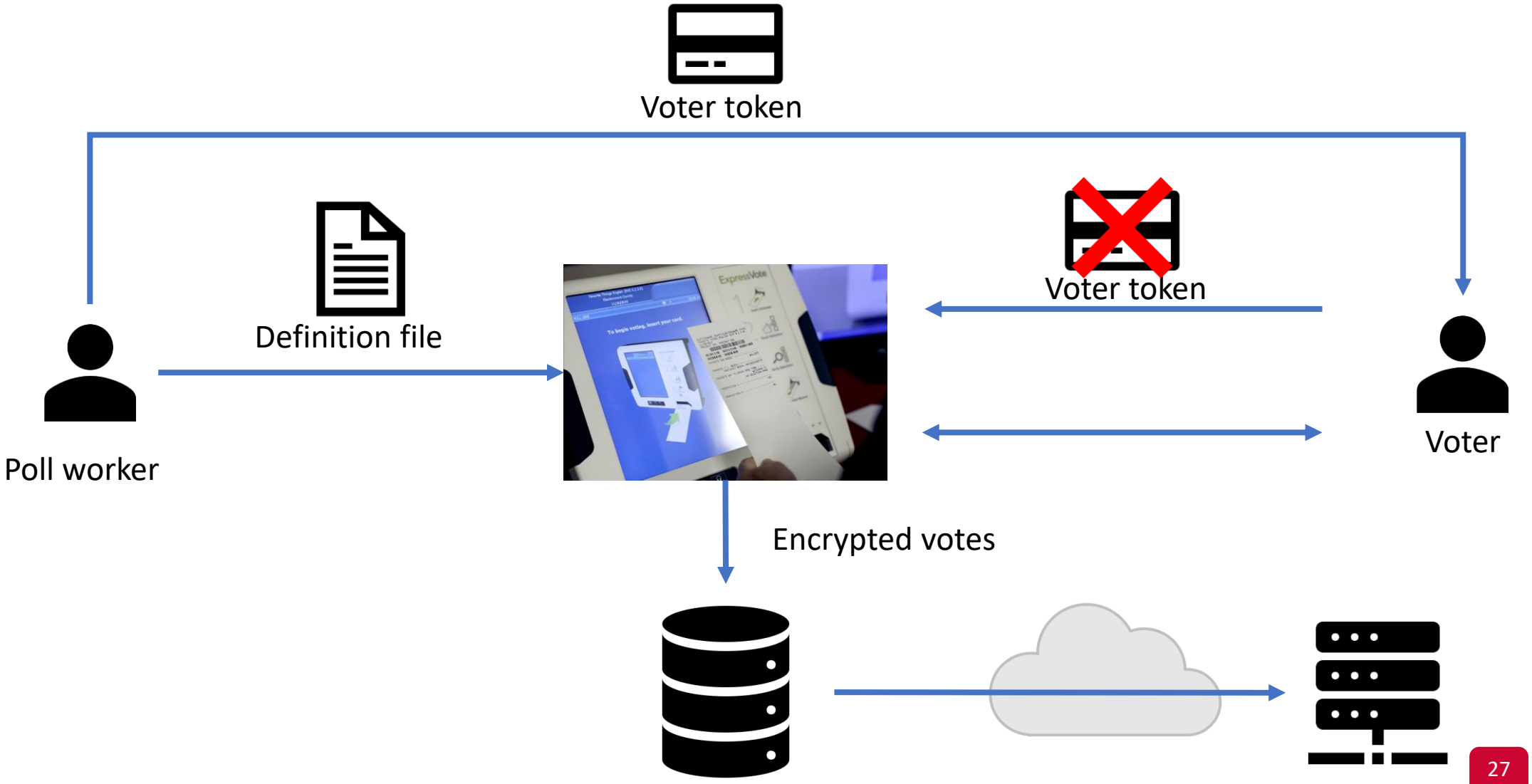
Post-election:

Stored votes transported to tabulation center.

eVoting Security

- Security goals:
  - Adversary should not be able to tamper with the election outcome
    - By changing votes (**integrity**)
    - By voting on behalf of someone (**authenticity**)
    - By denying voters the right to vote (**availability**)
  - Adversary should not be able to figure out how voters vote (**confidentiality**)

What are the potential concerns?



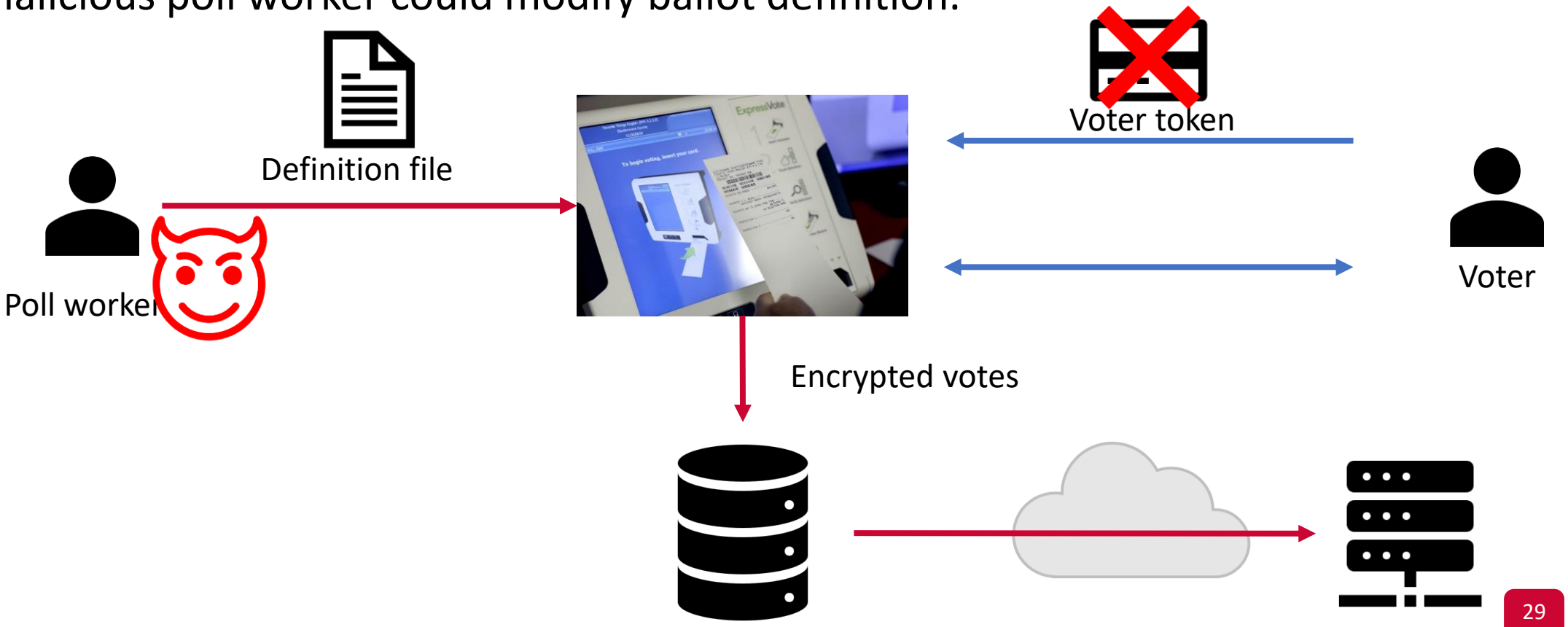
Potential Adversaries

- Voters
- Election officials
- Employees of voting machine manufacturer
  - Software/hardware engineers
  - Maintenance people
- Other engineers
  - Makers of hardware
  - Makers of underlying software or add-on components
  - Makers of compiler
- …

Examples

Problem: Ballot definition files are not authenticated.

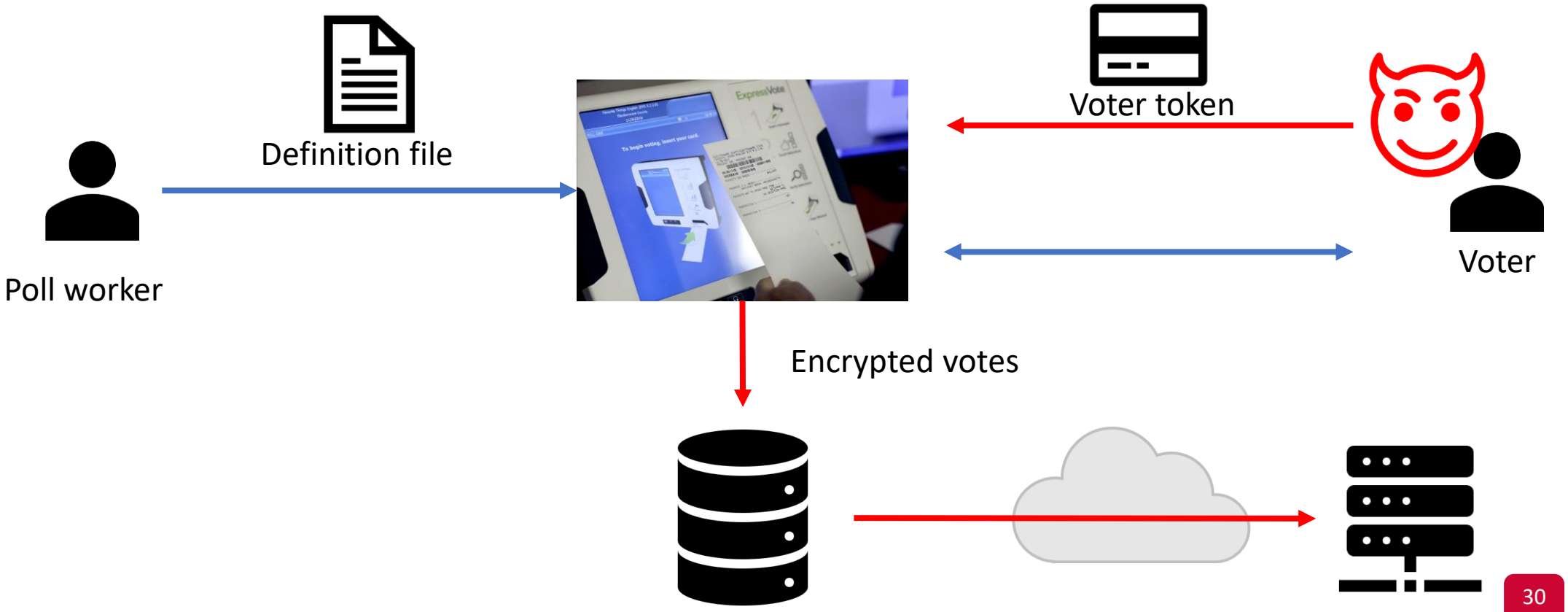
Example attack:
A malicious poll worker could modify ballot definition.



Examples

Problem: Smartcards can perform cryptographic operations. But there is no authentication from voter token to terminal.

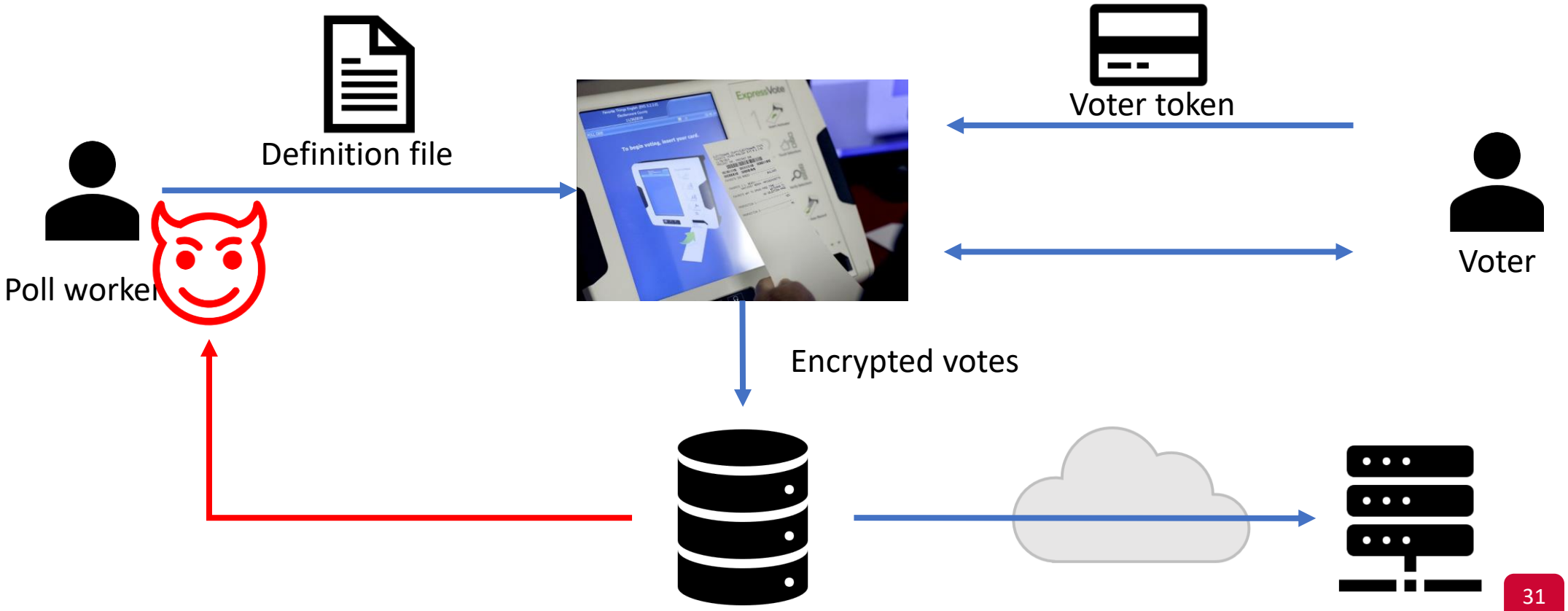
Example attack: A regular voter could make his or her own voter token and vote multiple times.



Examples

Problem: Votes stored in the order cast.

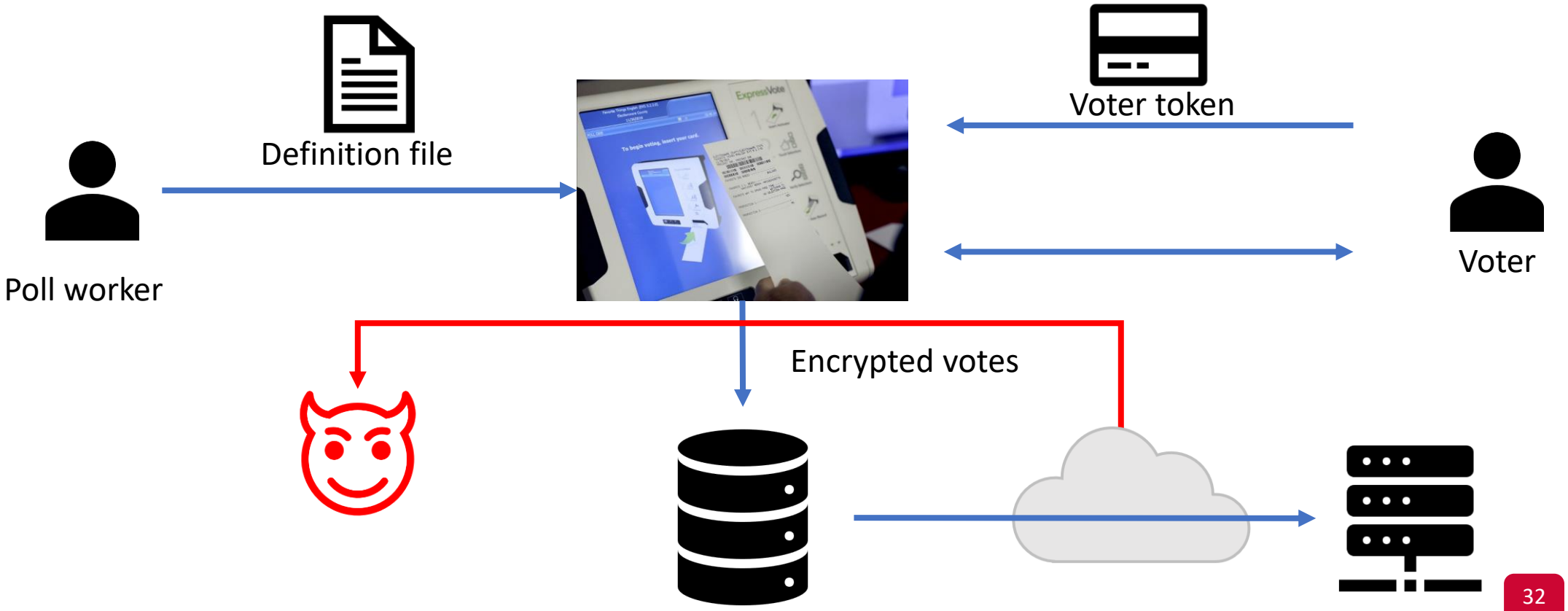
Example attack: A poll worker could determine how voters vote.



Examples

Problem: When votes transmitted to server, they are decrypted first; the cleartext results are sent the server.

Example attack: A sophisticated outsider could determine how voters vote.



Security Approaches

- Prevention
  - Stop an attack
- Detection
  - Detect an ongoing or past attack
- Incident Response
  - Respond to attacks

Prevention

- Preventing an incident requires careful analysis and planning:
- Design and implementation of:
  - Security policies
  - Security awareness
  - Access controls

Detection

- Perfect security is impossible

→*no matter what level of protection a system may have it will get compromised*

- Timely detection and notification of a compromise is critical

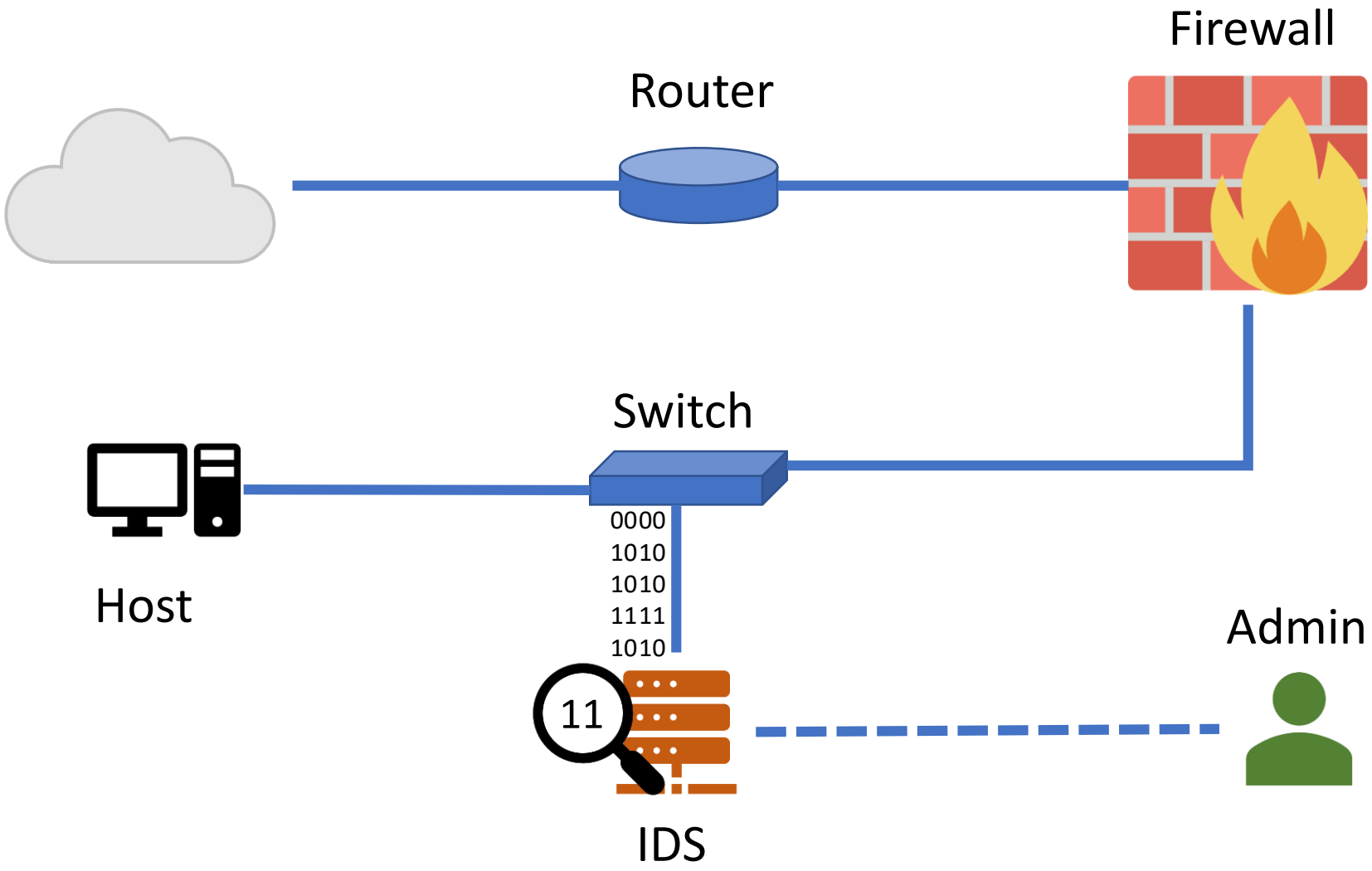
→*Intrusion Detection Systems (IDS)*

Intrusion Detection Systems

- Alarm with brains
- Imagine a fire alarm that had the capability of:
  - detecting a fire,
  - distinguish the type of fire,
  - pinpoint its source and path,
  - alert the building occupants and fire department,
  - and forward intelligence to the firehouse prior to their response.
- All of this while distinguishing normal activity such as bad cooking!

Intrusion Detection Systems

- IDS should be strategically placed at the network and application levels



Intrusion Detection Systems

- Monitoring and notification
- Detecting attack signatures and also changes in files, configurations and activity
- IDS must have the ability to distinguish normal system activity from malicious activity.
  - FPs → too many alarms
  - FNs → too many undetected attacks

Technical Enablers

- Crypto
- Roots of trust
  - Trusted hardware
  - Trusted hypervisor
- Program Analysis/Verification
- (Anomaly) Detection Algorithms

Crypto Primitives

1. Encryption/Decryption

2. Digital Signatures

3. One-way hash fun

- Applications?

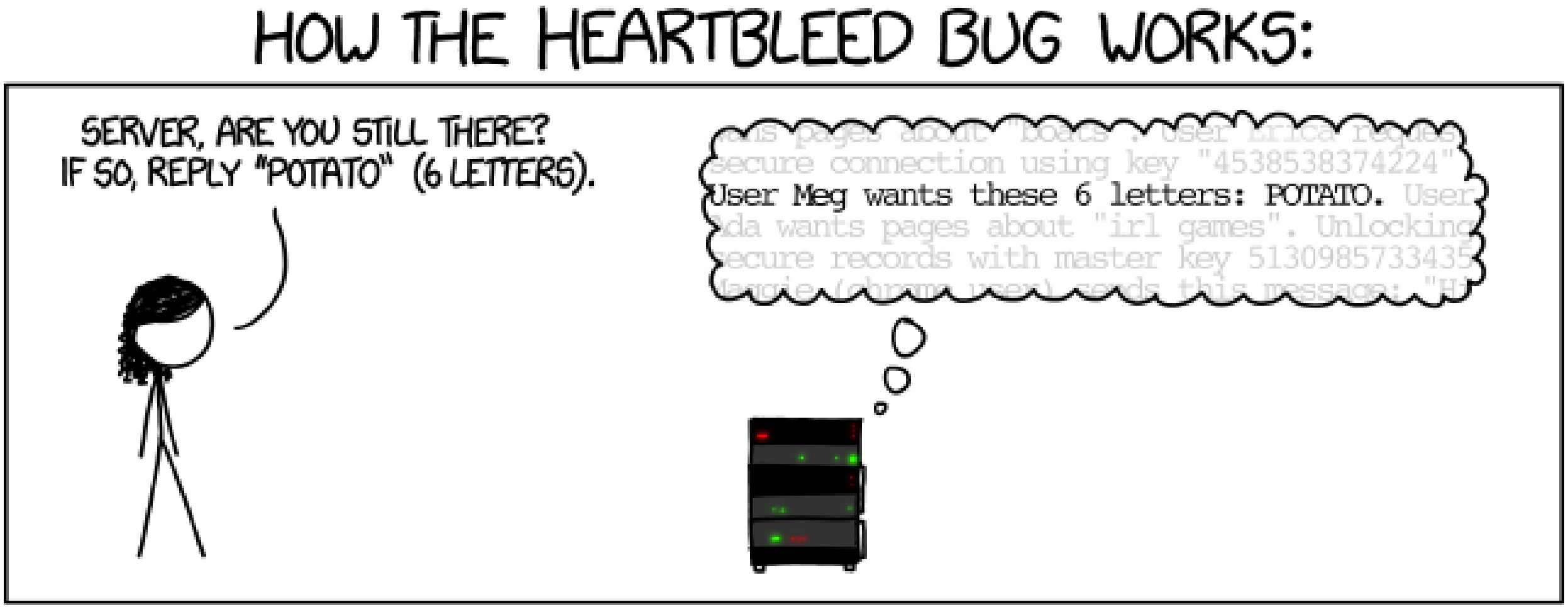
Crypto != Security

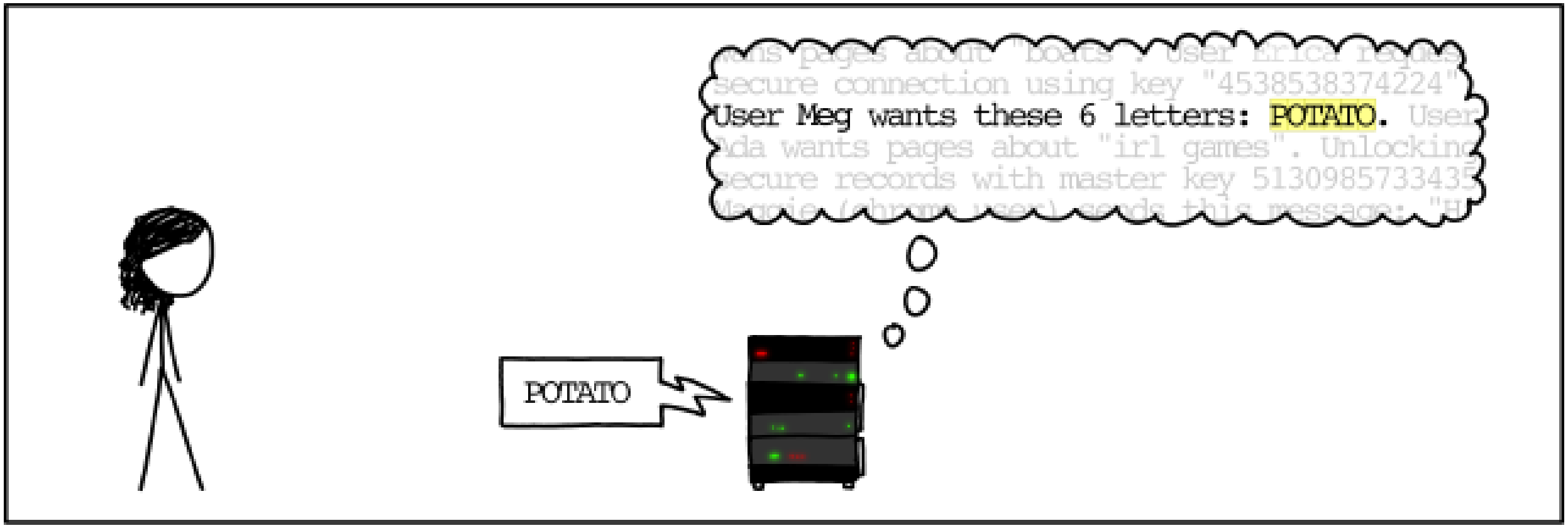
- Key technology enabler, but ..

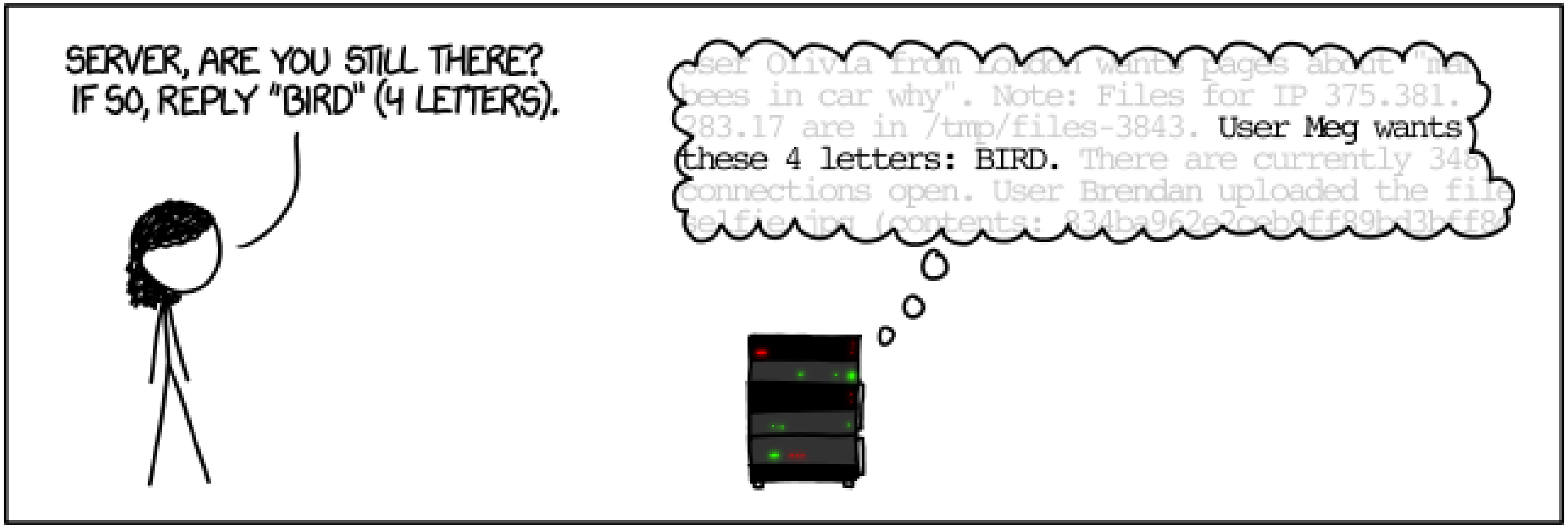
- Many other things could go wrong

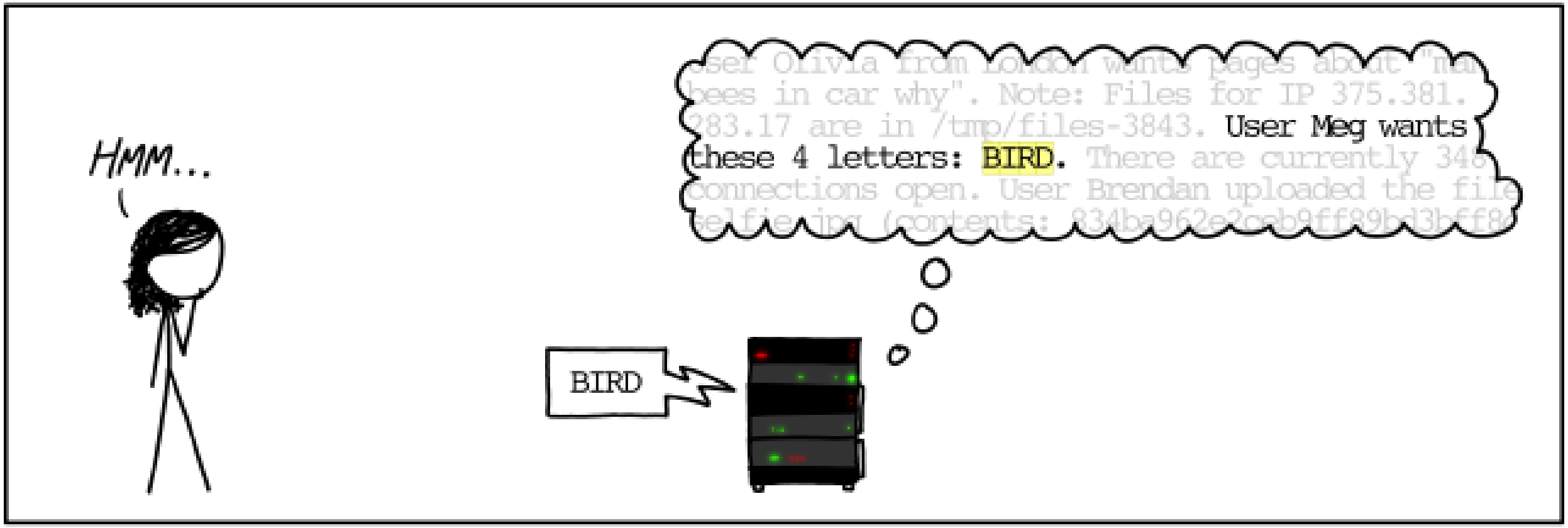
- Crypto Implementation vulnerabilities
- Architectural flaws
- Insider threats
- …

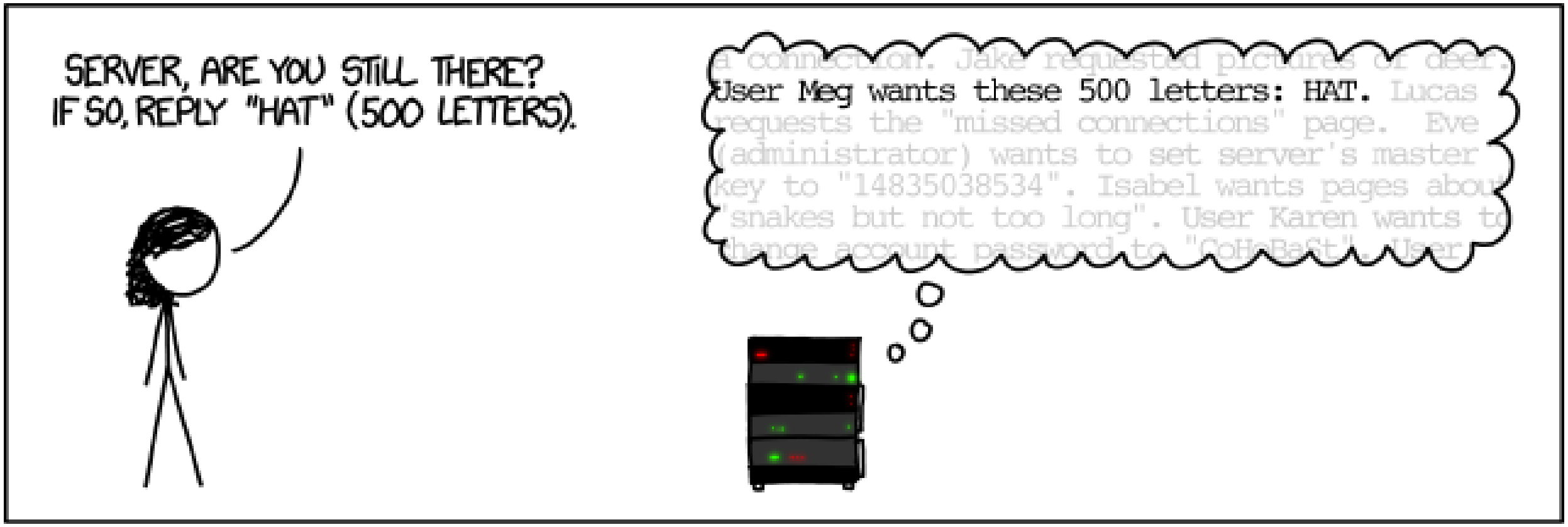
Heartbleed

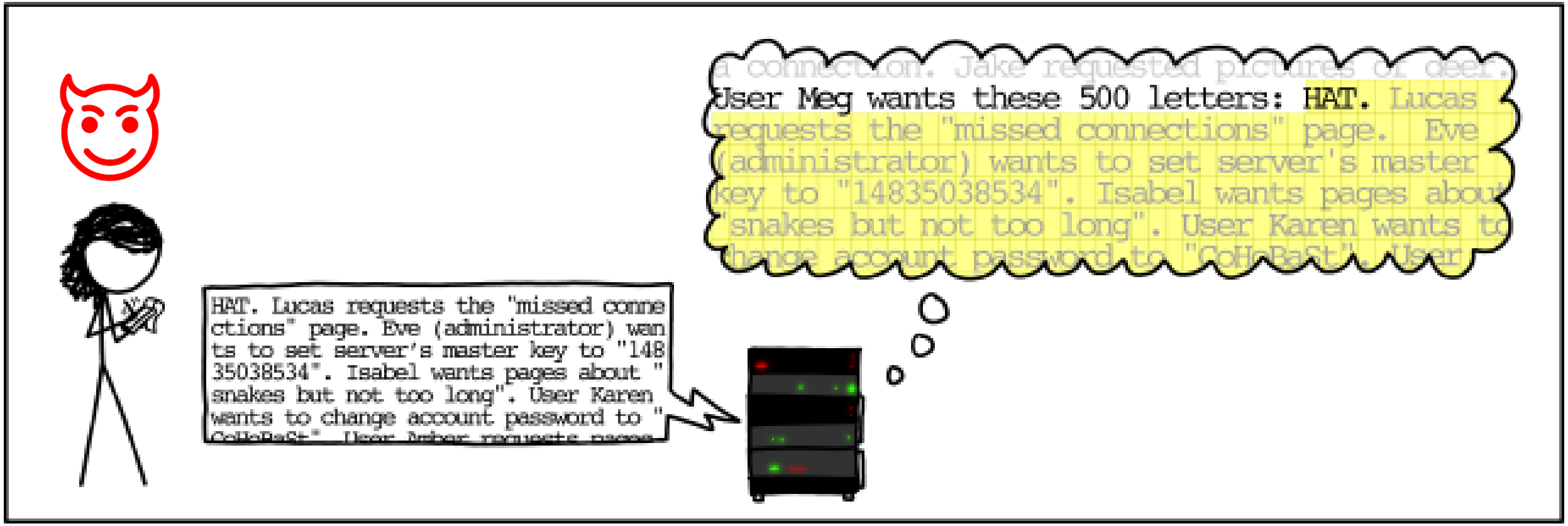

HOW THE HEARTBLEED BUG WORKS:
SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).
User Meg wants these 6 letters: POTATO.


User Meg wants these 6 letters: POTATO.
POTATO


SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).
these 4 letters: BIRD.


HMM...
User Olivia from London wants pages about "man 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: 834ba962e2ceb9ff89bd3bff8
BIRD


SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
User Meg wants these 500 letters: HAT.


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 "
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

Attacker Asymmetric Advantage

Attacker Asymmetric Advantage

- Attacker only needs to win in one place
- Defender’s response: Defense at every layer

Whole System is Critical

- Securing a system involves a whole-system view
  - Cryptography
  - Implementation
  - People
  - Physical security
  - Everything in between

- No reason to attack the strongest part of a system if you can walk right around it.

Linux Backdoor

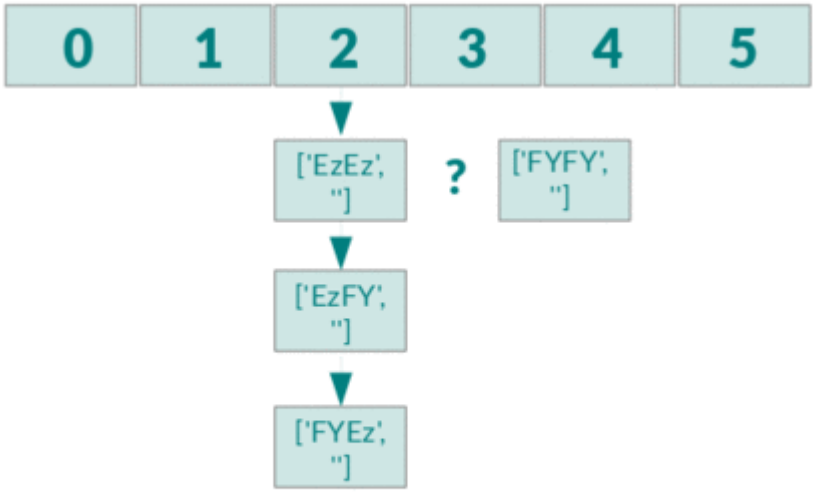
```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
        retval = -EINVAL;
```

- Was never pushed to Linux master copy in BitKeeper
- Was noticed by a developer in CVS

https://lwn.net/Articles/57137/
https://freedom-to-tinker.com/2013/10/09/the-linux-backdoor-attempt-of-2003/

PHP Hash Collision DoS

- PHP stores arrays using hash tables
- If an attacker controls the input in a specific way, all the inputs will collide



- number of elements to traverse is quadratic (for every insertion)

→ more CPU cycles (3000X delay compared to normal operation)

→ Resulting in a DoS attack

https://fahrplan.events.ccc.de/congress/2011/Fahrplan/attachments/2007_28C3_Effective_DoS_on_web_application_platforms.pdf

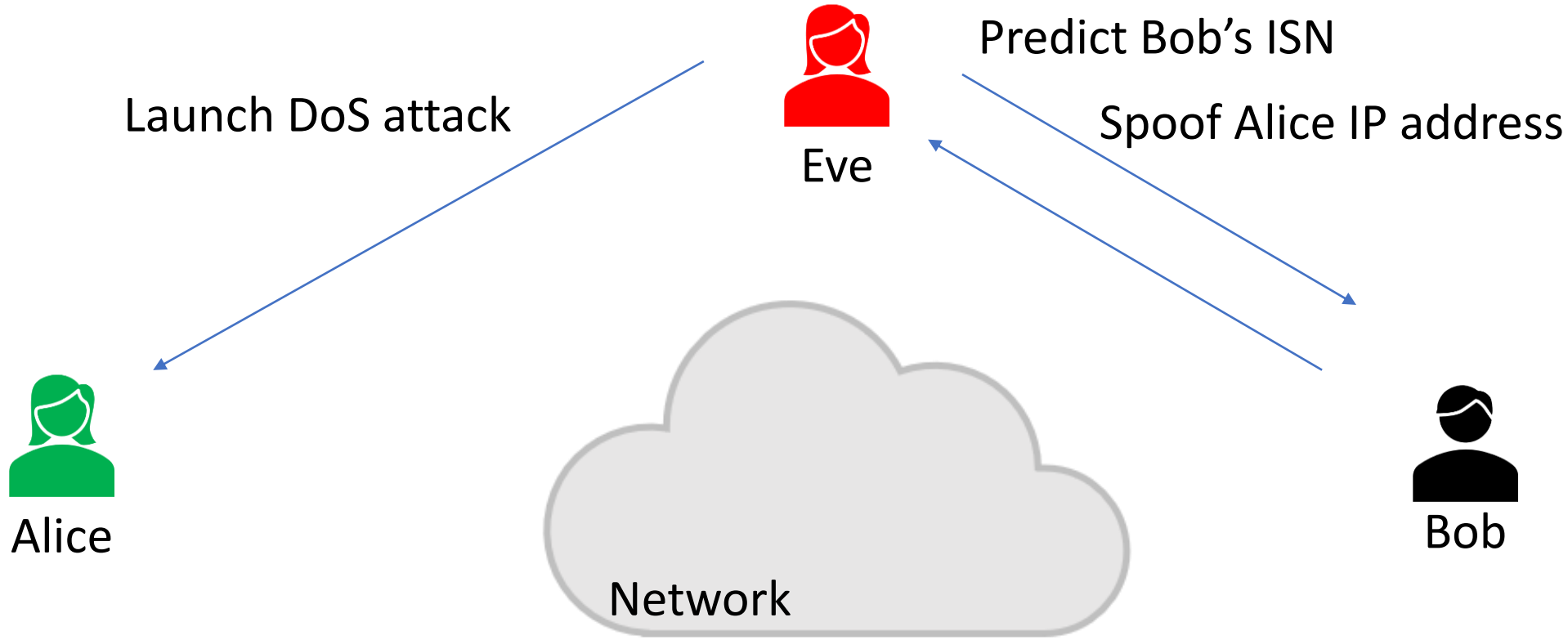
PHP Hash Collision DoS

- How did PHP solve this problem?
  - Set max. number of inputs

- Is this a good solution?
- What is the root cause of the attack?
- How do other languages address this vulnerability?

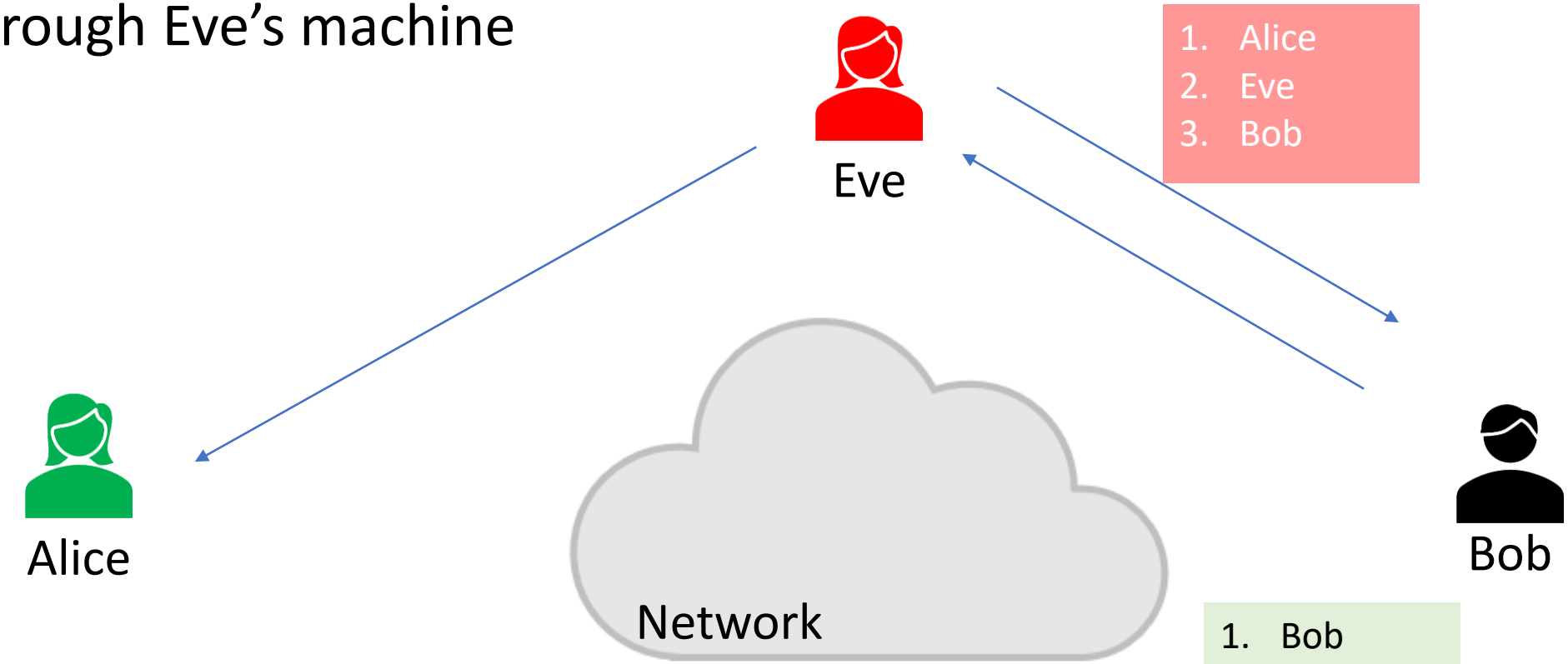
TCP Sequence Number Prediction

- All TCP packets are numbered with a seq. number
  - Starting from an initial seq. number (ISN)



IP Source Routing Attack

- Eve constructs a source-routed packet.
- Includes her IP address in the route, any response from Bob will pass through Eve's machine



Next Lecture

- Read “x86 Assembly Guide”

Acknowledgment

- Some of today's slides are based on or adapted from Franziska (Franzi) Roesner slides.