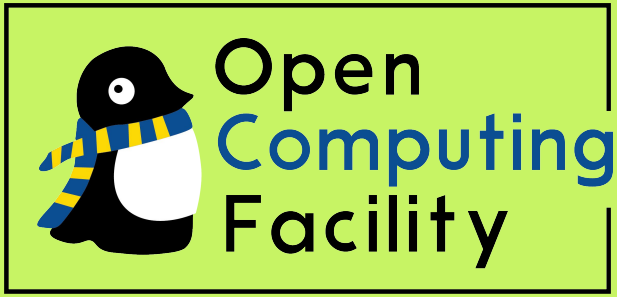


Security Fundamentals

Lecture 7

trinityc

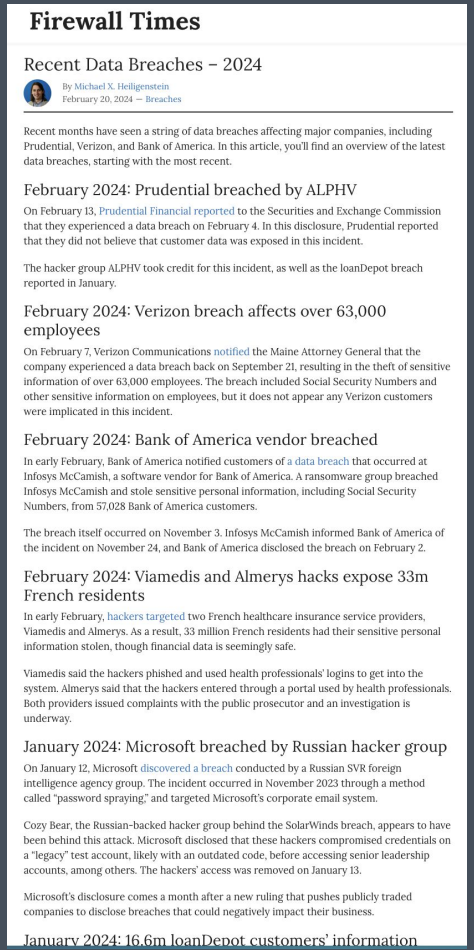
(slide credits abizer, longlian, ning, billqmao)

Security Introduction

- Why do we care?
- Basic Principles
- Security Goals
  - Confidentiality
  - Integrity
  - Authentication
  - Availability

Why do we care?

- Basic government functions at risk:
  - Voting security sucks (2018)
- Hospitals suffering from ransomware attacks (NYT 2020)
- Financial security: Equifax breach (2017)
- Personal information: UC Accellion data breach
- Job security!
  - According to Forbes, computer security market size in 2020 is ~$173 billion, expected to reach $270 billion in 2026.



Firewall Times

Recent Data Breaches – 2024

By Michael X. Heiligenstein
February 20, 2024 — Breaches

Recent months have seen a string of data breaches affecting major companies, including Prudential, Verizon, and Bank of America. In this article, you'll find an overview of the latest data breaches, starting with the most recent.

February 2024: Prudential breached by ALPHV

On February 13, Prudential Financial reported to the Securities and Exchange Commission that they experienced a data breach on February 4. In this disclosure, Prudential reported that they did not believe that customer data was exposed in this incident.

The hacker group ALPHV took credit for this incident, as well as the loanDepot breach reported in January.

February 2024: Verizon breach affects over 63,000 employees

On February 7, Verizon Communications notified the Maine Attorney General that the company experienced a data breach back on September 21, resulting in the theft of sensitive information of over 63,000 employees. The breach included Social Security Numbers and other sensitive information on employees, but it does not appear any Verizon customers were implicated in this incident.

February 2024: Bank of America vendor breached

In early February, Bank of America notified customers of a data breach that occurred at Infosys McCamish, a software vendor for Bank of America. A ransomware group breached Infosys McCamish and stole sensitive personal information, including Social Security Numbers, from 57,028 Bank of America customers.

The breach itself occurred on November 3. Infosys McCamish informed Bank of America of the incident on November 24, and Bank of America disclosed the breach on February 2.

February 2024: Viamedis and Almerys hacks expose 33m French residents

In early February, hackers targeted two French healthcare insurance service providers, Viamedis and Almerys. As a result, 33 million French residents had their sensitive personal information stolen, though financial data is seemingly safe.

Viamedis said the hackers phished and used health professionals' logins to get into the system. Almerys said that the hackers entered through a portal used by health professionals. Both providers issued complaints with the public prosecutor and an investigation is underway.

January 2024: Microsoft breached by Russian hacker group

On January 12, Microsoft discovered a breach conducted by a Russian SVR foreign intelligence agency group. The incident occurred in November 2023 through a method called "password spraying," and targeted Microsoft's corporate email system.

Cozy Bear, the Russian-backed hacker group behind the SolarWinds breach, appears to have been behind this attack. Microsoft disclosed that these hackers compromised credentials on a "legacy" test account, likely with an outdated code, before accessing senior leadership accounts, among others. The hackers' access was removed on January 13.

Microsoft's disclosure comes a month after a new ruling that pushes publicly traded companies to disclose breaches that could negatively impact their business.

January 2024: 16.6m loanDepot customers' information

Basic Principles

- Security is economics
- Least privilege
- Defense in depth
- Complete mediation
- Accounting for human factors

Forbes

FORBES > INNOVATION > CYBERSECURITY

Criminals Hacked A Fish Tank To Steal Data From A Casino

Most important: **know your threat model**

Understand what is at risk and what you can do to minimize risk

Security Goals

1. **Confidentiality**
    a. Ensure only those with approved access can read data
2. **Integrity**
    a. Ensure data has not been tampered with
3. **Authentication**
    a. Prove the author/source of data
4. **Availability**
    a. Ensure the uptime of a service

1. Confidentiality

Ensure only those with approved access can read data

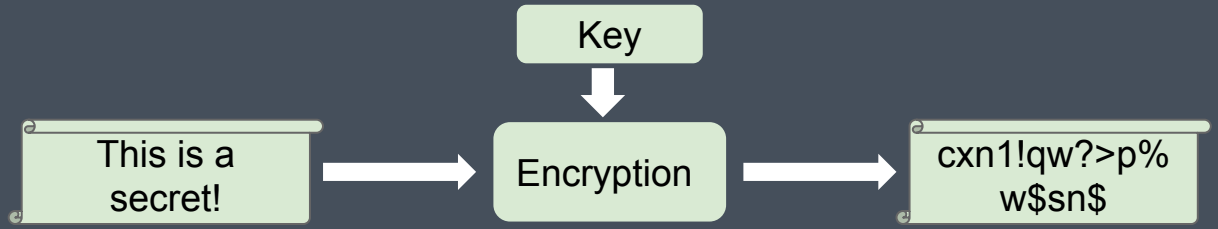
Plaintext:

- Vulnerable data
- What you want to hide from the attacker

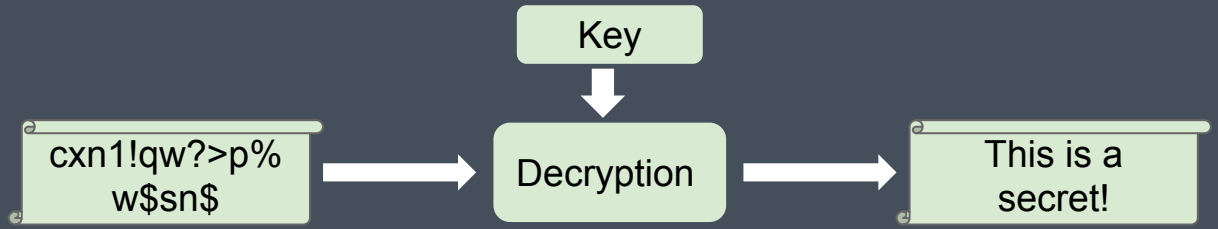
- Ciphertext:
  - Secured data that is indistinguishable from garble
  - What you want the attacker to see
- Key:
  - Secret necessary for converting plaintext into ciphertext and vice-versa

1. Confidentiality

- Encryption: plaintext + key → ciphertext



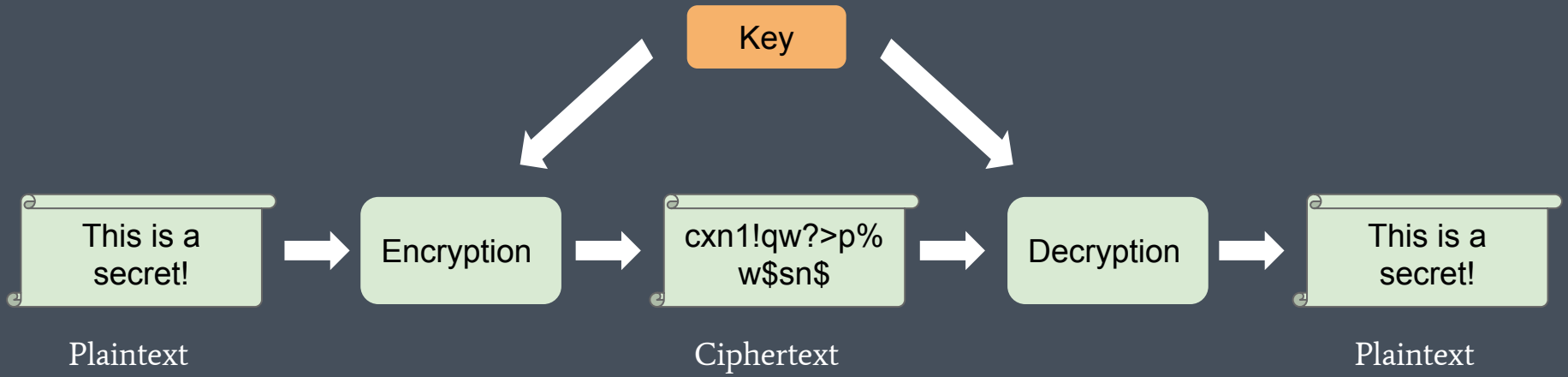
- Decryption: ciphertext + key → plaintext



1. Confidentiality

Symmetric cryptography:

Same key for encrypting and decrypting data



1. Confidentiality

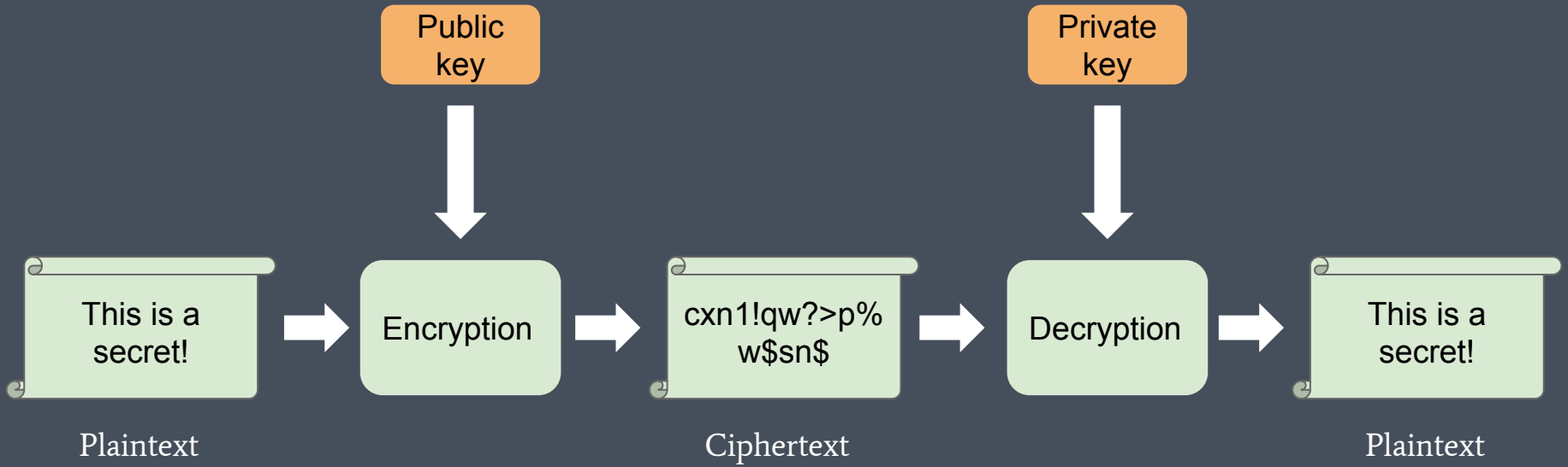
Asymmetric cryptography (AKA public key cryptography):

Comes in public-private key pairs where public key is for encryption and private key is for decryption

- Public key: can be distributed to everyone
- Private key: must be kept secret
- Anyone can encrypt data with public key but only the person possessing private key can decrypt data

1. Confidentiality

Asymmetric cryptography



2. Integrity

Ensure data has not been tampered with

- Hash function: maps arbitrary-length data to a fixed-length string of bits (known as a hash)
  - Hashes act as “summaries” of the input data

2. Integrity

Cryptographic hash functions possess properties that make it difficult to find two inputs with the same hash

- Hash-based MACs (Message Authentication Code):
  - Tag message with its hash
  - The recipient can verify whether the message was modified by re-computing the hash and comparing it with the one they received
- Checksums:
  - When a file is downloaded, its hash can be computed and checked against a reference hash. No need to compare bit by bit.

2. Integrity

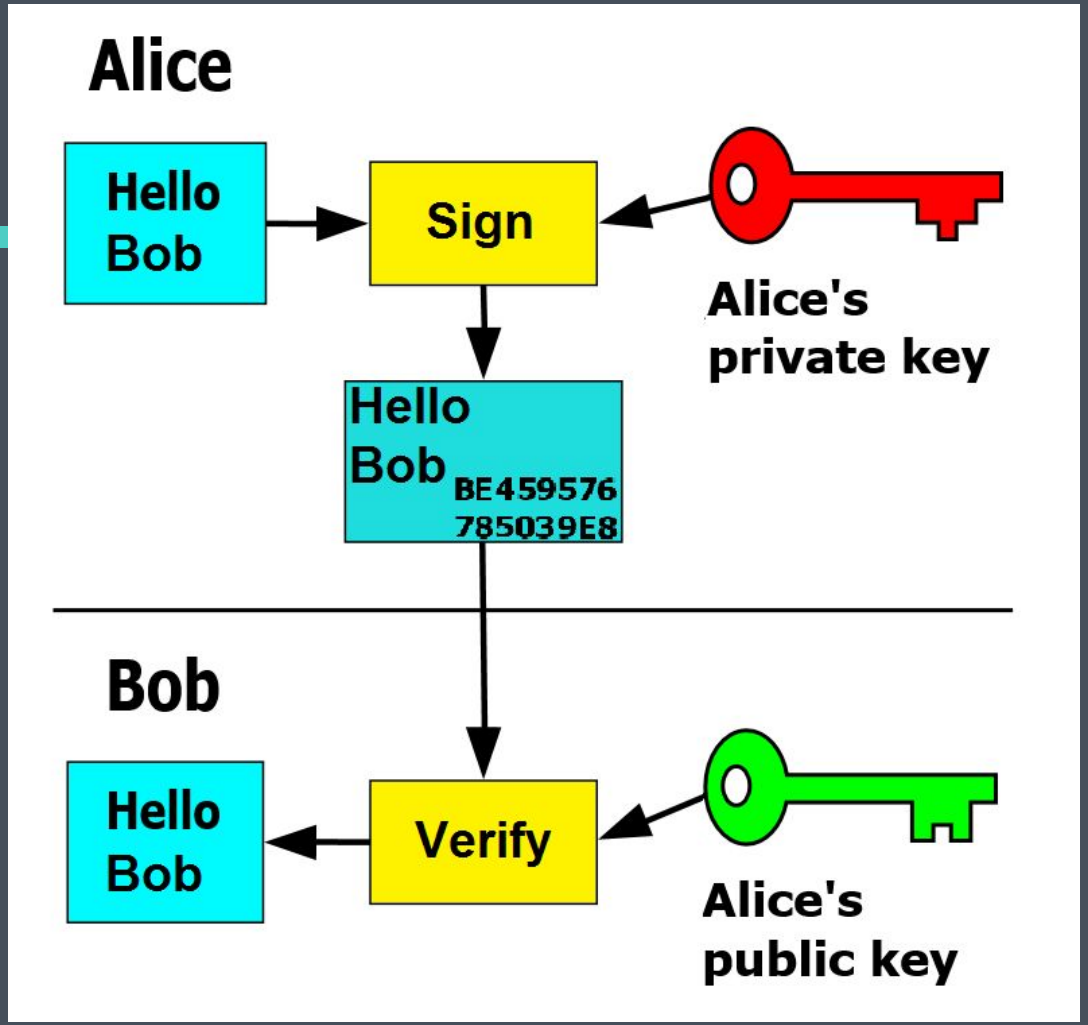
It is difficult to revert a hash to its input

- Password storage: store hashes of passwords instead of plaintext, so in case of server breach, only hashes would be exposed (passwords cannot be recovered from hashes)

3. Authentication

Prove the author/source of data

- Asymmetric cryptography (AKA public key cryptography)
- **Signature**: use private key to sign a file such that anyone with the public key can verify the source of the file
  - Since private key must be kept secret, only the party in possession of private key could have signed the data
  - file + private key → signature
  - signature + public key → verification


Alice
Hello Bob
Sign
Alice's private key
Hello Bob
BE459576
785039E8
Bob
Hello Bob
Verify
Alice's public key

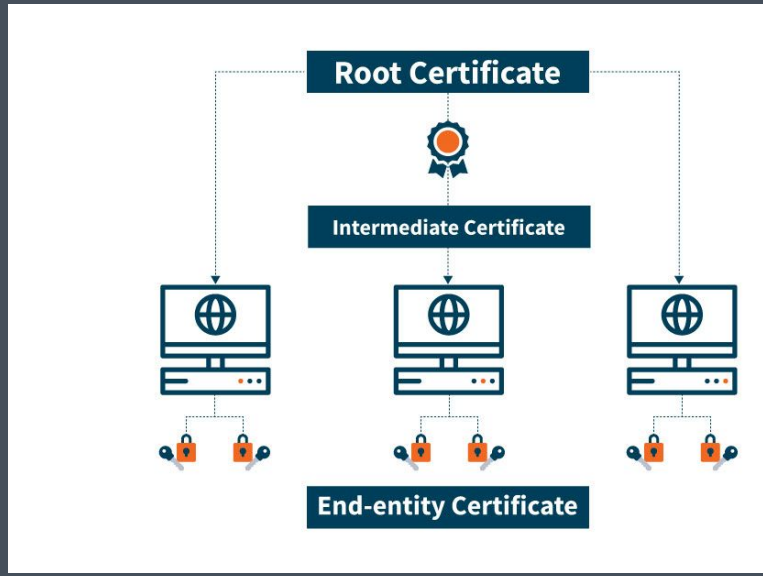
3. Authentication

- But how do we know we can trust the public key?!
  - Consider *man in the middle attack:* You need your bank's public key to encrypt a message. Instead, I give you a public key and claim it belongs to your bank.
- **Certificate**: cryptographically-signed message (from a trusted third party) indicating trust in a public key

- ....but why should I trust the certificate?!?

3. Authentication

- **Root certificates**: OS's include a number of root certificates that are the basis of trust over the network. Certificates are signed in a chain leading up to a root; if the chain is valid, the cert at the end is *presumed* to be trusted.
- Not a foolproof system…



KIM ZETTER SECURITY SEP 20, 2011 3:05 PM

DigiNotar Files for Bankruptcy in Wake of Devastating Hack

A Dutch certificate authority that suffered a major hack attack this summer has been unable to recover from the blow and filed for bankruptcy this week.

4. Availability

Ensure systems and data are available to authorized users when they need it. Mostly applicable to services hosted on servers.

- **Filtering**: prevent malicious requests from reaching server.
- **Load balancers**: improve distribution of workloads across multiple resources.
- **Redundancies**: account for when a component in the system fails.
- **Backups**: when system goes down, bring it back up to latest state

Questions?

1. Confidentiality
2. Integrity
3. Authentication
4. Availability

File Security

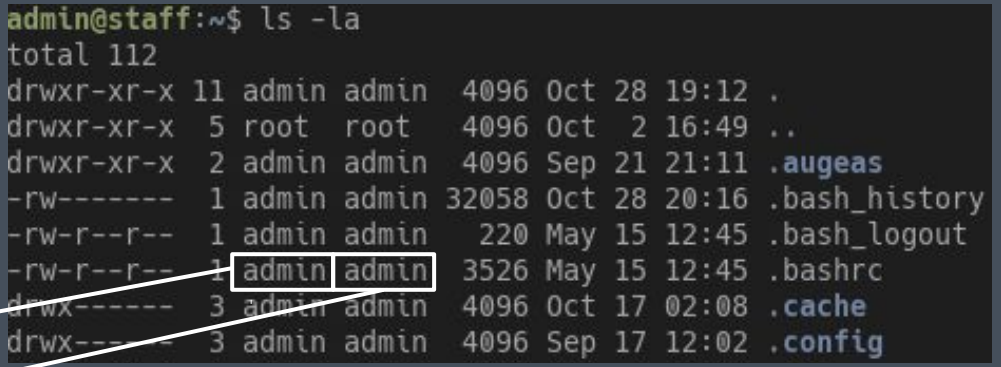
Permissions and Ownership

Background

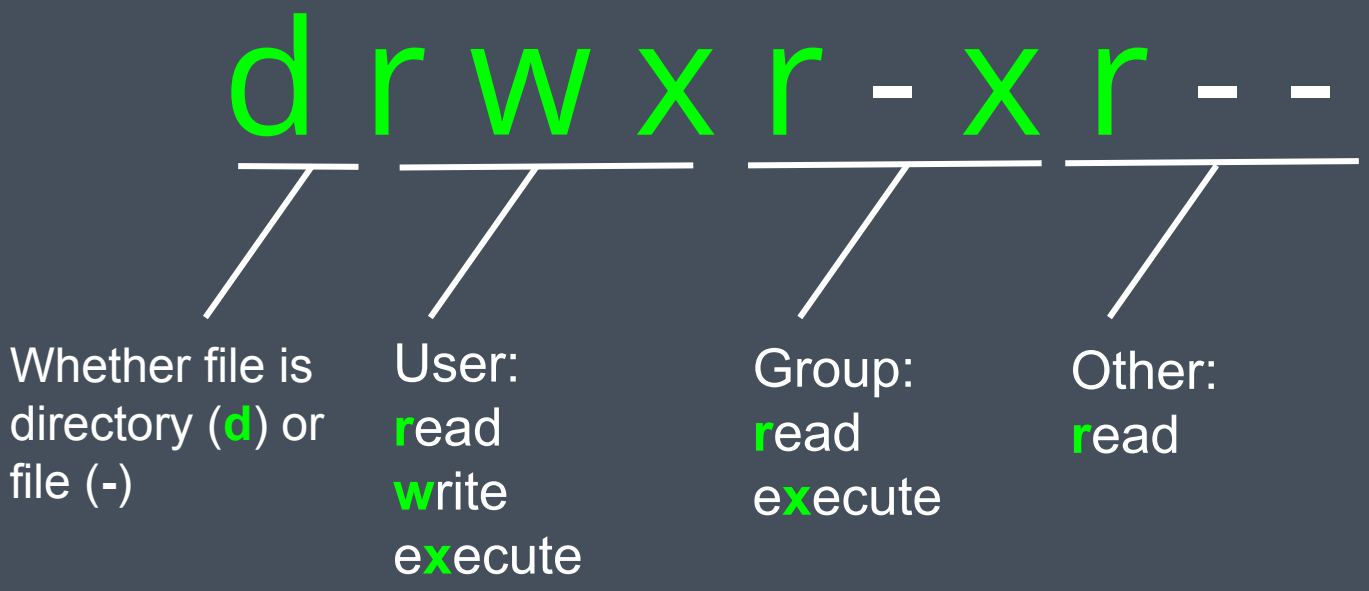
- UNIX is a multi-user environment
- If multiple people can login but you have files you want to keep private (e.g., your private keys), you need a permissions and ownership setup to let you and only you access those files

UNIX Permissions Model

- Each file has 3 “ownerships”:
  - owning user
  - owning group
  - others (everyone else)



Permissions



Modifying Permissions

2 primary ways to modify permissions/file access:

- Change file ownership: **chown**
- Change file permissions directly: **chmod**

Changing File Ownership

[sudo] chown [-R] newuser:newgroup

```
admin@staff:~/test/chown$ ls -la
total 12
drwxr-xr-x 2 admin admin 4096 Oct 31 16:49 .
drwxr-xr-x 4 admin admin 4096 Oct 31 16:49 ..
-rw-r----- 1 root  root    20 Oct 31 16:49 important_document.txt
admin@staff:~/test/chown$ cat important_document.txt
cat: important_document.txt: Permission denied
admin@staff:~/test/chown$ sudo chown admin:admin important_document.txt
admin@staff:~/test/chown$ cat important_document.txt
some important text
admin@staff:~/test/chown$ ls -la
total 12
drwxr-xr-x 2 admin admin 4096 Oct 31 16:49 .
drwxr-xr-x 4 admin admin 4096 Oct 31 16:49 ..
-rw-r----- 1 admin admin   20 Oct 31 16:49 important_document.txt
```

Changing File Permissions

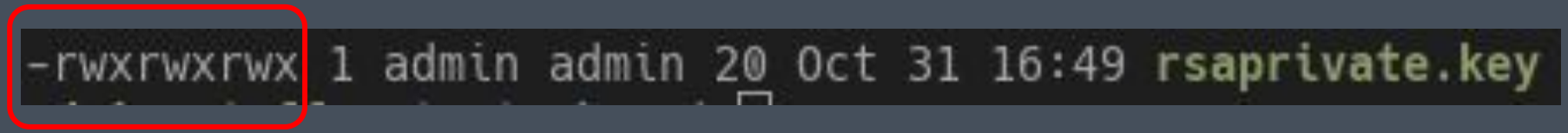
[sudo] chmod [-R] [permissions]

```
admin@staff:~/test/chown$ ls -la
total 12
drwxr-xr-x 2 admin admin 4096 Oct 31 16:49 .
drwxr-xr-x 4 admin admin 4096 Oct 31 16:49 ..
-rw-r----- 1 root  root    20 Oct 31 16:49 important_document.txt
admin@staff:~/test/chown$ cat important_document.txt
cat: important_document.txt: Permission denied
admin@staff:~/test/chown$ sudo chmod o+r important_document.txt
admin@staff:~/test/chown$ ls -la
total 12
drwxr-xr-x 2 admin admin 4096 Oct 31 16:49 .
drwxr-xr-x 4 admin admin 4096 Oct 31 16:49 ..
-rw-r--r-- 1 root  root    20 Oct 31 16:49 important_document.txt
admin@staff:~/test/chown$ cat important_document.txt
some important text
```

Why is this important?

Poor file security is one of the easiest ways to leak information or give an attacker too much privilege on your system.

What happens if you set these permissions on your private key?



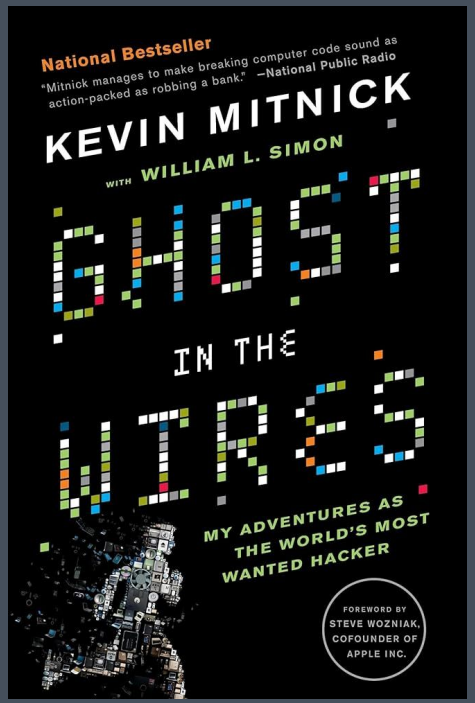
Questions?

- Unix Permission Model
- Changing file perms
  - chown
  - chmod

BeyondCorp and Zero Trust

- The traditional firewall + privileged intranet model doesn't really work nowadays: remote workers, PaaS, networked apps
- Google's done some work talking about a new approach with dynamic policies and more fine-grained access controls.
- Identifying access by user and device info and other heuristics
- Yes, this shit is buzzwordy as hell

Interested in security?



← Read this fun book!

(A bit outdated but helps you understand the origins of hacking culture :)

Take CS 161 →

Possibly worth your time

Join BERKE1337

https://discord.gg/AfDzRxRP