CS 177 - Computer Security

- Instructor: Christopher Kruegel

CS 177 Information

- Class home page (for slides)
  http://www.cs.ucsb.edu/~chris/teaching/cs177/index.html
- Piazza as the main channel for logistics and questions
  - class page: https://piazza.com/ucsb/spring2023/cs177/home
  - signup: https://piazza.com/ucsb/spring2023/cs177
- We also plan to create a Slack channel for the class
  - invites will go out soon to all students on Piazza
- Class email: cs177@cs.ucsb.edu

Requirements

- The course requirements include
  - several projects
  - a midterm and a final exam
- The projects (and exams) are individual efforts
- The final grade will be determined according to the following weight
  - projects: 50%
  - exams: 50%

Lab Projects

- You will interact with remote services and have to solve challenges to obtain flags
- You can then submit these flags to prove to us that you solved a challenge

- Some Past Challenges
  1. Get started with a simple network client
  2. Craft ICMP packets to exploit a ping-of-death-style vulnerability
  3. Exploit basic web application vulnerabilities
  4. Exploit memory corruption vulnerabilities
  5. Find and exploit a smart contract (Web3) vulnerability
  6. Decrypt a variety of cipher texts and password hashes
  7. Check TLS certificates and launch golden ticket attack against Kerberos-style service
  8. Launch a cryptanalysis attack

Why Does Security Matter?

The Top 50

BIGGEST DATA BREACHES

from 2004 - 2021

A data breach is an incident where protected information is copied, stolen, or exposed to an unauthorized person. The largest breach in recent times was the LinkedIn breach of 2021 in which 700 million records were lost. The visual on the right highlights the Top 50 known data breaches from 2004 to 2021.

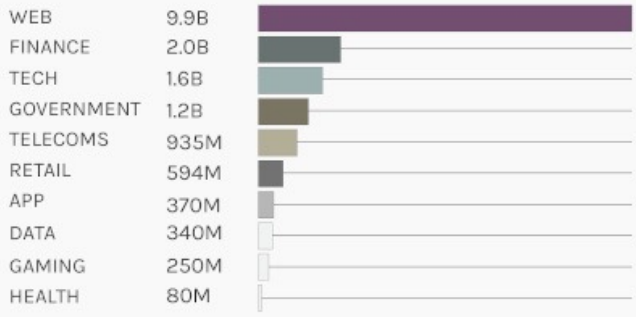
The Web sector was impacted the most. 9.9B records were lost. The Tech and Finance sectors were also severly impacted, and they lost 1.6B and 2.0B records, respectively.

SECTORS - These are industry sectors which the companies belong to. There are 10 in total.

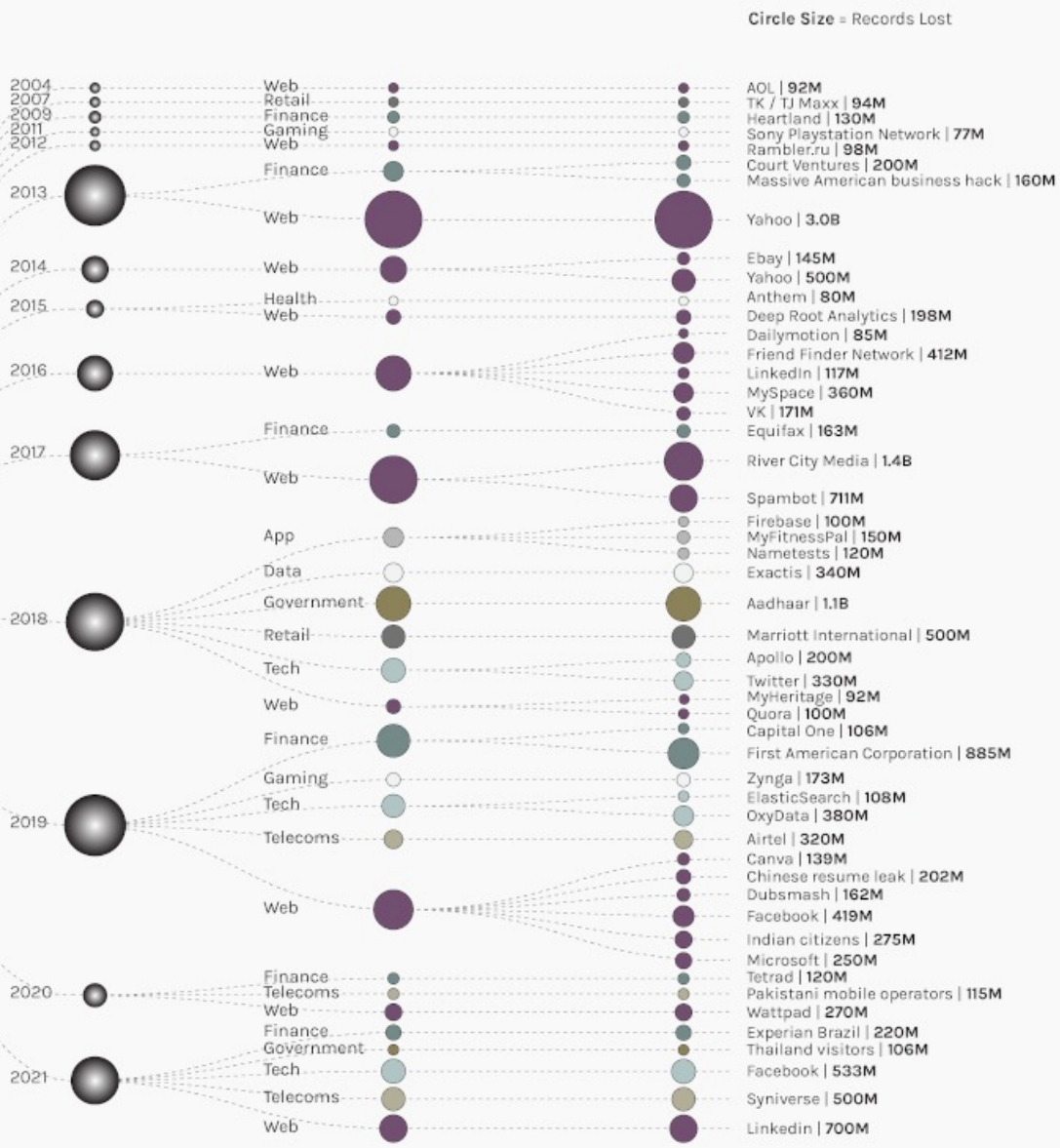
17.2B

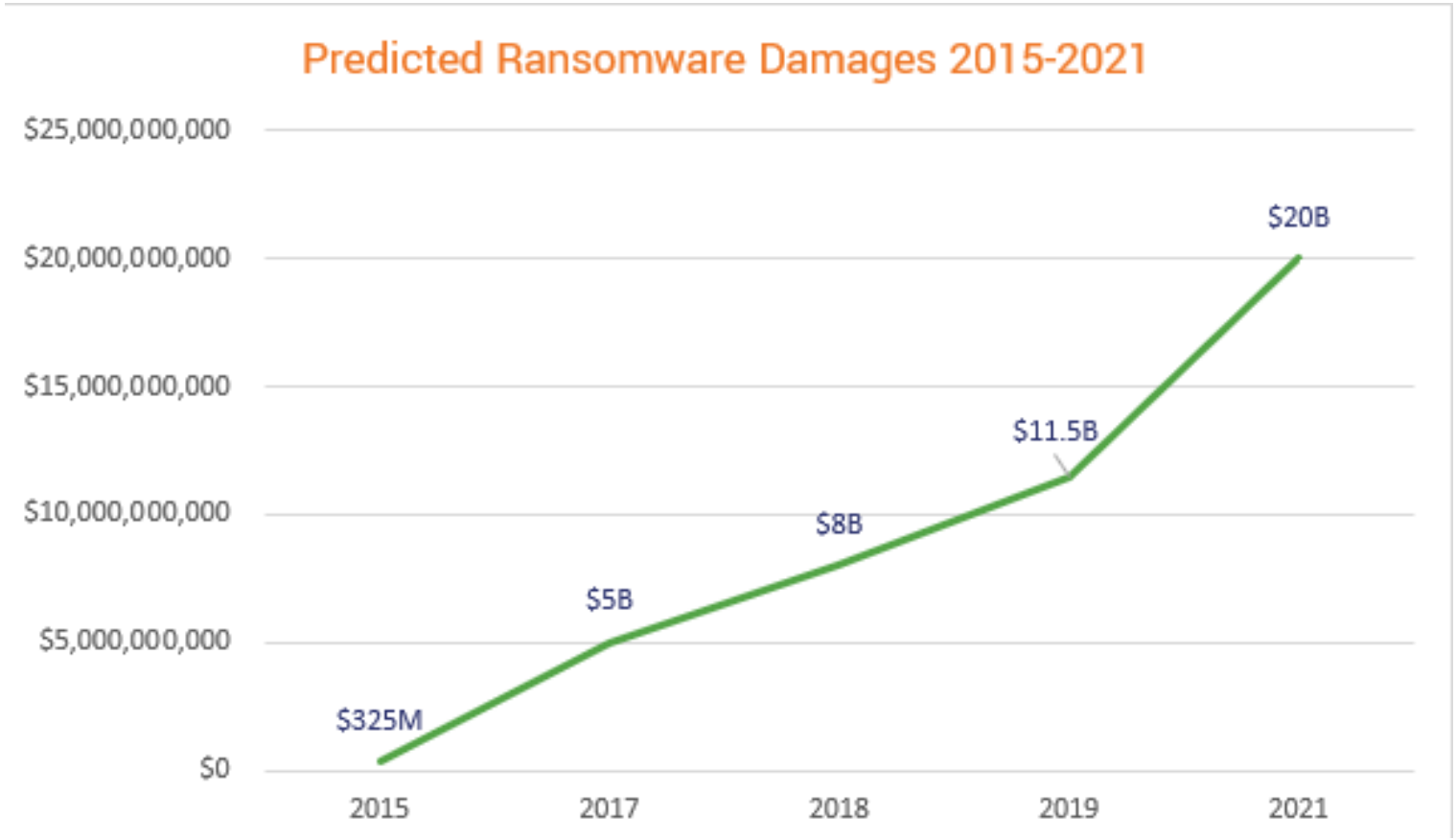
Total number of records lost

The number of records lost per sector is shown below:



Sources: News reports

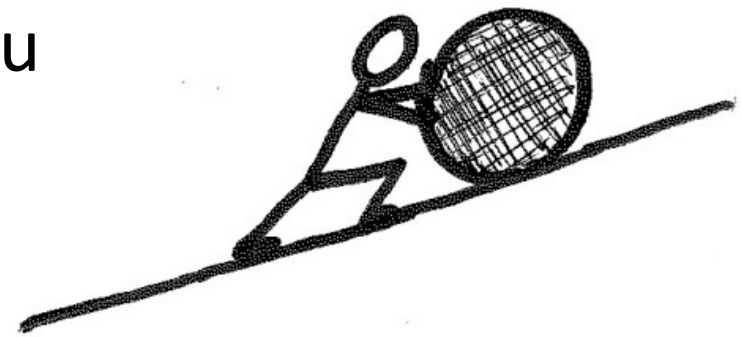



Predicted Ransomware Damages 2015-2021
$25,000,000,000
$20,000,000,000
$15,000,000,000
$10,000,000,000
$5,000,000,000
$0
$325M
$5B
$8B
$11.5B
$20B
2015
2017
2018
2019
2021

The night is dark and full of terror

Many worst-case prophecies by computer-security researchers have become true.

It's a uphill battle, and you have to play your part.



Goal of this Class

We will focus on

- **Principles** of computer security
- With many **applications** to the real-world

Technology changes very fast, basic security issues remain the same.

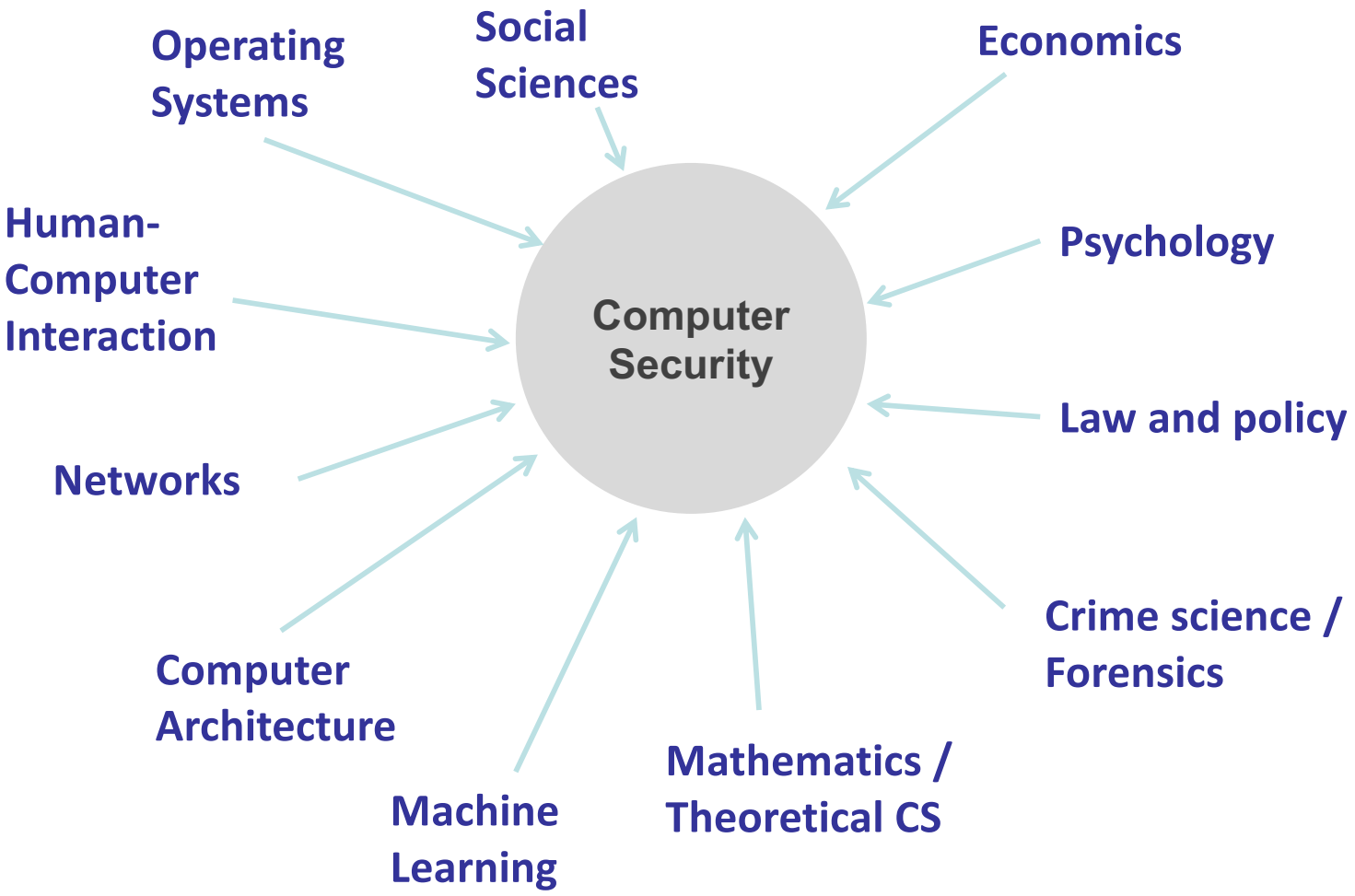
Many security issues today due to lack of proper training and education at all levels

Acquired Skills

- Adversarial Thinking = What would happen if I perform this one action the system designers have not thought of?
- Requires creativity, out-of-the-box thinking, extremely detailed understanding of both general principles as well as specific technologies

After taking this class: You might not know all answers, but you should know the questions!

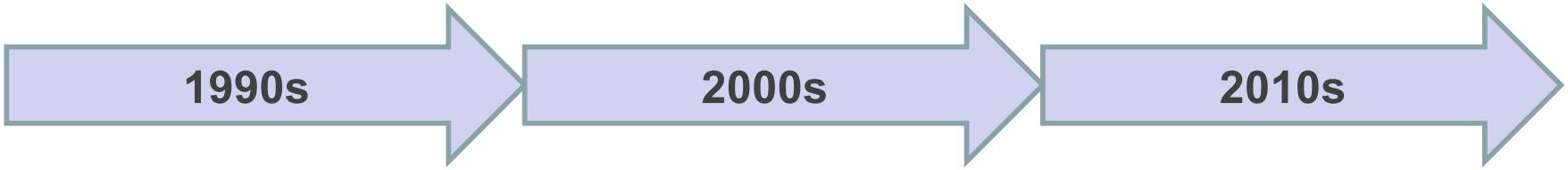
Computer Security



Topics

- Security Principles
- Network Security
- Application Security
- Web Security
- Malware
- Applied Cryptography
- Secure Authentication and Passwords
- Privacy
- Web3 / Smart Contract Security

The Evolution of Cybersecurity



- The term *hacker* used to have a positive connotation
- Today, hacking is considered a tool for achieving economic, social, or political objectives
- Hacking for profit (Cybercrime)
  - High volume, low sophistication
- Hacking for intel/espionage
  - APT - (State-sponsored) Advanced Persistent Threat actors
  - High sophistication, highly targeted

Insecure Software

Or, why do good people write bad code?

- Technical factors
  - complexity and composition
- Economic factors
  - deadlines
  - insufficient funding
- Human factors
  - risk assessment
  - mental models

Basic Security Definitions

- Policies and mechanisms for enforcing protection properties over data and resources

- We reason in terms of properties that we want to hold
  - Security policies precisely specify those properties
- Mechanisms enforce these properties
- Always with respect to a threat model
- Attackers exploit vulnerabilities to violate properties

Security Properties

Security Properties

- These properties form an essential framework for thinking about security
  - Confidentiality, integrity, availability ("CIA triad")
  - Authenticity, non-repudiation
- Many security problems can be cast in terms of one or more of these properties
- Let's consider a hypothetical scenario where a general gives the order "*Attack at dawn*"

Confidentiality

"Hey, we're going to attack at dawn"

- Data must only be released to *authorized principals*
- Temporal aspect, relation to difficulty or work factor

Integrity

"Sir, we received an order to retreat at dawn"

- Data must not be modified (in an undetectable manner)
- But what constitutes a modification?
  - Malicious tampering
  - Accidental modification
  - Dropped, replayed, or reordered messages

Availability

"We couldn't make contact with command"

- Data and resources must be accessible when required
- Related to integrity, but more concerned with denial-of-service (DoS) attacks
- Relies on some asymmetric advantage for success

Authenticity

"Someone told us to attack, but we don't know who"

- Data must be bound to identity
- Authentication enables the ability to make trust decisions
- Cryptographic origins (e.g., certificate authorities, other trusted third parties)

Non-Repudiation

"The general claims he never issued that order, sir"

- Non-repudiation prevents denial of authorship of a message
- Not always a desirable property!

Further Goal - Privacy

- The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others.

- Often confused with confidentiality, but these are two different concepts

Security Mechanisms

Security Model

- Security models are mechanisms for specifying and enforcing security policies (i.e., guaranteeing security properties)

- Access control is the central principle
  - allows one to specify *who* can interact with *what*
  - requires authentication as a building block

- Principals — Participants (users) in a system
- Subjects (**who**) — Entities that operate on behalf of principals
- Objects (**what**) — Resources acted upon by subjects

Authentication

- Verification of a claim of identity made by a subject on behalf of a principal

- Involves examination of factors or credentials
  - Something you *have*
  - Something you *know*
  - Something you *are*

- Desirable properties
  - unforgeable, unguessable, revocable

Authorization

- Access control decision

  → statement in terms of different properties (e.g., spatial, temporal, history, trust relationships) of subjects and objects

- Given that a principal is authenticated, one can define what actions they are authorized to perform

Types of Access Control

- Discretionary access control (DAC)
  - subjects can change access control permissions
  - typically used in modern operating systems
- Mandatory access control (MAC)
  - system defines mandatory access control permissions
- Role-based access control (RBAC)
  - principals are assigned to roles, and decisions are based on role membership

Security Models

- Abstract models
  - Access Control Matrix, Access Control Lists (ACLs), Capabilities, Bell-LaPadula, Biba Integrity, Clark-Wilson, Brewer-Nash, …
- Concrete models
  - UNIX, Windows, Java, Web, Android, iOS

Security Models

- Access Control Matrix
  - First formal access control model (Lampson, 71)
  - Static description of entire system protection state

$$\mathbf{S_{m,n}} = \begin{pmatrix} \text{RW} & \text{RX} & \emptyset & \cdots \\ \emptyset & \text{RWX} & \text{R} & \\ \text{RWX} & \text{RWX} & \text{RWX} & \\ \vdots & & & \ddots \end{pmatrix}$$

Security Models

- Access Control List
  - Access control matrices in another form
  - Authorization checked against list of tuples

$$\langle \text{subject}, \text{object}, \text{operation} \rangle$$

  - Used pervasively in filesystems and networks

Security Models

- Capabilities
  - Authorization ⟺ Possession of a capability
  - Capability is an unforgeable and transferable token
- Systems
  - EROS (1999), Capsicum (2010 for FreeBSD, Linux)
- Web
  - bearer tokens, random URLs, cookies, …

Threat Models and Vulnerabilities

Threat Model

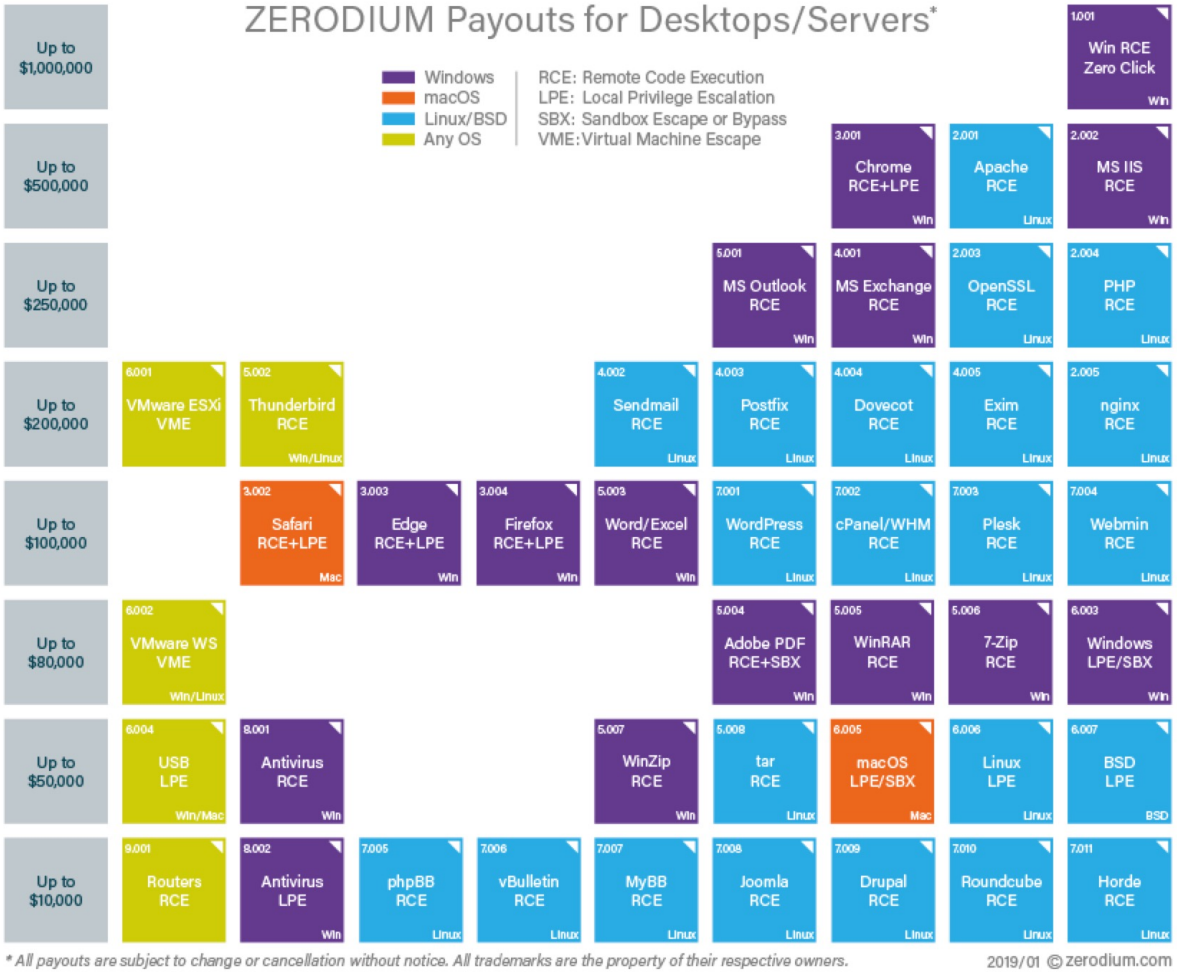
- Threat models describe what an attacker can do
- They also bound the capabilities of an attacker
  - Common in cryptography
    - Dolev-Yao, IND-CPA, IND-CCA, …
  - Equally important for systems, networks, and software
    - passive network attacker, active network attacker, on-or off-path network attacker, privileged local user, web attacker, benign-but-buggy, insider threats, ...
- Sometimes implicit, but must always be taken into consideration

Security Vulnerabilities

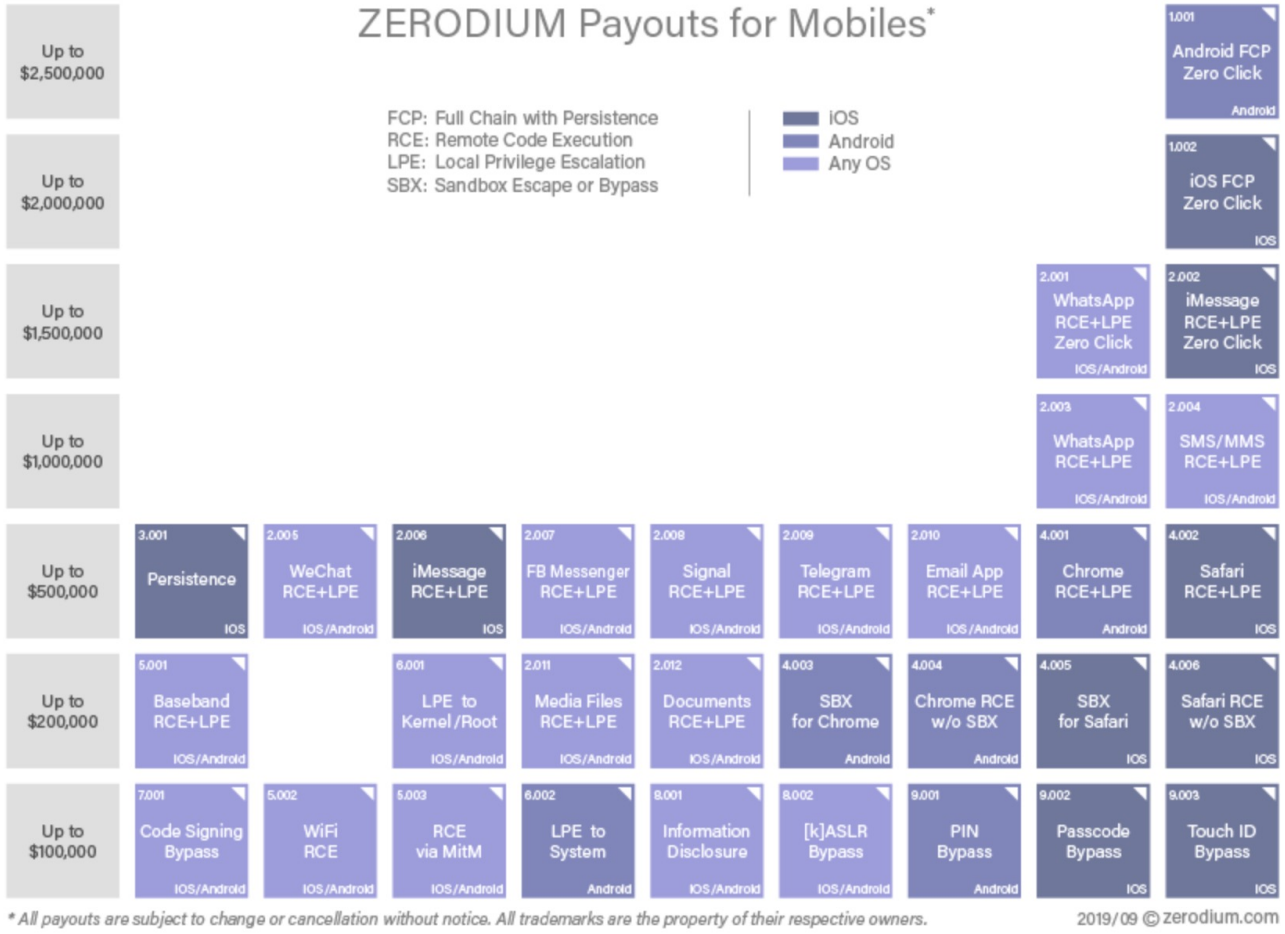
Vulnerability: A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate a security policy.

- Zero-day vulnerability
  - Vulnerability unknown to the vendor
- Patch / security fix
  - software change that removes vulnerability
- Window of vulnerability
  - time between the introduction and removal of a vulnerability
- Exploit
  - Piece of software leveraging a vulnerability

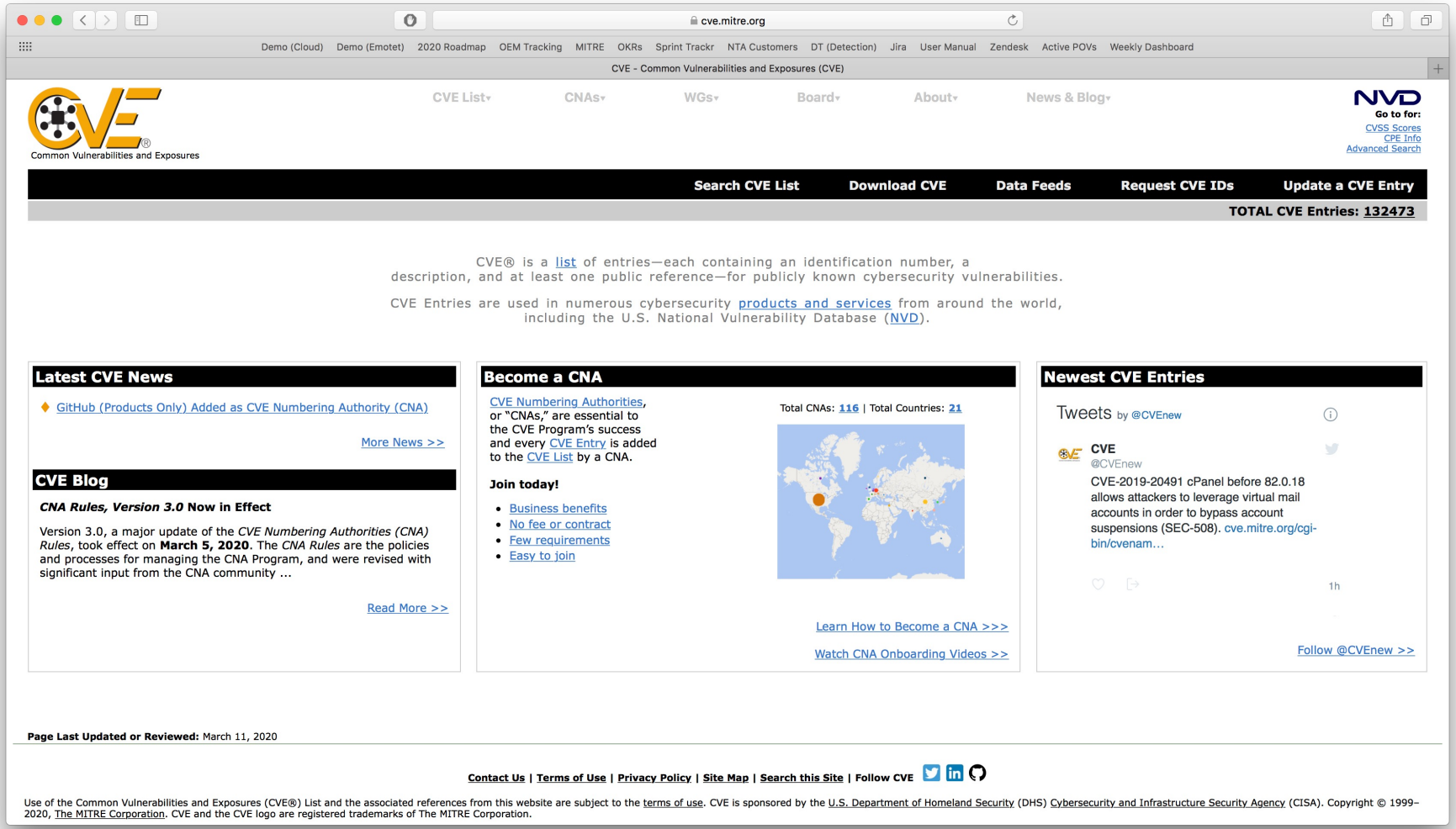
Vulnerability Markets



Vulnerability Markets



Vulnerability Databases



Security Approaches and Principles

General Security Approaches

- Avoidance
  - Prevent introduction of vulnerabilities in design/development
  - Integration of security models into design
    - Secure development practices
    - Preemptive identification and removal of vulnerabilities
- Detection
  - monitor deployed systems to identify attacks at run-time
    - Intrusion detection systems (IDS)
    - Anti-virus (AV)
    - Malware analysis sandboxes
    - Signature vs. anomaly-based approaches

General Security Approaches

- Prevention
  - Interdict attacks at run-time
  - Related to avoidance, but operates at run-time
  - Usually focused on mitigating specific classes of attacks
    - Buffer overflows, code injection, XSS, …
- Recovery
  - Continuity of service during and after exploitation
  - Concedes that attacks will occur
  - Focuses on integrity guarantees

Security Principles

- We have seen some basic properties, policies, mechanisms, models, and approaches to security
- But designing secure systems, as well as breaking them, remains as much art as science
- Security principles serve as guidelines to help bridge the gap between art and science
- Initial set introduced by Saltzer and Schroeder (1975)

Economy of Mechanism

Simplicity of design implies a smaller attack surface

- Design should be as simple as possible
  - KISS -- keep it simple, stupid
  - Brian W. Kernighan: “Debugging is twice as hard as writing the code in the first place. Therefore, if you write the code as cleverly as possible, you are, by definition, not smart enough to debug it.”
  - Correctness of protection mechanisms is critical
  - We need to be able to reason about security mechanisms in order to trust them

Defense in Depth

Do not depend on a single protection mechanism, since they are apt to fail

- Even very simple or formally verified defenses fail
- Layering defenses increases the difficulty for attackers
- When does layering make sense? When does it not?

Fail-safe Defaults

Absence of explicit permission means no permission

- Systems should be secure out of the box
  - deny as default action
  - grant access only on explicit permission
  - users should have to opt-in to less-secure configurations
  - in case of mistake, access denied (noticed quickly)

Complete Mediation

Every access to every object must be authorized

- Complete access control
  - check every access to every object
  - include all aspects (normal operation, initialization, maintenance, ..)
  - caching of checks is dangerous
  - identification of source of action (authentication) is crucial
- Incomplete mediation implies a path exists to bypass a security mechanism

Open Design

The design must not be secret

- Kerckhoff's Principle: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge
- Generalization: A system should be secure even if the adversary knows everything about its design (but not necessarily all run-time parameters)

- Contrast with "security through obscurity"

Separation of Privilege

Privilege should be distributed so as to avoid central points of failure

- Spreading privileges among multiple principals avoids single-point compromises
- Requiring multiple parties to mutually agree on a course of action lessens likelihood of security failures
  - for example, two keys are required to access a resource
    - launch of nuclear weapons requires two people
    - bank safe

Least Privilege

Subjects should possess only that authority that is required to operate successfully

- Subjects should have the least privilege necessary to perform a task
- If a compromise occurs, the potential damage is (hopefully) limited
- Can minimize privilege as well as time privileges are held

Separation

Separate data and control

- Failed separation is reason for many security vulnerabilities
  - distinction between control information and data has to be clear
  - examples buffer overflows, macro viruses, JavaScript, …

Psychological Acceptability

Make things easy and intuitive for users

- Easy-to-use human interface
  - easy to apply security mechanisms routinely
  - easy to apply security mechanisms correctly
  - interface has to support mental model

Work Factor

Allow defenders to scale difficulty of mounting attacks

- Attacks only get better
- Introducing a work factor allows defenses to scale to future threats without wholesale replacement
  - Often entails the introduction of hidden non-determinism
    aka, make keys longer
  - Related to ideas of adaptive defense and artificial diversity