CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous Class

- Assets
- Security Threats
- Security Services
- Security Tools/ Mechanisms

- Term Project
  - Group of 2 max 3 students (for significant contribution)
  - Both Implementation and Analysis

This Class

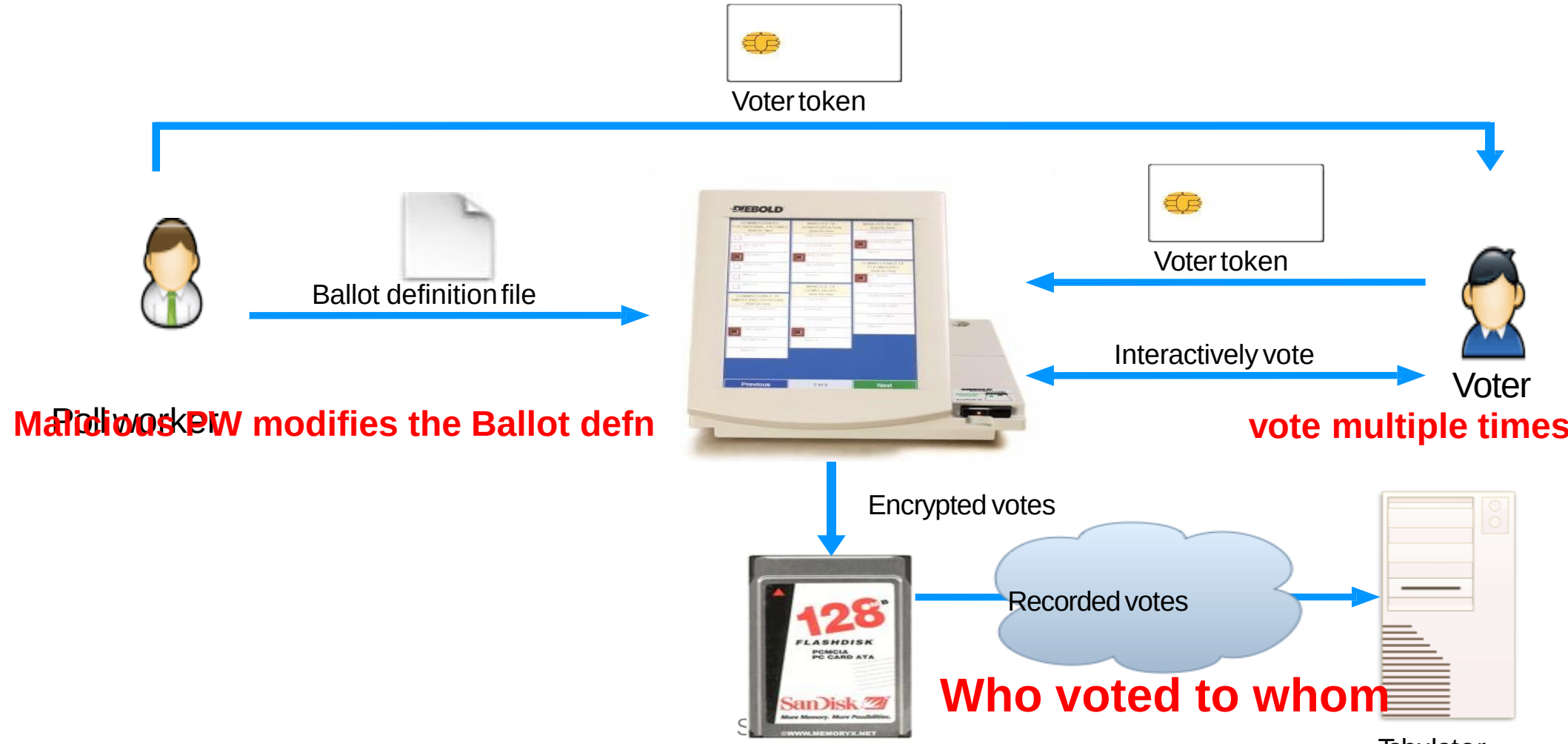
- Program security
  - Flaws, faults, and failure
  - Types of security flaws
  - Unintentional security flaws
    - Buffer overflows

Computer and Network Assets & Security goals

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Use case: Electronic Voting

What an Adversary could do?



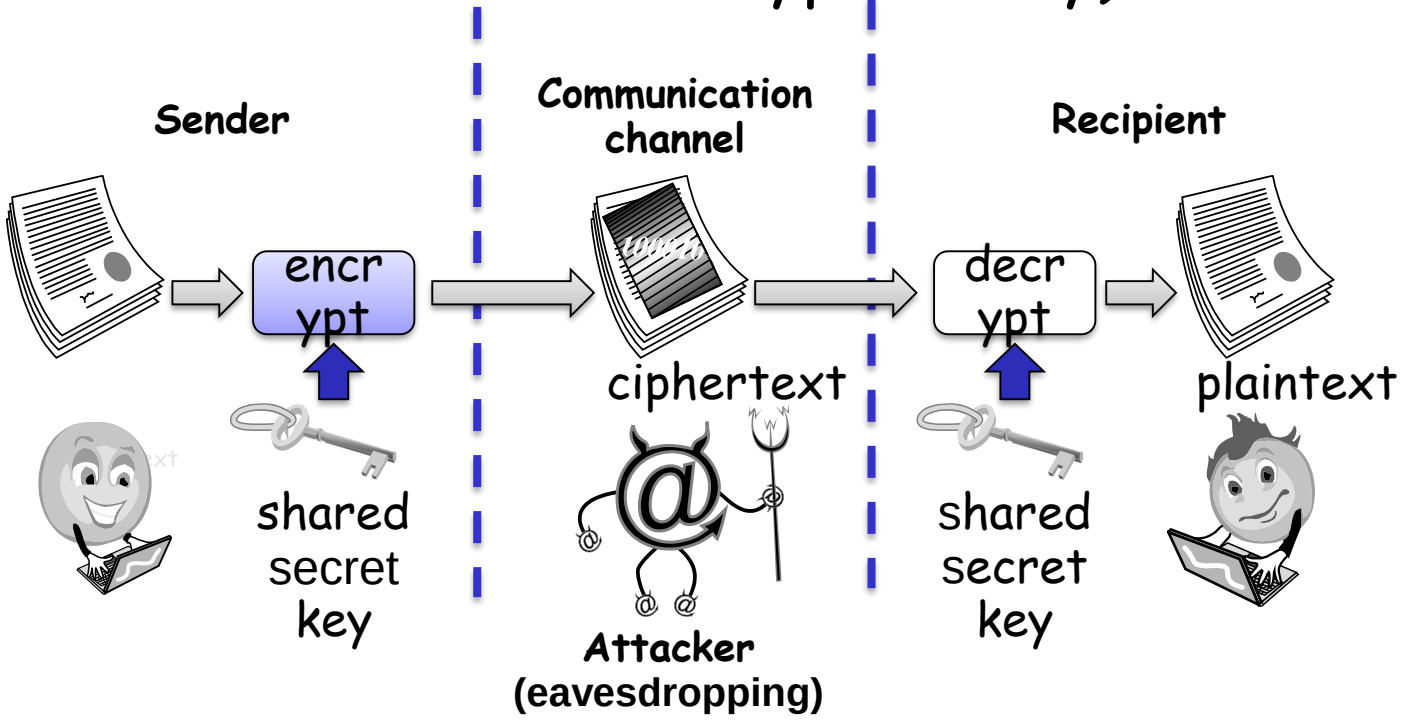
Security Goals

Basic Security Services
Key Security Concepts (FIPS PUB 199)

- preserving authorized restrictions on information access and disclosure.
- guarding against improper information modification or destruction,
- ensuring timely and reliable access to and use of information

Tools for Confidentiality

- **Confidentiality** is the avoidance of the unauthorized disclosure of information.
- **Encryption:** the transformation of information using a secret, called an encryption key, so that the transformed information can only be read using another secret, called the decryption key (which may, in some cases, be the same as the encryption key).

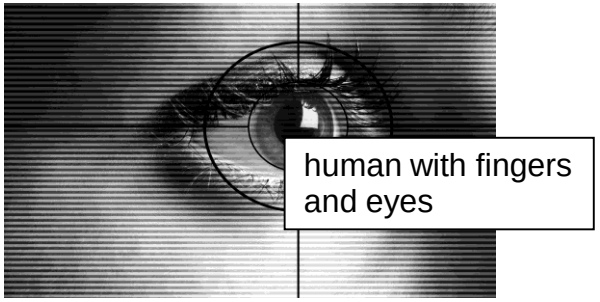


Tools for Confidentiality

- **Access control:** rules and policies that limit access to confidential information to those people and/or systems with a "need to know."
  - This need to know may be determined by identity, such as a person's name or a computer's serial number, or by a role that a person has, such as being a manager or a computer security specialist.

Tools for Confidentiality

- **Authentication:** the determination of the identity or role that someone has. This determination can be done in a number of different ways, but it is usually based on a combination of
  - something the person has (like a smart card or a radio key fob storing secret keys),
  - something the person knows (like a password),
  - something the person is (like a human with a fingerprint).



Something you are

Something you know

Something you have

Tools for Confidentiality

- **Authorization:** the determination if a person or system is allowed access to resources, based on an access control policy.
  - Such authorizations should prevent an attacker from tricking the system into letting him have access to protected resources.
- **Physical security:** the establishment of physical barriers to limit access to protected computational resources.
  - Such barriers include locks on cabinets and doors, the placement of computers in windowless rooms, the use of sound dampening materials, and even the construction of buildings or rooms with walls incorporating copper meshes (called **Faraday cages)** so that electromagnetic signals cannot enter or exit the enclosure.

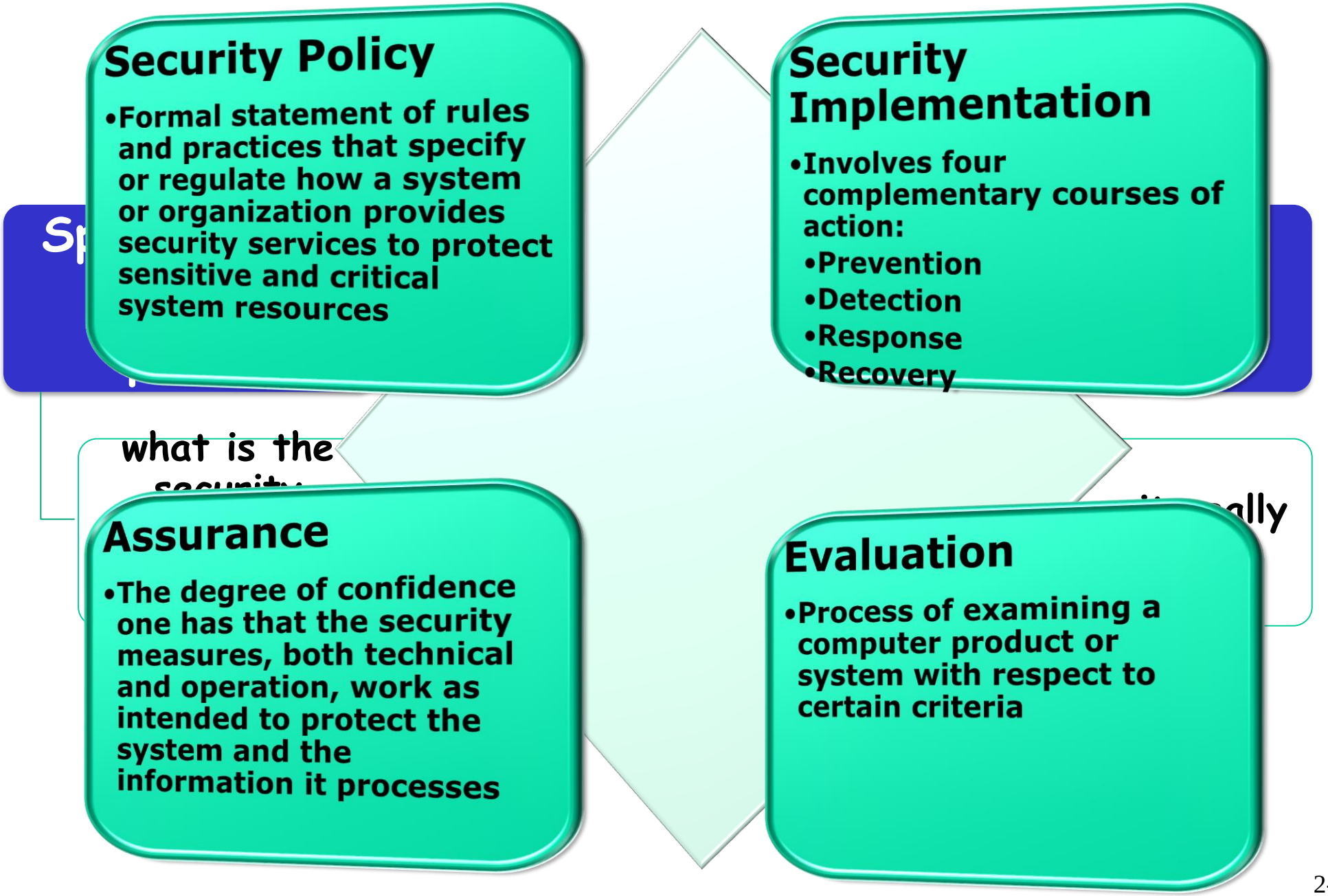
Integrity

- **Integrity:** the property that information has not be altered in an unauthorized way.
- **Tools:**
  - **Backups:** the periodic archiving of data.
  - **Checksums:** the computation of a function that maps the contents of a file to a numerical value. A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value.
  - **Data correcting codes:** methods for storing data in such a way that small changes can be easily detected and automatically corrected.

Availability

- **Availability:** the property that information is accessible and modifiable in a timely fashion by those authorized to do so.
- **Tools:**
  - **Physical protections:** infrastructure meant to keep information available even in the event of physical challenges.
  - **Computational redundancies:** computers and storage devices that serve as fallbacks in the case of failures.

Computer Security Strategy



Policy to Implementation

- After figured out the security requirements for application, i.e, framed policy, there are challenges:
- Requirements bugs
  - Incorrect or problematic goals
- Design bugs
  - Poor use of cryptography
  - Poor sources of randomness
- Implementation bugs
  - Buffer overflow attacks
- **Is the system usable?**

Whole system is critical

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

  - "security is only as strong as the weakest link," and security can fail in many places
  - Attacker only needs to win in one place

Defense Mechanism

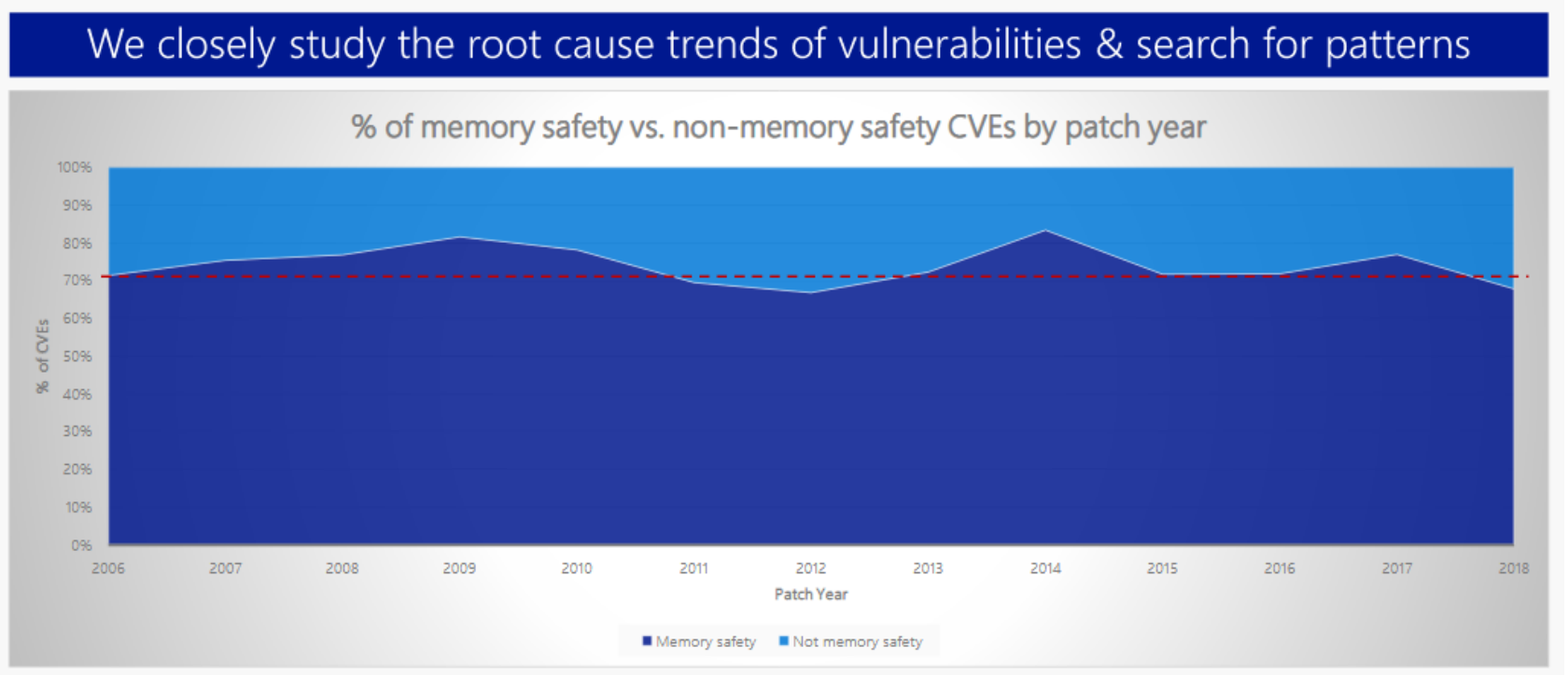
- There are a lot of defense mechanisms
  - We'll study some, but not all
  - It's important to understand their limitations

- "If you think cryptography will solve your problem, then you don't understand cryptography… and you don't understand your problem" -- Bruce Schneier

Program Security

Program security is the first step to apply security in computing

70% of Microsoft's vulnerabilities are memory safety issues



- ~70% of Microsoft vulnerabilities 2006-2018 memory safety issues
  - Memory safety = "Accesses system memory in a way that exceeds its allocated size & memory addresses" (for example, a buffer overflow)
- Not as common a problem for many other organizations
  - Problem only occurs if programming language is not memory-safe

Source: "Microsoft: 70 percent of all security bugs are memory safety issues" by Catalin Cimpanu, 2019-02-11, https://www.zdnet.com/article/microsoft-70-percent-of-all-security-bugs-are-memory-safety-issues/

Program Security Issues

- Issues:
  - How to keep program free from flaws?
  - How to protect computing resources from pgms with flaws?

- Issues of trust *not* considered:
  - How trustworthy is that program you buy?
  - How to use it in its most secure way?
    - Partial answers:
      - Third-party evaluations
      - Liability and s/w warranties

Secure programs

- Why is it so hard to write secure programs?
  - Programs have bugs
  - Security-relevant programs have security bugs

  - **Symantec security flaws are "as bad as they get,"**
  - Ref. http://www.zdnet.com/article/symantec-antivirus-product-bugs-as-bad-as-they-get/

Program Security Issues

- Many vulnerabilities result from poor programming practices
  - consequence from insufficient checking and validation of data and error codes
  - awareness of these issues is a critical step in writing more secure program code
- Program error categories:
  - insecure interaction between components
  - risky resource management
  - porous defenses

2020 CWE/SANS Top 25 Most Dangerous Software Weakness

Rank	ID	Name	Score
[1]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	
[2]	CWE-787	Out-of-bounds Write	46.17
[3]	CWE-20	Improper Input Validation	33.47
[4]	CWE-125	Out-of-bounds Read	26.50
[5]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	
[7]	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	19.16
[8]	CWE-416	Use After Free	18.87
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	17.29
[10]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16.44
[11]	CWE-190	Integer Overflow or Wraparound	15.81
[12]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	
[13]	CWE-476	NULL Pointer Dereference	8.35
[14]	CWE-287	Improper Authentication	8.17
[15]	CWE-434	Unrestricted Upload of File with Dangerous Type	7.38
[16]	CWE-732	Incorrect Permission Assignment for Critical Resource	6.95
[17]	CWE-94	Improper Control of Generation of Code ('Code Injection')	6.53
[18]	CWE-522	Insufficiently Protected Credentials	5.49
[19]	CWE-611	Improper Restriction of XML External Entity Reference	5.33
[20]	CWE-798	Use of Hard-coded Credentials	5.19
[21]	CWE-502	Deserialization of Untrusted Data	4.93
[22]	CWE-269	Improper Privilege Management	4.87
[23]	CWE-400	Uncontrolled Resource Consumption	4.14
[24]	CWE-306	Missing Authentication for Critical Function	3.85
[25]	CWE-862	Missing Authorization	3.77

2021 CWE Top 10

Rank	ID	Name
[1]	CWE-787	Out-of-bounds Write
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[3]	CWE-125	Out-of-bounds Read
[4]	CWE-20	Improper Input Validation
[5]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[7]	CWE-416	Use After Free
[8]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[9]	CWE-352	Cross-Site Request Forgery (CSRF)
[10]	CWE-434	Unrestricted Upload of File with Dangerous Type

Thanks