Introduction to IT and OT Security

Azqa Nadeem
PhD candidate and lecturer
Cybersecurity group
Delft University of Technology

TU Delft

Today…

Part I

- Security basics: CIA and cryptography
- Identity/access management

Part II

- Threat detection
- Vulnerability management

Part III

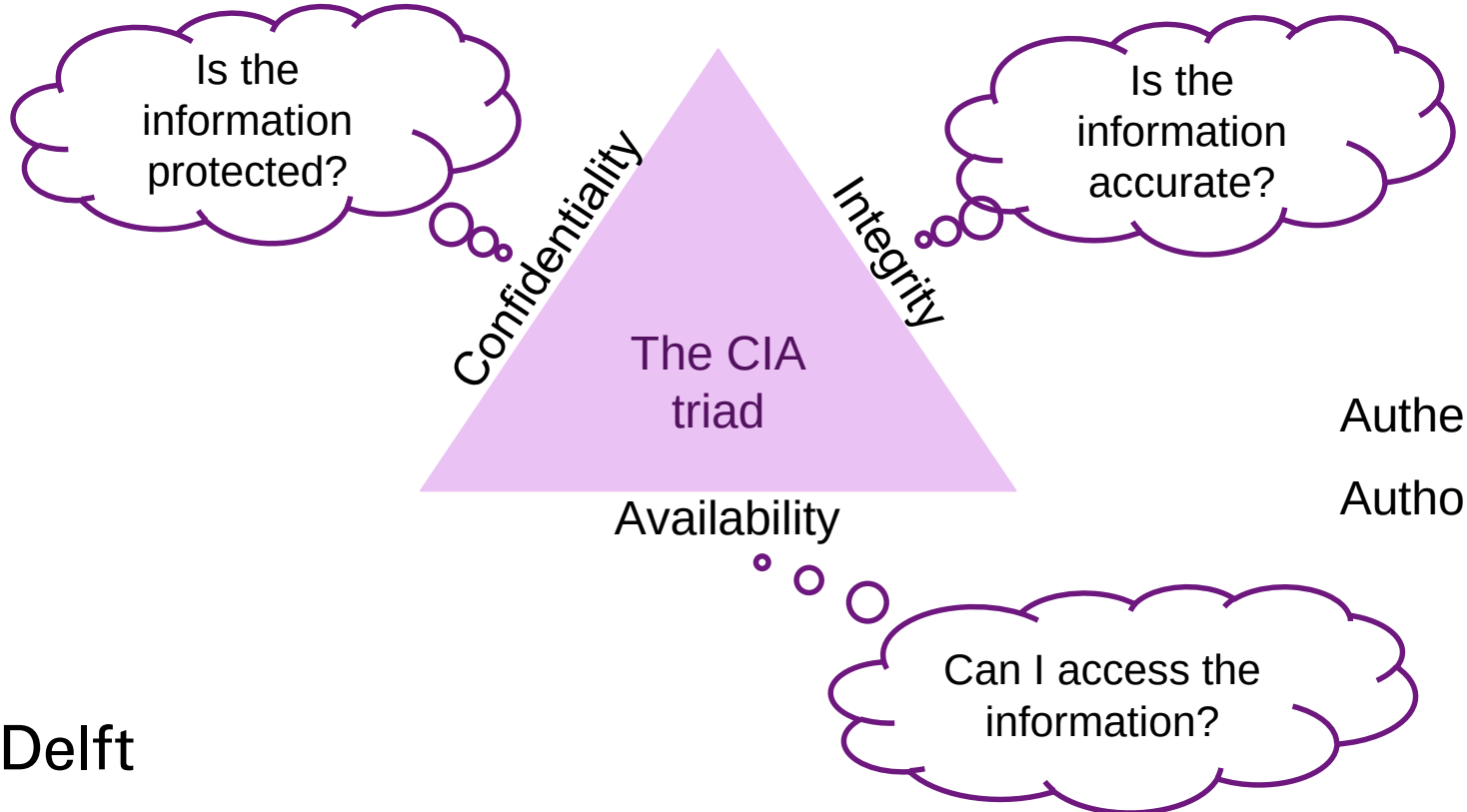
- Web/e-mail security
- Cloud/end-point security

Part IV

- Security by design
- OT security

TU Delft

Information security



Authentication

Authorization

Identity and Access Management (IAM)

- Managing entity access for people via their digital identity

- Authentication factors
  - Password
  - Physical device
  - Biometrics

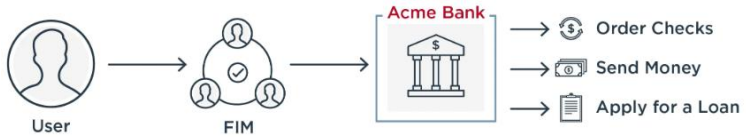
- Allow/block access to assets
  - More granular: Time of day, location, device, …
- Limit platform access
- Limit sensitive data transmission
- Improve logging/reporting

TU Delft

https://www.cisco.com/c/en/us/products/security/identity-services-engine/what-is-identity-access-management.html

Identity and Access Management (IAM)

- Multi-factor authentication (MFA)
  - Multiple authentication factors
  - Time-based One time passwords (TOTP)
  - Inherent factors, e.g., biometrics
- Single-sign on
  - Common authentication factor for multiple Software-as-a-Service (SaaS) applications
  - Authentication token sharing between applications
  - Seamless user authentication (usability)
- Federated Identity Management (FIM)
  - SSO but for different organizations/domains

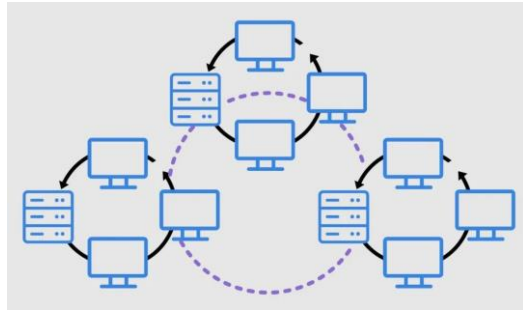


https://www.pingidentity.com/en/resources/blog/post/sso-vs-federated-identity-management.html

Exercise - Access Management

Let’s build an authentication system for a social media site, Schwitter

- Who are we building the authentication system for?
- What are we protecting?
- Whose access do we want to limit?
- How many access tokens are ideal?
  - What kind of authentication tokens are suitable?
- Who gets what access privileges?

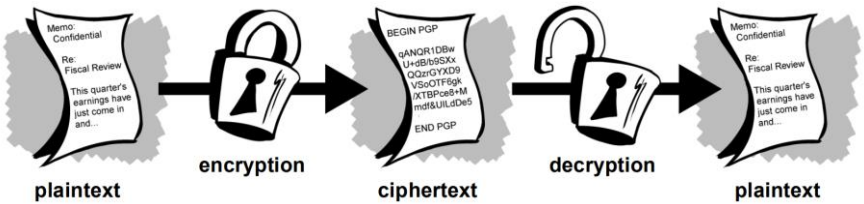


Cryptography basics

"Cryptography is the science of using mathematics to encrypt and decrypt data"

- Phil Zimmermann

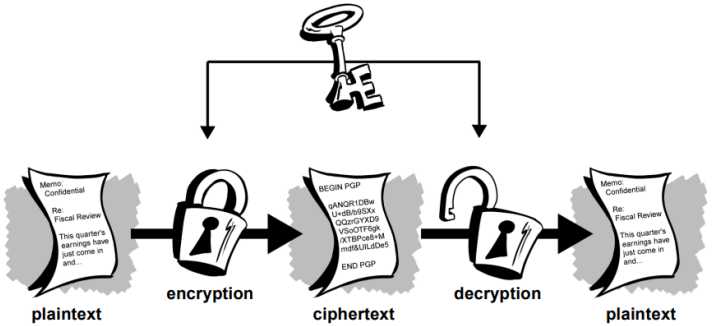
- Plaintext: Message in clear text
- Ciphertext: Garbled message
- Encryption/Decryption: The process of hiding/unhiding plaintext
- Cipher: Algorithm for encryption/decryption
- Encryption/Decryption key: Secret keys for encryption/decryption



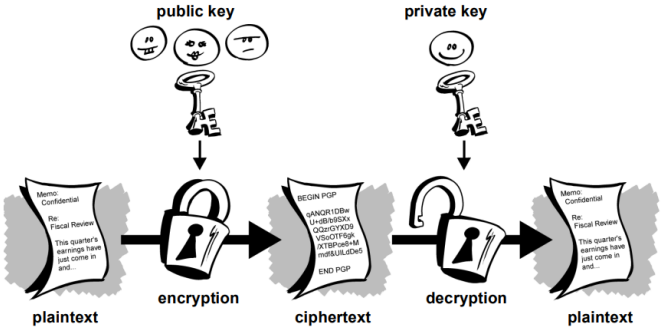
https://www.cs.stonybrook.edu/sites/default/files/PGP70IntroToCrypto.pdf

Cryptography basics

- Symmetric key cryptography
  - Conventional cryptography
  - Sender and receiver of plaintext share a secret key
  - Key management can be a nightmare



- Asymmetric key cryptography
  - Public-key cryptography
  - A pair of keys is used for encryption/decryption
  - Public key for encrypting the plaintext
  - Private key for decrypting the ciphertext

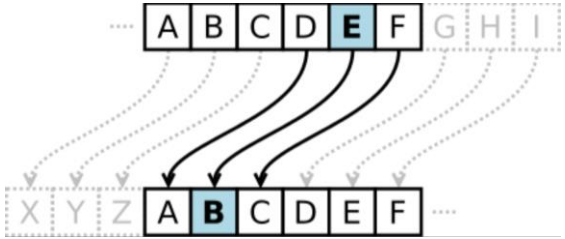


https://www.cs.stonybrook.edu/sites/default/files/PGP70IntroToCrypto.pdf

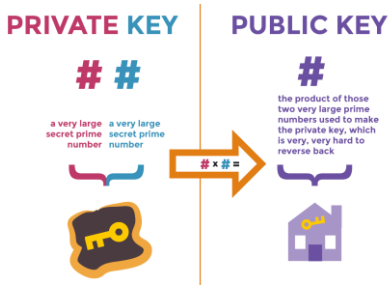
Exercise - Cryptography

- Divide in two groups: Alice and Bob (+ Eve 👽)

- Symmetric key cryptography
  - Cipher: Shift the characters by X
  - X = Secret key
  - Select a plaintext to transmit and encrypt it with X
  - Receiver: decrypt the message



- Asymmetric key cryptography
  - Private key: Alice and Bob select two random prime numbers
  - Public key: Multiply the prime numbers and share the key
  - Select plaintext to transmit and encrypt it with receiver's public key
  - Receiver: Decrypt with own private key



TU Delft

End of Part I
Questions?

TU Delft

Solutions for Threat Detection

"Proactive detection of threats for incident response and threat intelligence creation"

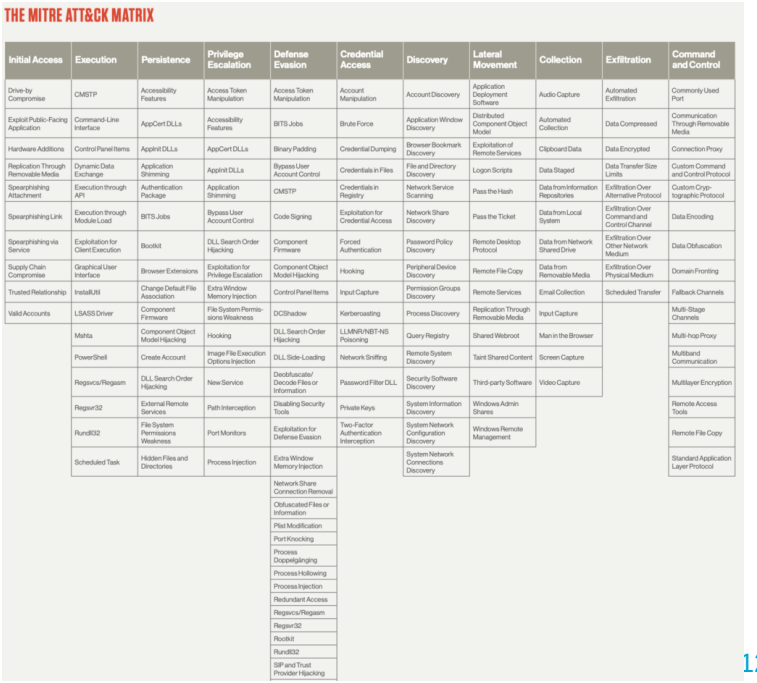
- Security event threat detection (logs, alerts)
- Network threat detection (traffic patterns)
- Endpoint threat detection (user device logs)

"Situational awareness is the understanding of the threat landscape, the risks and possible mitigating measures"

Attacker modeling

- Attacker modeling helps solidify risks
- Lockheed Martin's Cyber Kill Chain
  - Sequence of actions

- MITRE ATT&CK
  - Repository of Tactics, Techniques and Procedures (TTPs)



Monitoring via Security Operations Centers (SOC)

Security Operations Center (SOCs)

https://itsec.group/blog-post-csoc-guide.html

Monitoring via Security Operations Centers (SOC)

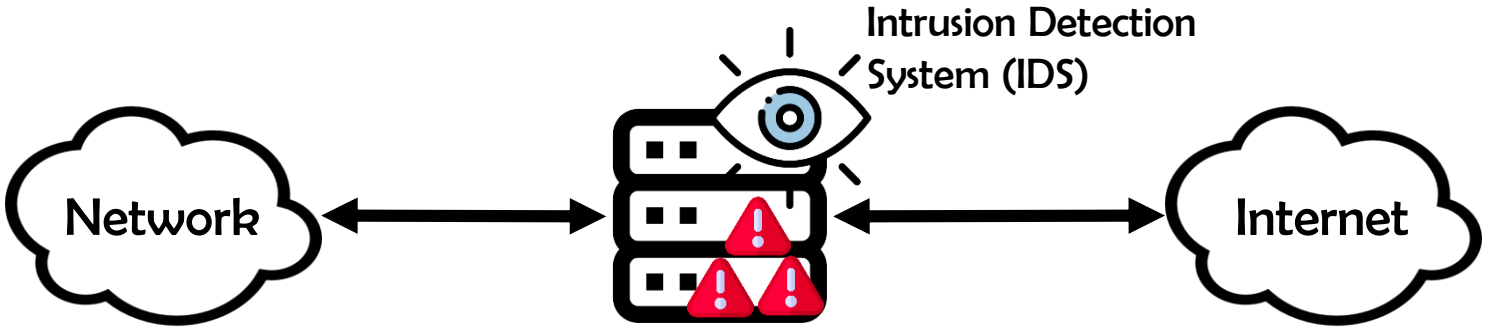
- Tier-1 SOC analysts: Triage threats
  - Monitoring for suspicious activity
- Tier-2 SOC analysts: Incident response and investigation
  - Investigate the origin of a threat and how to respond
- Tier-3 SOC analysts: Threat hunters
  - Look for threats that defenses *did not* pick up

https://itsec.group/blog-post-csoc-guide.html

How can we detect threats?

- Leveraging threat intelligence
  - Open-source Intelligence (OSINT)
  - Public threat intelligence feeds
  - Can detect threats similar to previously seen attacks
- Analyzing attacker behavior
  - Investigate log events for suspicious behavior (deviations from ‘normal’)
  - Can detect previously unseen threats
- Honeypots/honeynets
  - Traps set for attackers
  - Excellent source for behavior analytics and attacker strategy extraction
- Threat hunting/Penetration testing
  - Pretend to be the attacker, generate threat intelligence

Intrusion Detection/Prevention Systems



Alerts


```
{   '_sourcetype': 'suricata:alert',
    'alert': {  'category': 'Attempted Information Leak',
                'severity': 2,
                'signature': 'ET POLICY Python-urllib\\/ '
                             'Suspicious User Agent'},
    'dest_ip': '169.254.169.254',
    'dest_port': 80,
    'src_ip': '10.0.0.20',
    'src_port': 56952,
    'timestamp': '2018-11-03T13:51:58.205548+0000'}
```


Security Operations Center (SOCs)

True threat or False alarm?
What's happening?
Attacker strategy?
Multiple attackers?
…

Intrusion Detection/Prevention Systems

- Intrusion Detection System (IDS)
  - Detects and reports unauthorized access to a network/device
  - Compares incoming traffic with patterns (signatures) of known threats
  - Security analysts decide what to do next

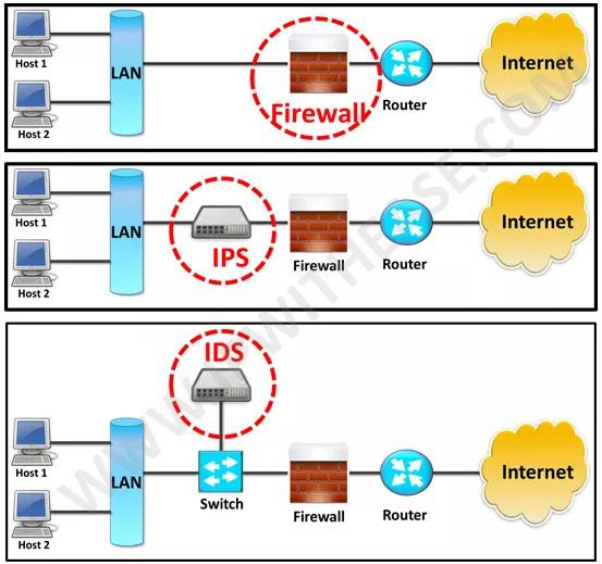
- Intrusion Prevention System (IPS)
  - Blocks, reports or drops unauthorized access events (deploys countermeasures)
  - Real-time traffic monitoring with low overhead
  - Also compares traffic with known patterns

- Both can be hardware or software systems either installed on the network (Network ID/PS) or host (Host ID/PS)

Firewalls

- Hardware or software that monitors traffic and blocks unauthorized access
- Filters network traffic based on firewall rules (e.g., IP addresses, ports)

- Difference from ID/PS
  - ID/PS are standalone devices that monitor/block network traffic invisibly based on general patterns
  - Firewalls are a first line of defense that block traffic based on lower-level Indicators of Compromise (IOCs)



https://ipwithease.com/firewall-vs-ips-vs-ids/

Vulnerability management

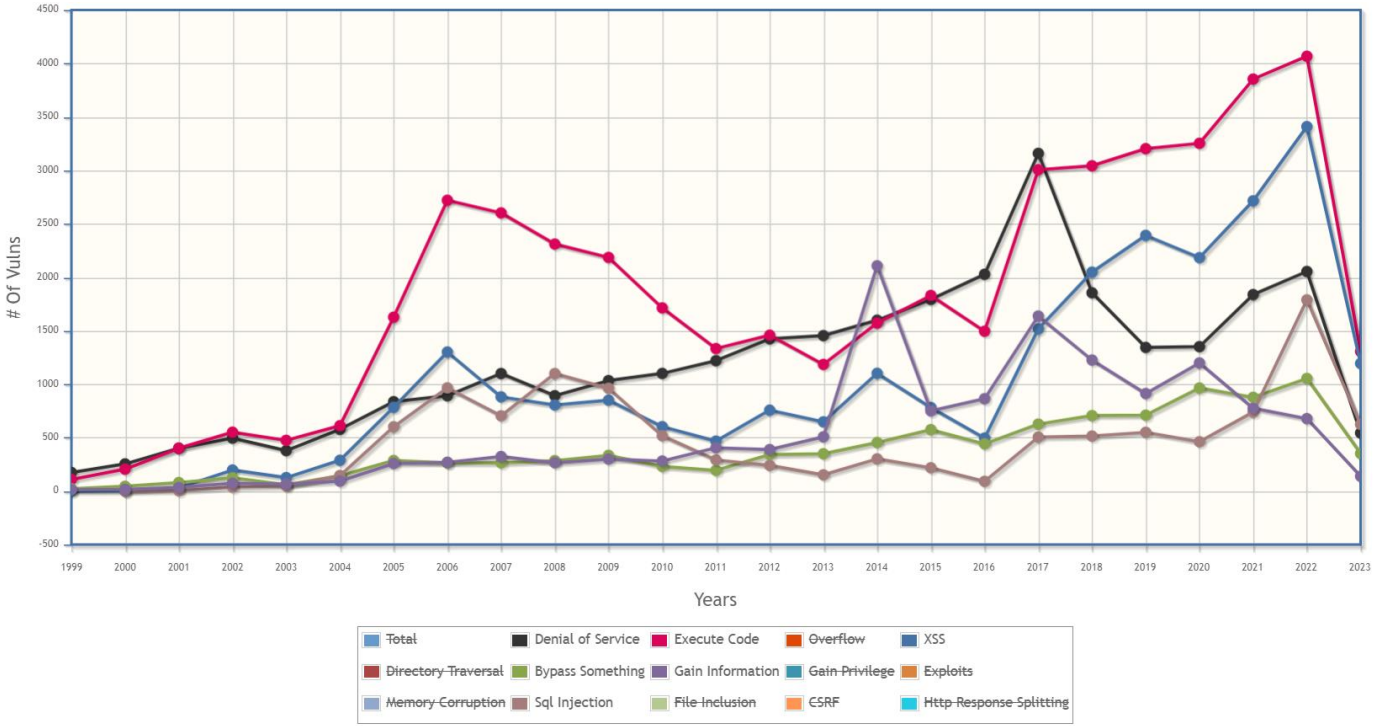
“Proactive approach to identify, manage, and mitigate system vulnerabilities”

- *Vulnerability identification*
  - *Vulnerability scanners/Bug bounties/Penetration testing*
- *Vulnerability Evaluation*
  - *Prioritization based on (CVSS) score and own situational awareness*
- *Vulnerability treatment*
  - *Patch or monitor vulnerabilities*
- *Vulnerability reporting*
  - *Log for future references*

TU Delft

Common Vulnerabilities and Exposures

- NVD database: https://www.cvedetails.com/



OWASP Top-10 Vulnerabilities

- OWASP Top-10 project: https://owasp.org/www-project-top-ten/

1. Broken Access Control
   - Users acting outside of their intended permissions. Leads to information disclosure and destruction.
2. Cryptographic failures
   - Protection of data in transit and at rest. Transmitted in plaintext? Weak algorithm/keys?
3. Injection
   - Insufficient validation enabled attackers to execute code in unauthorized places
4. Insecure design
   - Design flaws that lead to security problems. Insecurity by design.
5. Security misconfiguration
   - Issues like password management, verbose errors, outdated software, improper permission configuration

OWASP Top-10 Vulnerabilities

6. Vulnerable and outdated components
   - Missing awareness of library versions, no scanning, insecure component configurations
7. Identification and authentication failures
   - Enables brute forcing, default or weak passwords, missing MFA, reuse session identifier
8. Software and data integrity failures
   - Issues with integrity, allows installing a new version of software in place of a previously trusted one
9. Security logging and monitoring failures
   - Missing or misconfigured infrastructure for logging that allows to detect, escalate and respond to breaches
10. Server side request forgery (SSRF)
    - Due to poor validation, attackers can coerce a server to redirect a request to an unauthorized location

Exercise – OWASP Top-10

- OWASP Juice Shop: https://juice-shop.herokuapp.com/
- Log in with administrator’s account
- Get to administration’s console
- Get access to secret documents

TU Delft

End of Part II
Questions?

TU Delft

Web security

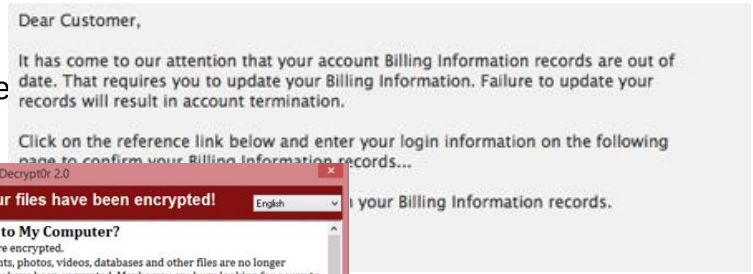
“Protecting networks, computer systems, and web applications from cyber attacks”

- Web Application Firewalls (WAFs)
  - Monitoring all HTTP communication
- Vulnerability scanning and patching
  - Patch the OWASP Top-10
- Black-box testing tools
  - Fuzzing/password cracking tools

E-mail security

“Protecting e-mail users from unauthorized access, data loss, or breach”

- Phishing
  - Attempts to steal passwords/money/assets on websites that pre
  - Examples?
- Ransomware
  - Malware designed to encrypt files and re
  - Examples?
- Spam
  - Unsolicited e-mails sent out in bulk
  - Examples?



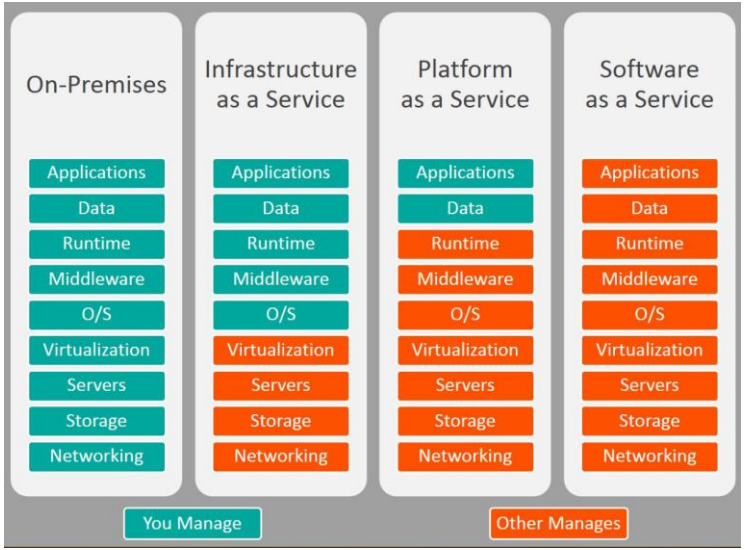
E-mail security

- Verification system
  - Verify the identity of senders
- Spam filters
  - Filter unwanted spam e-mails
- E-mail encryption
  - Prevent messages from being intercepted by attackers
- Detonation capabilities
  - Scan e-mails for malicious links/attachments
- Image and content controls
  - Scan embedded images for malware

Cloud security

"Cloud computing allows users/companies to use cloud servers (located in data centers) without having to manage physical servers or run software applications on their own systems"

- Software-as-a-service (SaaS) → Users
  - Cloud-based software applications hosted online
- Platform-as-a-service (PaaS) → Developers
  - Cloud-based software development and delivery framework that manages operating systems, software updates, storage, and supporting infrastructure
- Infrastructure-as-a-service (IaaS) → Administrators
  - Cloud-based infrastructure for hardware, storage, networking, …



Cloud security

- Increased attack surface and lack of visibility
  - 3rd party controls, PaaS and SaaS provide little control to administrators compared to IaaS
- Multi-tenancy
  - Multiple services housed under the same environment, making cross-contamination possible
- Access management and shadow IT
  - Bring your own device (BYOD) makes access control even more difficult
- DevSecOps
  - Development, Security, and Operations → Secure software development lifecycle (Secure SDLC)
- Compliance and governance
  - Heavy reliance on 3rd party services can make compliance more costly

Cloud security

- Granular, policy-based IAM and authentication controls across complex infrastructures
- Zero-trust network security controls across logically isolated networks and micro-segments
- Safeguarding all applications with next-gen web application firewall
- Enhanced data protection
- Threat intelligence that detects and mitigates known/unknown threats in real-time

https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/

End-point/Mobile device security

“Protecting end-points or entry devices, such as user laptops, printers, smartphones, smartwatches, etc. from malicious attacks. Endpoint security is the practice of safeguarding the data and workflows associated with the individual devices that connect to a network.”

- Workplaces have fundamentally changed
  - Remote work
  - Bring your own device (BYOD)

- Works in collaboration with cloud security to reduce overhead on end devices
- Monitoring devices/files as they enter a network
- Client software installation/updates managed remotely
- Stopping unauthorized users from accessing the enterprise network

TU Delft

End-point/Mobile device security

- Beware of apps
- Password policies and biometrics
- Avoid public WiFi networks
- Utilize VPNs
- Mobile device encryption
- Email security

TU Delft

Anti-virus/anti-malware

“A software that scans, detects, averts, and removes viruses/malware from a computer”

- Signatures
  - Files are scanned for suspicious signatures from a database
- Heuristics
  - The behavior and characteristics of a file are monitored
- Sandboxing
  - Runs a suspicious file in a sandbox to analyze it, preventing damage to the user’s system
- Removal
  - Quarantines the malicious file and removes it from the system

Malwarebytes

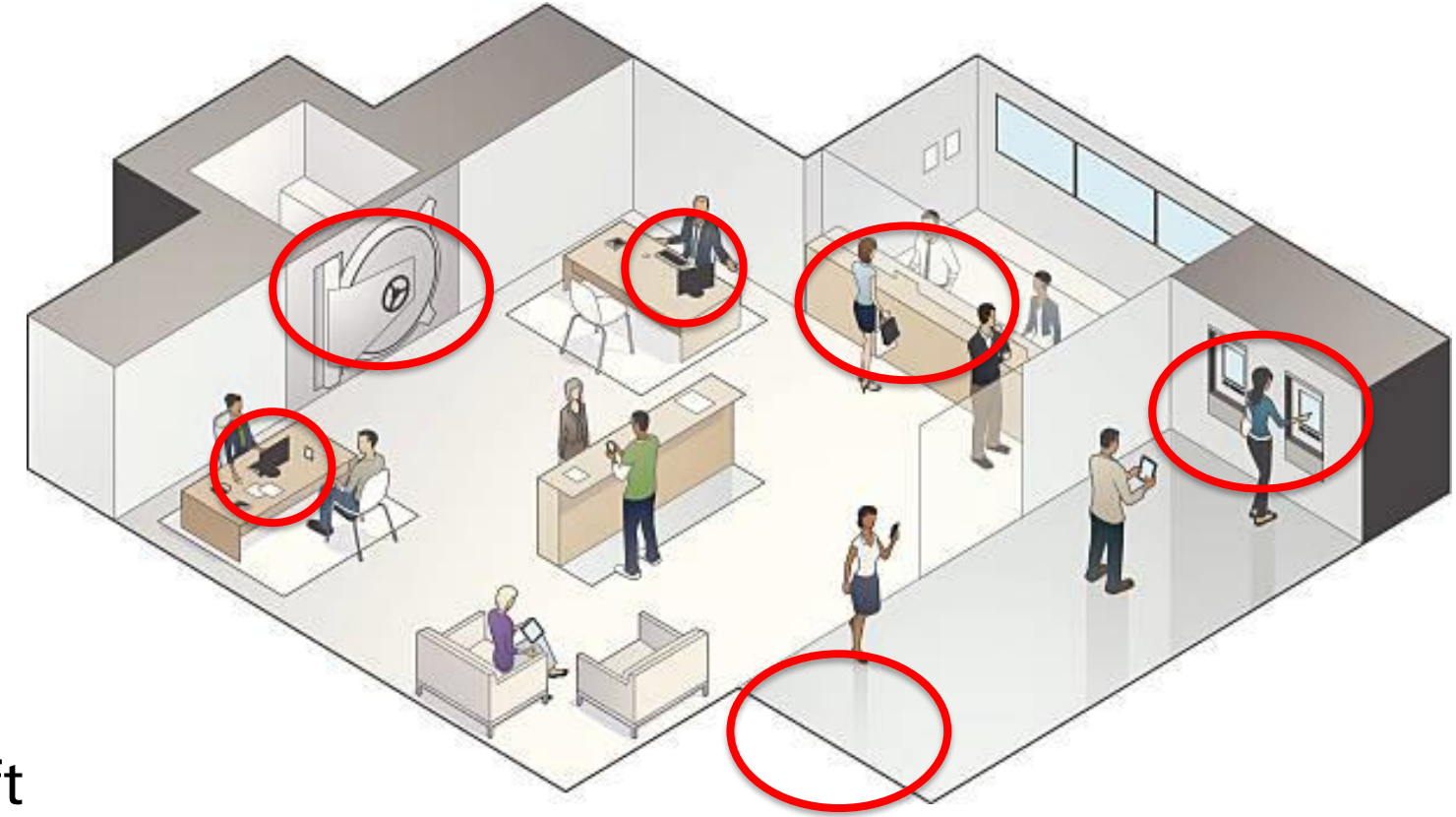
TU Delft

Exercise – Anti-Malware

- What capabilities do the following anti-virus/anti-malware provide?
- McAfee
- BitDefender
- Malwarebytes
- Norton

End of Part III
Questions?

Exercise - Defense-in-depth



Security by design

- How would you go about designing for security?

Security by design

- Defense in depth
- Least privilege
- Minimize attack surface
- Open design
- Isolated compartments
- Evidence production

https://learn.microsoft.com/en-us/azure/architecture/framework/security/design-segmentation
https://www.redhat.com/en/blog/security-design-security-principles-and-threat-modeling

OT Security

“The measures and controls in place to protect Operational Technology systems that use purpose-built software to automate industrial processes”

- Mission-critical applications with high availability requirement
  - Typically also legacy systems
  - Systems include sensors, monitors, actuators, generators, programmable logic controllers (PLCs), industrial robots, …
- Becoming important now that IT and OT are converging
- Risks to critical infrastructure, e.g., power stations, or smart city applications
- Attacks can be physically destructive

TU Delft

OT Security

- Map your environment
  - Situational awareness of all devices and assets in the network
  - Identify, classify, and prioritize assets
- Continuous monitoring
  - Identify unusual activity anywhere in the ecosystem
- Incorporate redundancy
  - Use multiple scanners to monitor sensors, etc.
- Adopt zero trust framework
  - Any device or user may be a threat until authenticated. Use MFA

TU Delft

OT Security

- Leverage identity and access management
  - In addition to IT environments, also necessary in OT environments
- Train your workforce
  - Most important: educate personnel to identify (modern) threats coming from IT and OT side
- Application-level micro segmentation
  - Defense-in-depth on steroids
  - Allows to protect every internal device with policy-driven, application-level security controls
  - Segment critical devices away from accessible network

OT Security

- Stuxnet attack: https://www.youtube.com/watch?v=DDH4m6M-ZIU&ab_channel=Stanford

End of Part IV
Questions?

TU Delft

Recap

Let’s fill it out together

- ??