Fundamentals of Network Security

CryptoWorks21 • July 12–16, 2021

Dr Douglas Stebila

https://www.douglas.stebila.ca/teaching/cryptoworks21

Fundamentals of Network Security

1. Basics of Information Security
   - Security architecture and infrastructure; security goals (confidentiality, integrity, availability, and authenticity); threats/vulnerabilities/attacks; risk management
2. Cryptographic Building Blocks
   - Symmetric crypto: ciphers (stream, block), hash functions, message authentication codes, pseudorandom functions
   - Public key crypto: public key encryption, digital signatures, key agreement
3. Network Security Protocols & Standards
   - Overview of networking and PKI
   - Transport Layer Security (TLS) protocol
   - Overview: SSH, IPsec, Wireless (Tool: Wireshark)
4. Offensive and defensive network security
   - Offensive: Pen-tester/attack sequence: reconnaissance; gaining access; maintaining access; denial of service attacks (Tool: nmap)
   - Defensive: Firewalls and intrusion detection
5. Access Control & Authentication; Web Application Security
   - Access control: discretionary/mandatory/role-based; phases
   - Authentication: something you know/have/are/somewhere you are
   - Web security: cookies, SQL injection
   - Supplemental material: Passwords

Fundamentals of Network Security

- Lectures:
  - Monday-Friday
  - 3:30-5pm Waterloo time
  - Zoom

- Practicals / assessment:
  - Practical hands-on exercises with network and application security, with a few questions to submit from each
    - Involves work on Kali Linux virtual machine
  - Download from https://www.douglas.stebila.ca/teaching/cryptoworks21
  - Due Friday August 12, 2021 for those taking the workshop for credit in CryptoWorks21 program

Fundamentals of Network Security

1. Basics of Information Security

CryptoWorks21 • July 12, 2021

Dr Douglas Stebila

UNIVERSITY OF WATERLOO

https://www.douglas.stebila.ca/teaching/cryptoworks21

Lecture Goals

- Develop a broader perspective on information security than just cryptography.

- Terminology for describing information security.
- How do organizations approach making information security decisions?

- Non-technical lecture today; technical lectures to follow.

Information Security Process

1. Identify information assets
2. Describe security goals for assets
3. Characterize threats
4. Identify vulnerabilities
5. Assess risks
6. Apply controls

SECURITY TERMINOLOGY

Information Security Process

1. **Identify information assets**
2. **Describe security goals for assets**
3. Characterize threats
4. Identify vulnerabilities
5. Assess risks
6. Apply controls

What is Security?

- **Security** is about the protection of assets from damage or harm.
- **Assets** are items or processes that are of value
  - Property
  - People
  - Intangibles

Assets

- For effective protection you need to know:
  - What the assets are
  - What they are worth, and how critical they are
  - What could possibly happen to affect them
    - Consider accidental and intentional events
  - How they could be protected, and at what cost?
    - Consider possibilities for:
      - Prevention of damage to asset (or minimising damage)
      - Detection of damage to asset – when, how, who?
      - Reaction to recover from damage

Information Security Goals or Services

Traditional definitions of information security are based on three information security goals or services:

- **Confidentiality**: preventing unauthorised disclosure of information
- **Integrity**: preventing unauthorised (accidental or deliberate) modification or destruction of information
- **Availability**: ensuring resources are accessible when required by an authorised user

Additional Goals or Services

These additional goals or services are becoming increasingly important for some applications:

- **Authentication**:
  - Entity authentication – the process of verifying a claimed identity
  - Data origin authentication – verify the source (and integrity) of a message
- **Non-repudiation**:
  - create evidence that an action has occurred, so that the user cannot falsely deny the action later

Information States

- Information security involves protecting information assets from harm or damage.
- Consider information in one of three possible states:
  - **Storage**
    - Information storage containers – electronic, physical, human
  - **Transmission**
    - Physical or electronic
  - **Processing** (Use)
    - Physical or electronic

THREATS, VULNERABILITIES, AND ATTACKS

Information Security Process

1. Identify information assets
2. Describe security goals for assets
3. **Characterize threats**
4. **Identify vulnerabilities**
5. Assess risk
6. Apply controls

Threats, Vulnerabilities, and Attacks

- Information security analysis involves considering:
  - **Threats:**
    - Sets of circumstances with the potential to cause harm by compromising stated security goals
  - **Vulnerabilities:**
    - Weaknesses in a system that could be used to cause harm by compromising stated security goals
  - **Attacks:**
    - Occur when vulnerabilities are deliberately exploited
    - **Security incidents** can also result from non-deliberate acts.

Threats

- Set of circumstances with *potential* to cause harm to an information asset by compromising stated information security goals.
  - **A breach of confidentiality**: information is disclosed to unauthorised entities
  - **A breach of integrity**: information assets have been modified or destroyed by unauthorised entity
  - **A breach of availability**: information assets are not accessible when required by an authorised entity

Threat Sources

- External:
  - Source of threat lies outside of the organisation
  - Example:
    - People who are not authorized to use information systems - commercial competitor, cyber-criminal, political activist, terrorists
- Internal:
  - Source of threat lies within the organisation
  - Example:
    - people who are authorized to use information systems - employees, contractors, clients, visitors

Internal Threat Sources

- Insiders are familiar with information systems used in an organisation:
  - Have knowledge of asset values
  - Know processes and procedures in use
  - May be aware of system vulnerabilities
  - Have opportunity to access assets
  - May misuse systems or exceed their authorization
  - Potential to cause harm is high
  - Outsourcing (cleaners, catering, support services) without security assurance brings outsiders in

Types of threats

- Natural events
  - E.g., Earthquake, fire, flood, storm, tornado, tidal wave
  - Most likely to compromise availability
- Human actions
  - Deliberate / malicious (intended to cause harm)
    - E.g. Espionage, fraud, sabotage, theft
  - Accidental / benign (no intent to cause harm)
    - E.g. Negligence, errors, omissions

Threat – Human action – Deliberate – **Malware**

- Malicious software deliberately designed to breach security of computer based information systems
- Depending on the payload action, malware could compromise:
    - Confidentiality: For example, logging keystrokes to obtain passwords
    - Integrity: For example, by writing a message, or corrupting data files
    - Availability: For example, by deleting data or application files

Threat – Human action – Deliberate – **Malware**

- Common malware types:
  - **Viruses** – programs with ability to replicate
    - Spreads by copying itself into other files (infecting) and is activated when these files are open or executables are run
  - **Worms** – programs with ability to self replicate
    - Spreads from computer to computer without human interaction
  - **Trojan horses** – programs with known desirable properties and hidden undesirable property.
    - User downloads the program and knowingly uses desirable features
    - Undesirable feature runs without user knowledge

Vulnerabilities

- Weaknesses in a system
  - that could be used to cause harm to information assets

- Need to consider components of information system:
  - Property
  - People
  - Procedures

Vulnerabilities: Property

- **Physical assets**: buildings and contents
  - Location; physical security; maintenance; monitoring and logging physical access
- **Hardware**: computer systems, data communications devices, data storage devices
- **Software**: Operating system, applications
  - Source; testing; updates; (mis)configuration
- **Data**: Files, databases, passwords

Vulnerabilities: People

- **Employees**:
  - Recruiting staff suitable for the position
    - Failure to check background is common
  - Monitoring access of people to property and processes
    - Disgruntled employees, clients or contractors can be threat source
  - Inadequate education of staff with respect to threats: for example, are staff aware of policies regarding:
    - providing information by email or over phone
    - downloading software,
    - use of mobile devices, etc

Vulnerabilities: People

- **Employees**:
  - Are there key personnel critical to organisation?
    - May be unavailable due to accident or illness, or other event (transport failure, natural disaster)
  - Vulnerable if no back-up for these people
    - If procedures are undocumented
- **Others**:
  - Are security conditions included in contracts with consultants, contractors, outsourcing?

Vulnerabilities: Processes

- **Access control** and privilege management
  - Including keys, cards, passwords
- **Backup** of files and systems
- **Business continuity plans**
  - for recovery of information assets after disaster
- **Communications**

Vulnerabilities: Processes

- **Checks and balances**:
  - People make mistakes: are there processes to detect, correct or reduce the impact of errors?
    - Example: Separation of duties
- Processes associated with staff **joining/leaving** organisation
  - Clear statement of duties
  - Nondisclosure/confidentiality agreements
- **Software management** processes and auditing

Attacks

- **Attacks**:
  - occur when vulnerabilities are deliberately exploited
- **Attacker**:
  - person who deliberately attempts to exploit a vulnerability to
    - gain unauthorized access, or
    - perform unauthorized actions

- **Security incidents** can also result from non-deliberate acts.

Attacks

Passive

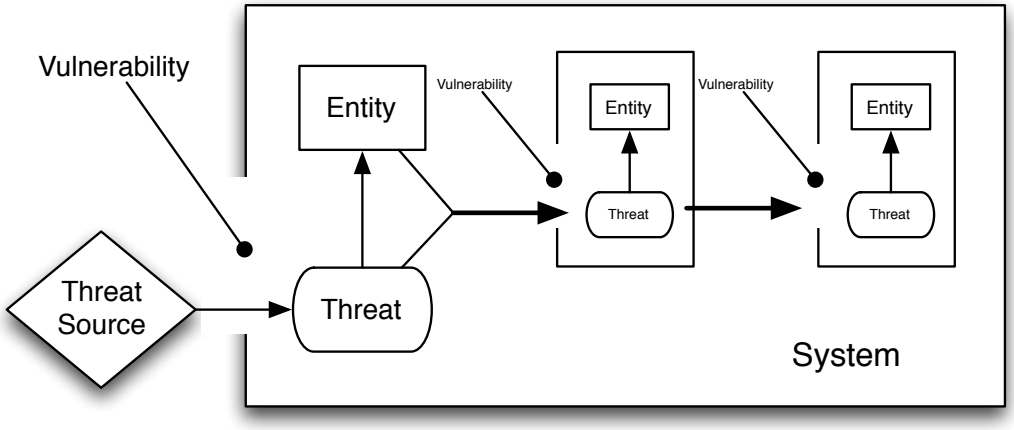
- Attacker's goal is to obtain information
- Attacker doesn't alter system resources or interact other than by listening or observing
  - E.g. eavesdropping, shoulder surfing
- Difficult to detect; usually try to prevent the attack.

Active

- Attacker's goal may be to modify, replicate or fabricate information
- Requires interaction with the information system by the attacker
  - E.g. Phishing, Denial of service, Man-in-the-middle
- Try to detect attacker's actions, recognise signs of attack and respond

Security Incidents and Attacks

- When threats and vulnerabilities coincide, information assets can be harmed
  - a security incident (maybe an attack) occurs
  - Sometimes can be a chain of events, especially in interconnected systems



Passive Attacks

- **Eavesdropping**
  - Listening to the conversations of others without their knowledge or consent
  - Wiretapping
    - Eavesdropping over telephone network
    - May be harder to detect in wireless network
  - Information can be obtained from:
    - the content of the conversations, and
    - knowing who is talking to who and when (traffic analysis)

Passive Attacks

- **Shoulder surfing**
  - Watching the actions of others (especially at data entry) without their knowledge or consent
  - Usually connected with entry of confidential information
    - PIN (for financial access at ATM)
    - Security code or password
  - Can also be for greater amounts of data
    - Use of mobile devices in insecure surroundings is vulnerability that can be exploited for this attack

Passive Attacks

- **Network monitoring and eavesdropping**
  - A packet sniffer or network analyzer can monitor network traffic
    - can be used for network maintenance (finding faults and traffic problems)
    - But can also be used to gain knowledge of confidential information
    - e.g passwords corresponding to user names
  - Confidential information should not be sent over untrusted networks without protection
    - Example: when logging on to a remote resource, passwords should not be sent ‘in the clear’

Active Attacks

- **Denial of Service (DoS) Attack**
  - Objective is to make an information asset or resource unavailable to authorized users
  - Common methods are:
    - To overload the resource, so it cannot respond to legitimate requests
    - To damage the resource, so that it can not be used
    - To deliberately interrupt communications between users and resource, so that it can not be accessed

Active Attacks

- **Distributed Denial of Service (DDoS) Attack**
  - Objective is same as DoS attack:
    - Breaches availability of information asset
  - Method:
    - Use multiple sources to make resource requests
    - Hope to overload resource, so it cannot respond to legitimate requests
    - Malware (e.g. virus) may be used to compromise many machines
      - all have same target, and payload is activated at same time, to make simultaneous resource request

Active Attacks

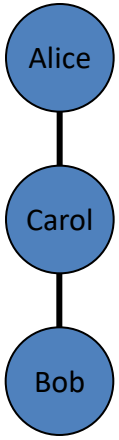
- **Masquerade/Spoofing**:
  - Where one entity pretends to be another in order to deceive others
- Common spoofing attacks include:
  - Email address spoofing
    - Altering the sender information on email to trick recipients into thinking the message is from another source
  - Webpage spoofing
    - Creating a fake webpage that looks like the page for a legitimate business to trick users
      - into giving the credentials they would use at legitimate site
      - Into downloading materials from an alternative site

Active Attacks

- **Phishing**:
  - Attempts to gain credentials to enable access to other resources by masquerading as a legitimate organisation (Bank, eBay, PayPal)
    - Example: account details, PIN number, password
  - Usually involves
    - spoofed emails and/or spoofed web pages
    - social engineering

Active Attacks

- **Man-in-the-Middle Attack (MITM)**
  - An attacker (Carol) positions herself between two entities who wish to communicate, say Alice and Bob.
  - Carol pretends to Alice she is Bob, and pretends to Bob she is Alice (spoofing).



MITM

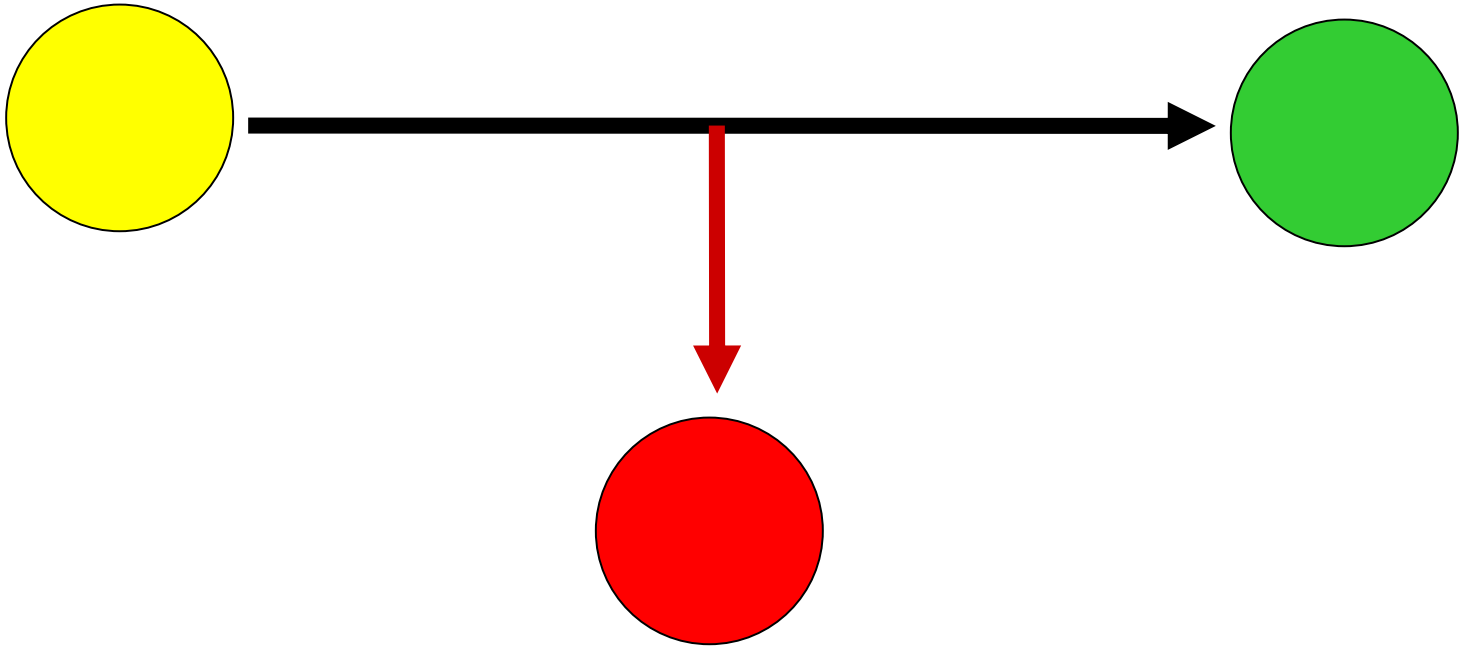
- Normal information flow

Information Source (Alice)

Information Destination (Bob)

MITM Interception

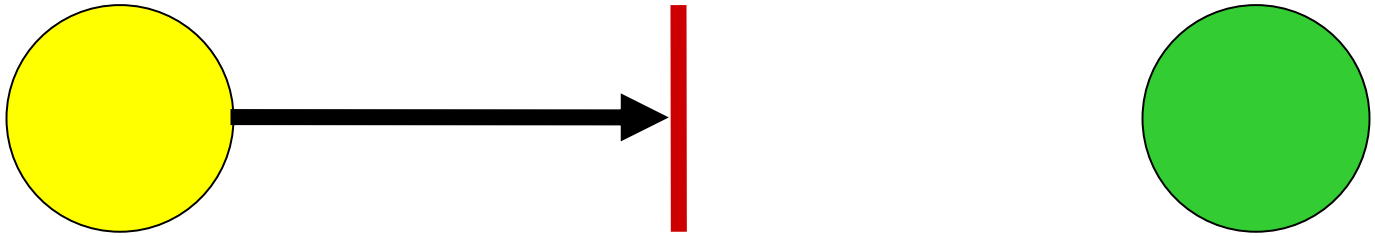
- The unauthorized MITM observes the information and transmits it



Breaches confidentiality

MITM Interruption

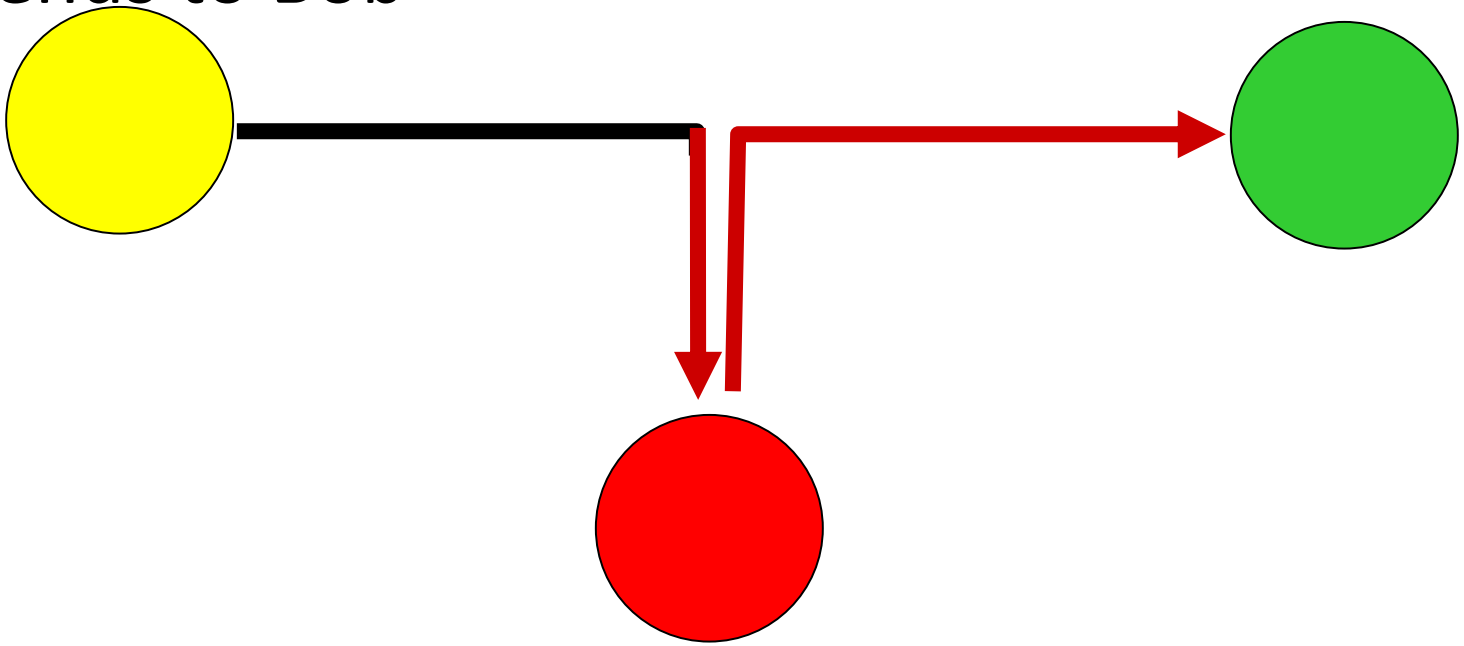
- The unauthorized MITM prevents transmission, so information assets are unavailable to Bob



Breaches availability

MITM Modification

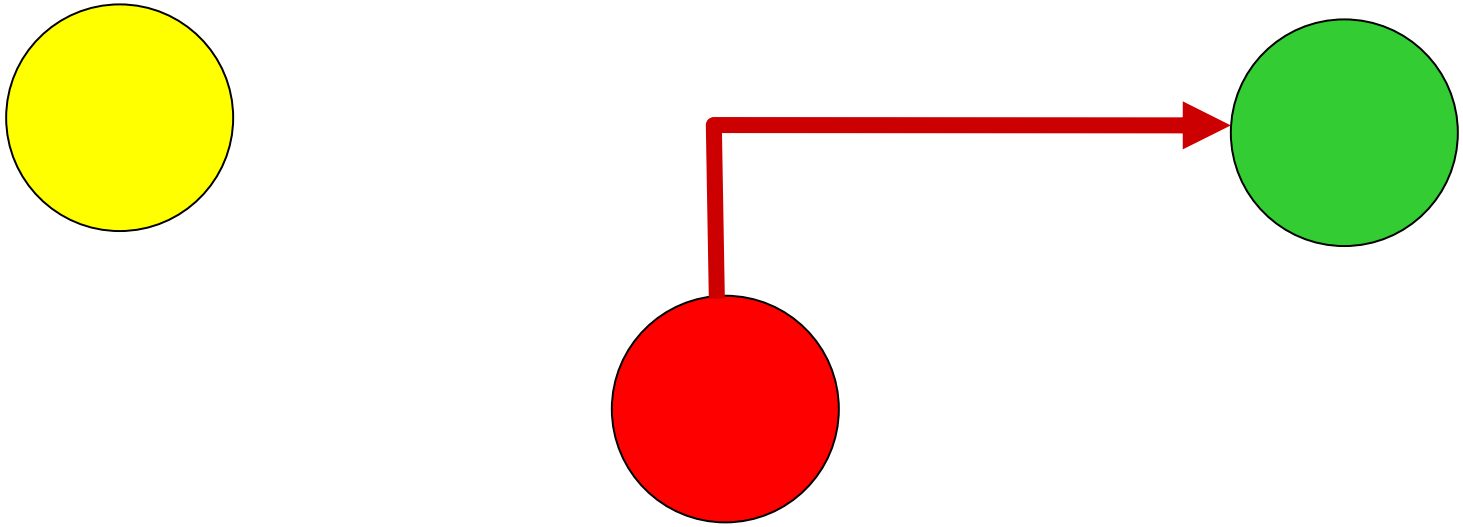
- The MITM modifies the information and then sends to Bob



Breaches integrity

MITM Fabrication

- The MITM creates information asset and sends to Bob but claims it is from Alice



Breaches authenticity

Active Attacks

- **Social Engineering**: using social skills to convince people to reveal information or permit access to resources.
- Examples:
  - Claim to be new employee, manager's assistant, maintenance person, etc and ask for assistance in accessing resource to complete an urgent task:
    - I've lost my password and I have to finish this today …
    - My swipe card doesn't work/left at home …
  - Tailgating – follow another person closely so that when they go into secure area you can also get in without providing appropriate credentials

Active Attacks

- **Replay attack**:
  - This is where a valid data transmission is recorded, and retransmitted at a later date
  - Example:
    - Access to a system requires use of password, but password is encrypted during transmission
    - Attacker records encrypted password, and replays this information in order to gain access
    - Doesn't matter that attacker doesn't know the password – they could provide the expected credential on request.

Threats, Vulnerabilities, and Attacks

- Information security analysis involves considering:
  - **Threats:**
    - Sets of circumstances with the potential to cause harm by compromising stated security goals
  - **Vulnerabilities:**
    - Weaknesses in a system that could be used to cause harm by compromising stated security goals
  - **Attacks:**
    - Occur when vulnerabilities are deliberately exploited
    - **Security incidents** can also result from non-deliberate acts.

RISK MANAGEMENT

Information Security Process

1. Identify information assets
2. Describe security goals for assets
3. Characterize threats
4. Identify vulnerabilities
5. **Assess risk**
6. Apply controls

Information security and risk management

- What is risk?
- How do we manage risk?
- Risk management and standards
  - ISO 31000:2009 Risk Management
  - ISO 27005:2012 Information Security Risk Management
- Information Security Management Standards
  - ISO 27001:2006 Info Sec Management Systems
  - ISO 27002:2006 Code of practice for IS management

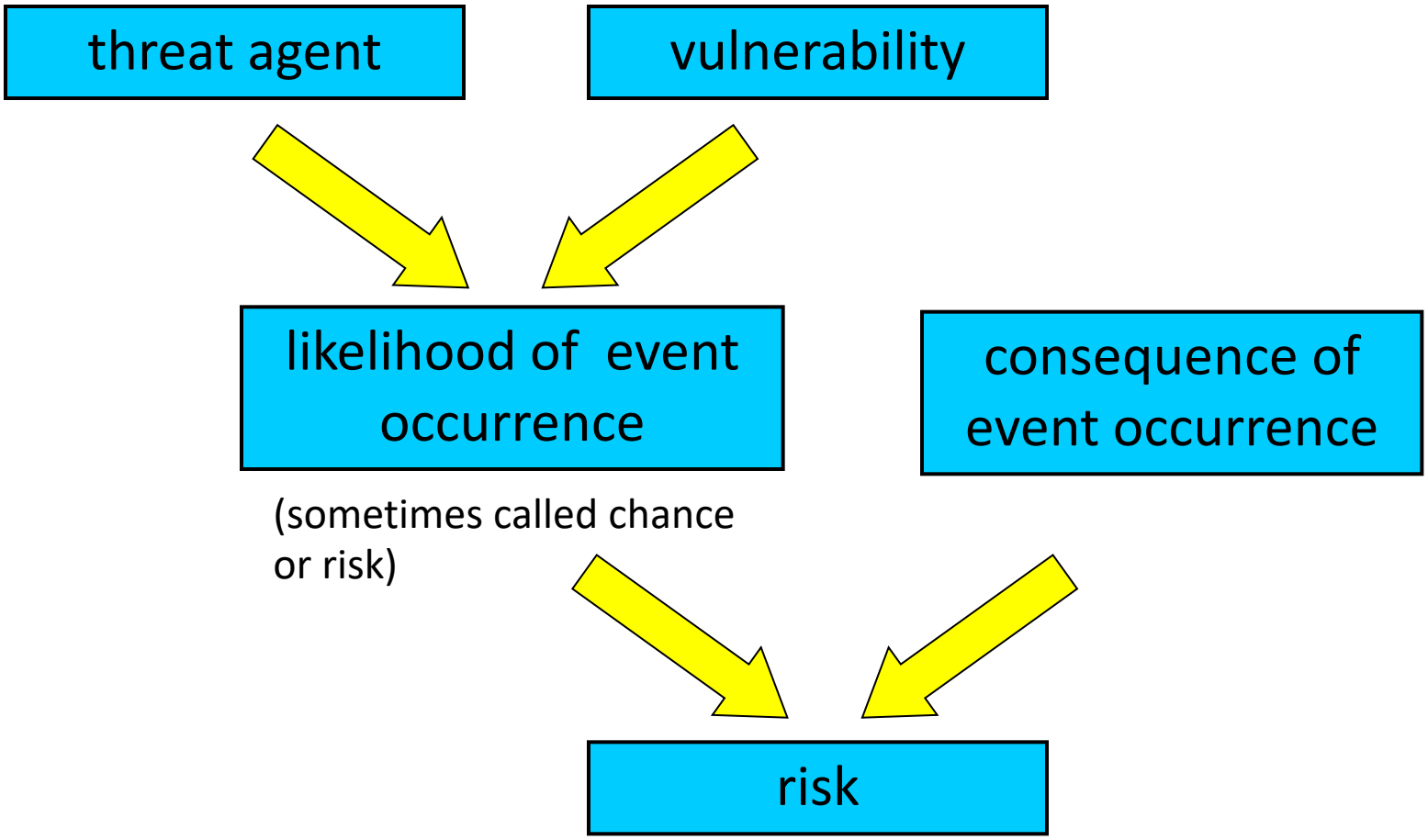
What is risk?

- Definition in ISO 27005:2012 Information security risk management

- **Risk: "effect of uncertainty on objectives"**

- Effect includes both positive and negative
- Aspects of objectives to consider:
  - financial, health and safety, information security, environmental
- May apply at different levels:
  - organizational, project, product, process
- Information security risk expressed in terms of consequences and likelihood
  - Consequence: "outcome of an event affecting objectives"
  - Likelihood: ‘chance of something happening’

Risk


threat agent
vulnerability
likelihood of event occurrence
consequence of event occurrence
(sometimes called chance or risk)
risk
(sometimes called business risk)

Risk management: **Establish context**

- Define **risk criteria** (Criteria against which risk is to be evaluated)
- For risk evaluation criteria consider:
  - Strategic value of the asset,
  - Criticality of the asset,
  - Legal, regulatory or contractual obligations,
  - Reputation
- For impact evaluation criteria consider:
  - Level of classification of asset, and type of breach (CIA)
  - Degree of impairment/disruption/loss of business
- For risk acceptance criteria consider:
  - What the timeframes will be
  - What level of risk is acceptable to organisation, etc

Risk management: **Identify risks**

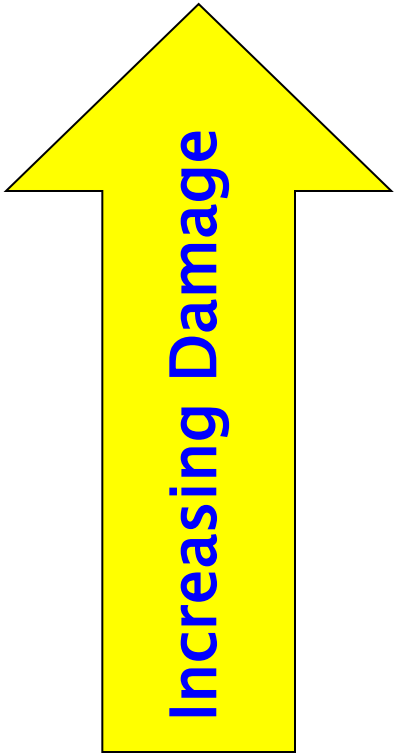
- What can happen, where and when?
  - Identify plausible threats and existing vulnerabilities: combine these to identify events and potential consequences
- Why and how it can happen?
  - Consider causes and scenarios
- Tools and techniques:
  - Identify risks using
    - Checklists (From other standards documents)
    - Judgements based on experience (own and others)
    - Systems analysis
- Include all risks, whether they are under the control of the organisation or not.

Risk management: Analyze risks

- Determine the magnitude of identified risks
- Types of analysis:
- **Qualitative**
  - Uses descriptive scales (in words). Example:
    - **Consequence**: Minor, moderate, major, catastrophic
    - **Likelihood**: Rare, unlikely, possible, likely, almost certain
- **Semi-quantitative**
  - Qualitative scales assigned numerical values
  - Can be used in formulae for prioritization (with caution!)
- **Quantitative**
  - Use numerical values for both consequence (e.g. $$$) and likelihood (e.g. probability value)

Example: Qualitative Risk Analysis

- **Qualitative Consequence** scale example:

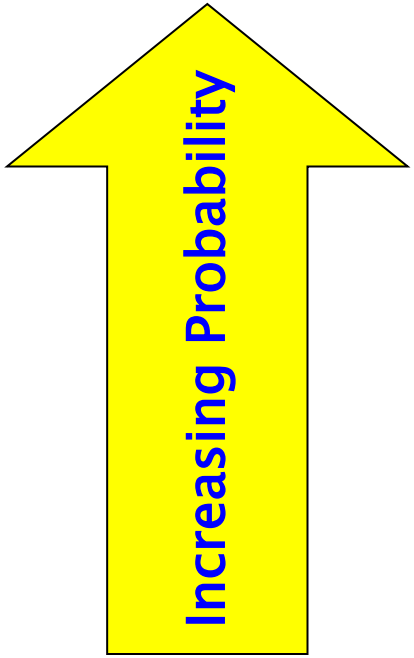


Measure	Description
Major	**Major problems** would occur and threaten the provision of important processes **resulting in significant financial loss**.
Moderate	**Services would continue**, but would **need to be reviewed or changed.**
Minor	Effectiveness of services would be **threatened but dealt with**.
Insignificant	Dealt with as a part of **routine operations**.

Information Risk Management Best Practice Guide p19

Example: Qualitative Risk Analysis

- **Qualitative Likelihood** scale example:



Measure	Description
High	Is expected to occur in most conditions (1 or more times per year).
Medium	The event will probably happen in most conditions (about once every 2 years).
Possible	The event should happen at some time (once every 5 years).
Unlikely	The event could happen at some time (once every 10 years).

Information Risk Management Best Practice Guide p19

Example: Qualitative Risk Analysis

- Match consequences to likelihoods to determine levels of risk

Consequence

Likelihood	Insignificant	Minor	Moderate	Major
High	M	H	E	E
Medium	M	M	H	E
Low	L	M	M	H
Unlikely	L	L	M	M

Legend
E: extreme risk; immediate action required
H: high risk; senior management attention needed
M: moderate risk; management responsibility must be specified
L: low risk; manage by routine procedures

Risk management: **Evaluate risks**

- Compare the level of risk found during risk analysis with the established risk criteria

- **Decide** which risks need treatment, and when
  - Prioritize list of risks for further action
    - Risks in low or moderate risk categories may be accepted without further treatment
    - High or extreme risks require immediate consideration of treatment possibilities

Risk management: Treak risks

- Select options for modifying risks:

- Options for risk treatment with negative outcomes include:
  - **Avoid** the risk
  - **Reduce likelihood** of negative outcome by:
    - Reducing the likelihood of the risk
    - Reducing the consequences
  - **Share** the risk
  - **Retain** the risk

Example risk assessment: effect of quantum computers on classical cryptography

- Context: a large bank uses RSA public key cryptography and AES encryption to secure communication over the public internet between its branches
- Identify risks: large-scale quantum computers will render RSA encryption completely insecure and impact key length of AES encryption

Example risk assessment: effect of quantum computers on classical cryptography

- Analyze risks:
  - consequence:
    major / moderate / minor / insignificant
  - likelihood:
    high / medium / possible / unlikely
- Evaluate risks: prioritize risks based on consequence x likelihood
- Treat high priority risks
  - Should the bank switch to QKD? post-quantum crypto?

CONTROLS

Information Security Process

1. Identify information assets
2. Describe security goals for assets
3. Characterize threats
4. Identify vulnerabilities
5. Assess risk
6. **Apply controls**

Security Measures or Controls

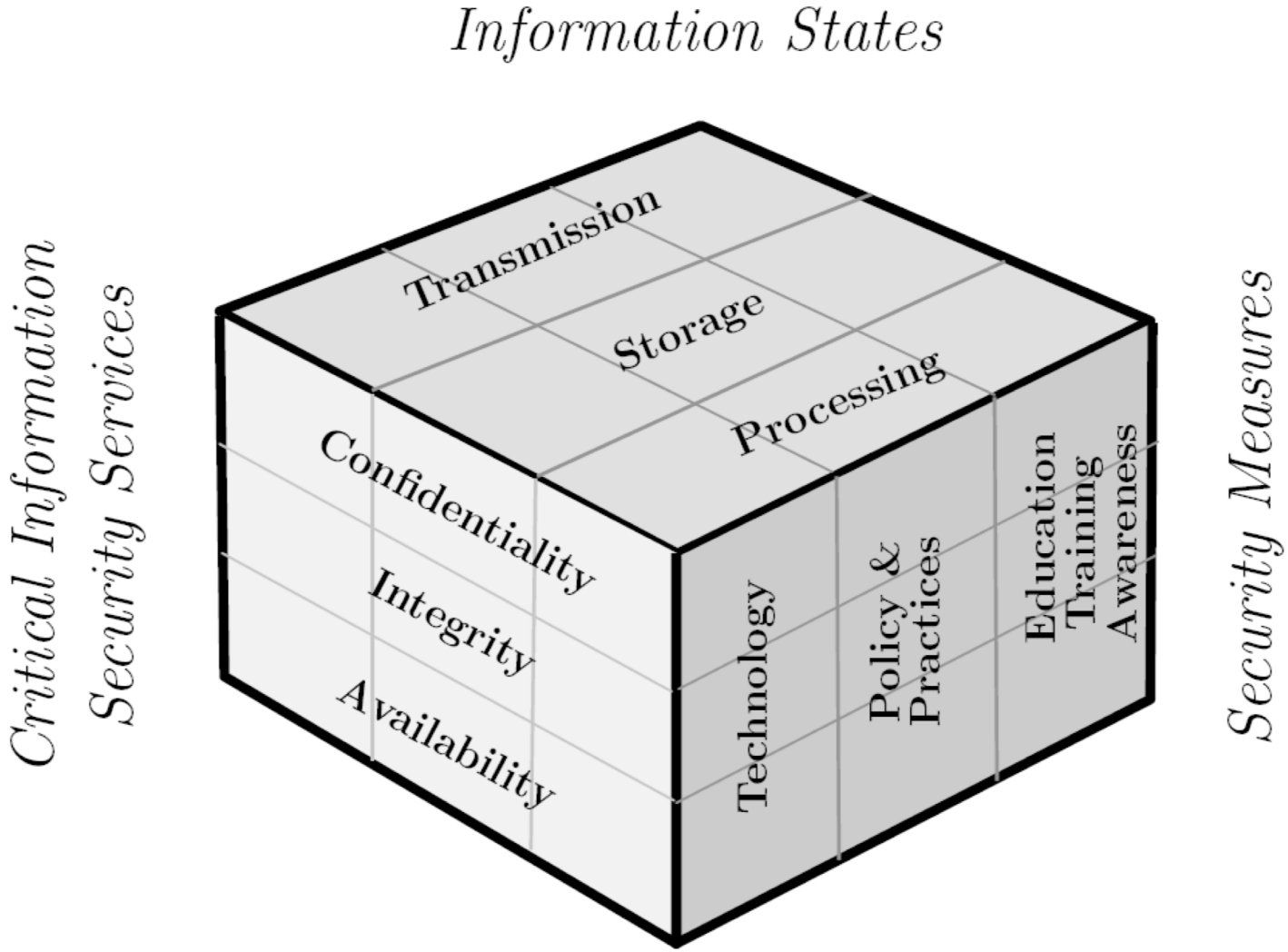
- Use security measures or controls to counter threats and prevent attacks
  - Also known as countermeasures

- **Preventive controls**:
  - prevent attempts to exploit vulnerabilities
    - Example: encryption of files to prevent eavesdropping
- **Detective controls**:
  - warn of attempts to exploit vulnerabilities
    - Example: Use of Checksum/MAC to detect data corruption
- **Corrective controls**:
  - correct errors or irregularities that have been detected
    - Example: Restoring all applications from the last known good image to bring a corrupted system back online

Security Measures or Controls

- **Technology**
  - E.g., Firewalls, encryption, digital signatures, intrusion-detection systems, , tamper-resistant systems, etc.
- **Policy and practice**
  - Plan outlining organisation's approach to managing information security
- **Education, training and awareness**
  - Employee training
    - E.g., against social engineering
  - Remember people are components of the information systems

Useful diagram to combine ideas: NSTISSI 4011 Security Model



NSTISSI 4011 provides a framework for discussing Information Security

Information Security Process

1. Identify information assets
2. Describe security goals for assets
3. Characterize threats
4. Identify vulnerabilities
5. Assess risk
   - Identify
     -> analyze
     -> evaluate risks
6. Apply controls