

Information Assurance and Security

LECTURE 1 : INTRODUCTION TO INFORMATION
SECURITY

Resource Personnel



Kavinga Yapa Abeywardena (Lecturer in Charge)

Lecturer

Department of Computer Systems Engineering

Email: kavinga.y@sliit.lk



Ms. Chethana Liyanapathirana (Co-Lecturer)

Lecturer

Department of Computer Systems Engineering

Email: chethana.l@sliit.lk



Mr. Kanishka Yapa (Co-Lecturer)

Lecturer

Department of Computer Systems Engineering

Email: kanishka.y@sliit.lk

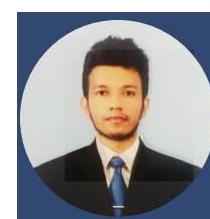


Dr. Harinda Fernando (Co-Lecturer)

Assistant Professor

Department of Computer Systems Engineering

Email: harinda.f@sliit.lk



Mr. Deemantha Siriwardana (Co-Lecturer)

Asst. Lecturer

Department of Computer Systems Engineering

Email: binura.g@sliit.lk

Lecture Delivery

| | | |
|--------------------------------|----------|-------------------|
| Lectures (Face-to-face) | 2 | Hours/Week |
| Tutorials | 1 | Hours/Week |
| Labs | 2 | Hours/Week |

Assessment Criteria

| Continuous Assessments | | | |
|--------------------------------|--------------|---------|--|
| • Midterm Examination | 20 % | L01-L03 | |
| • Assignment | 30 % | LO2-LO4 | |
| End Semester Assessment | | | |
| • Final Examination | 50 % | LO1-LO5 | |
| TOTAL | 100 % | | |

Introduction to Information Security

Objective:

- Describe the formal definition of Computer Security and Information Security
- Describe Confidentiality, Integrity, and Availability as the key security requirements
- Describe the security threats and attacks types

Recommended Texts

W. Stallings and L. Brown, "Computer Security, Principles and Practice, 2nd edition, Pearson, 2012, Chapter 1.

Supplementary text

Charles P. Pfleeger and Shari L. Pfleeger, Security in Computing (3rd edition). Prentice-Hall. 2003. ISBN: 0-13-035548-8.

Computer Security

Definition (NIST Computer Security Handbook)

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Key objectives of Computer Security:

- Confidentiality
- Integrity
- Availability

Information Security (InfoSec)

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

(Source : NIST Glossary of Key Information Security Terms)

Information Assurance (IA)

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

(Source : NIST Glossary of Key Information Security Terms)

CIA Triad



Confidentiality (C)

This term covers two related concepts.

- **Data confidentiality** : Assures that confidential information is not made available or disclosed to unauthorized individuals.
- **Privacy** : Assures that the owners have control on:
 - What information related to them may be collected and stored,
 - By whom and to whom that information may be disclosed.

NIST's Requirement: Preserve authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Loss of confidentiality means unauthorized disclosure of information.

Integrity (I)

This term covers two related concepts.

- **Data integrity:** Information and programs are changed only in a specified and authorized manner.
- **System integrity:** A system performs its intended function in an unimpaired manner, and free from deliberate or inadvertent unauthorized manipulation of the system.

Requirement: Guard against improper information modification or destruction, including ensuring information nonrepudiation authenticity.

Loss of Integrity means unauthorized modification or destruction of information.

Availability (A)

Systems work promptly and service is not denied to authorized users.

NIST's requirement: Ensuring timely and reliable access and use of information.

Loss of Availability means disruption to the authorized users in accessing or use of information.

Additional Objectives

Authenticity: Able to verify that

- the users are who they claim they are, and
- the system receives data from a trusted source.

NIST includes authenticity as part of Integrity

Accountability: Able to trace back the actions performed by an entity to that entity.

Accountability supports: nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, after-action recovery and legal action.

Read the examples of C-I-A in the textbook (Stallings & Brown)

Computer Security Model (RFC 2828)

1) System Resource or asset that needs to be protected

- Hardware: e.g., Computer System, data storage, communication devices.
- Software: e.g., operating systems, program utilities and applications.
- Data: e.g., data and password files, databases.
- Communication facilities and networks: e.g., LAN, WAN, routers, etc.

2) Vulnerabilities of system resources

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

When the resource is corrupted → violate Integrity

When the resource is leaky → violate Confidentiality

When the resource is unavailable → violate Availability

Computer Security Model (cont.)

3) **Threat** is a possible danger that might exploit a vulnerability.

It represents a potential harm to the system resource.

4) **Attack** is a threat that is carried out (threat action)

Two attack types:

- ★ Active attack: An act that has negative effects on system resources
- ★ Passive attack: An act to make use of system information but it does not affect the system

The origin of an attack:

- ★ Inside attack is carried out by an entity inside the security perimeter.
- ★ Outside attack is performed by an unauthorized users.

Computer Security Model (cont.)

5) **Adversary** is an entity that carried out an attack

- A threat agent or an attacker.

6) **Countermeasure** is any means taken to address an attack,

- to prevent an attack from being successful,
- to detect the attack if the attack is successful, and
- to recover from the damage due to the attack.

7) **Risk** is the expected loss due to a particular attack.

- Examples?

Exploits

An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized).

Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack.

- *Used as a verb, exploit refers to the act of successfully making such an attack (make use of a vulnerability).*

Vulnerability Assessment

A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in Information systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.

Penetration Testing

Penetration testing (also called pen testing or ethical hacking) is the practice of testing a Information system, network or web application to find security vulnerabilities that an attacker could exploit. The process involves gathering information about the target before the test, identifying possible entry points, attempting to break in either virtually or for real and reporting back the findings.

Penetration testing can be automated with software applications or performed manually.

Goal of Penetration Testing

- Identify weak spots in an organization's security posture
- Measure the compliance of its security policy
- Test the staff's awareness of security issues
- Determine whether and how the organization would be subject to security disasters.

Passive Attacks

Passive attack is performed by eavesdropping or monitoring data transmission

- The attacker only learns or makes use of information without affecting system resources
- Passive attack is hard to detect because data is not altered
- Use attack prevention (not detection) to handle it

Two types of passive attacks.

- Release of message contents (confidentiality) – Ex: Eavesdropping on Communication Channels
- Traffic analysis, if the data is encrypted.

Active Attacks

Active attacks alters system resources or affecting their operations. Active attack is difficult to prevent but easy to detect

Four categories of active attack:

- Replay. Capture and retransmit data unit to produce an unauthorized effect
- Masquerade. One entity pretends to be another entity
- It usually includes other form of attack, e.g., replay
- Data modification. Alter some portion of legitimate data, delay the data, or reorder the data to produce an unauthorized effect
- Denial of Service. Prevent or disallow the legitimate use of facilities

Inside attacks

Attack vectors can also originate from inside the network. An internal user, such as an employee, can accidentally or intentionally:

- Steal and copy confidential data to removable media, email, messaging software, and other media.
- Compromise internal servers or network infrastructure devices.
- Disconnect a critical network connection and cause a network outage.
- Connect an infected USB drive into a corporate computer system.

Internal threats also have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Employees also have knowledge of the corporate network, its resources, and its confidential data.

Outside attacks

Many attack vectors originate from outside the corporate network. Outside attacks are performed by an unauthorized users.

- For example, attackers may target a network, through the Internet, in an attempt to disrupt network operations and create a denial of service (DoS) attack.

Computer Security Model

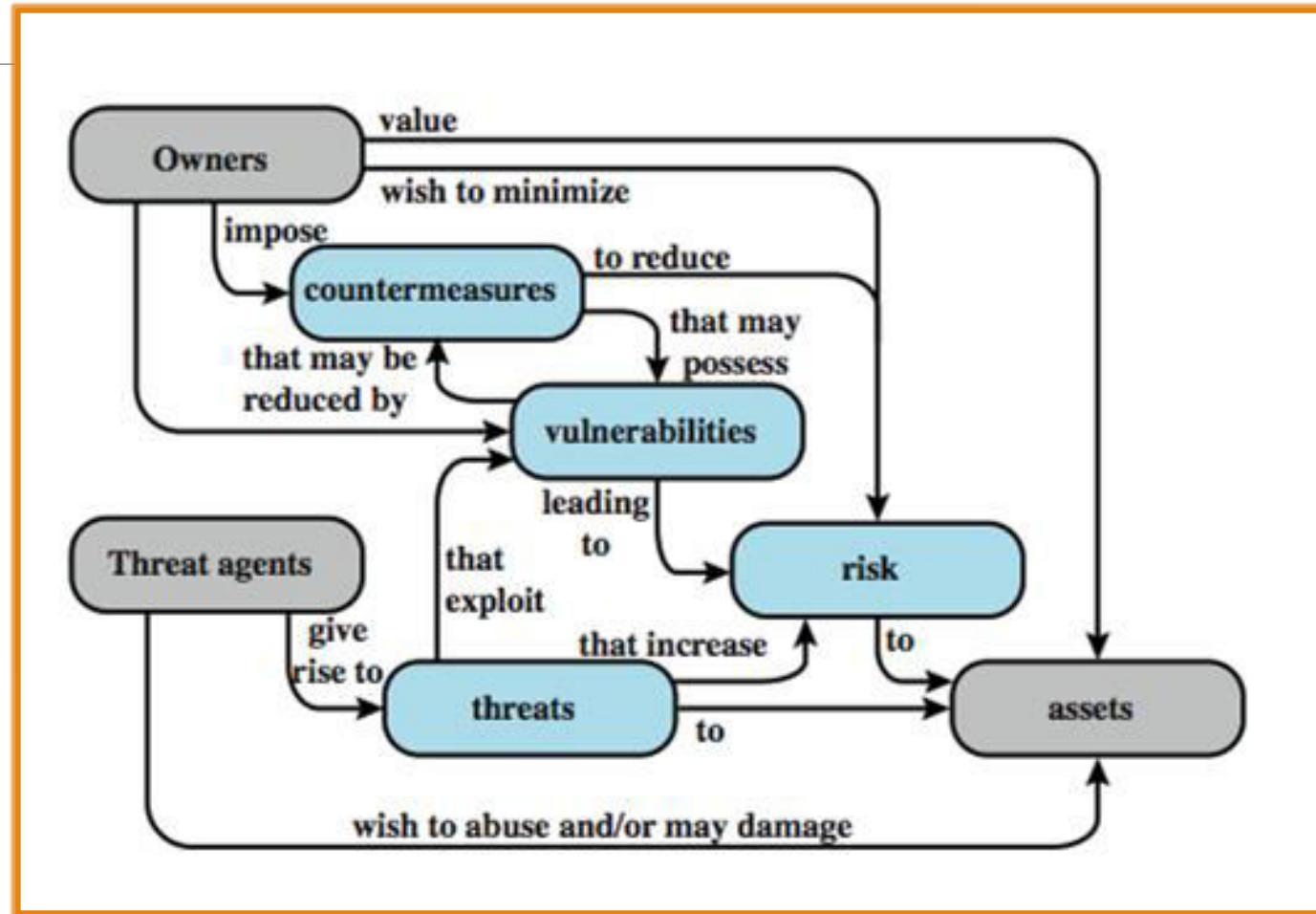
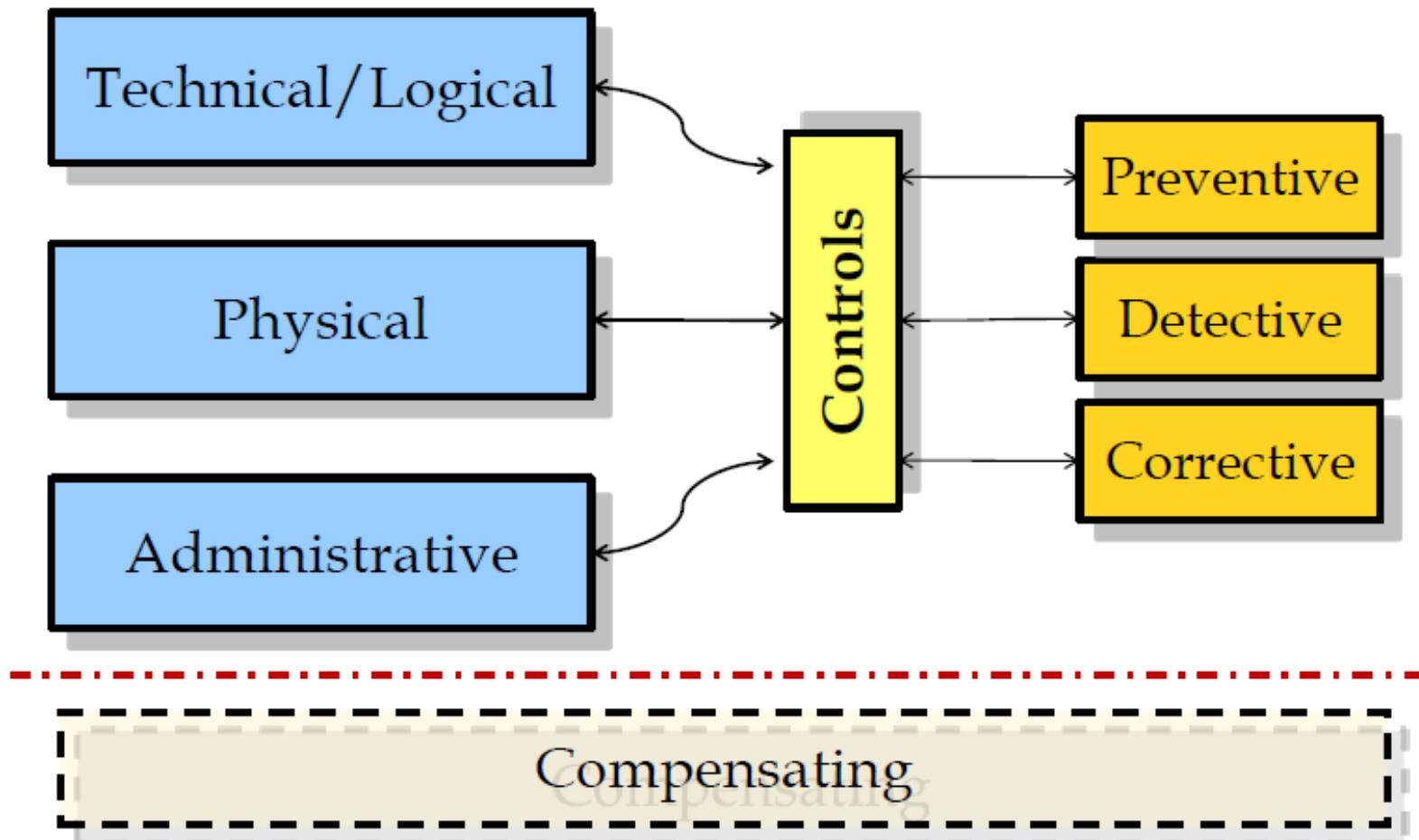


Figure from Stallings & Brown textbook

Information Assurance and Security

LECTURE – 2 : INTRODUCTION TO INFORMATION
SECURITY PART II

Security Controls



Security Controls

Computer/information security controls are often divided into three distinct categories

- Physical controls
- Technical/Logical controls
- Administrative controls

Physical Controls

The Physical control is the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material.

- Surveillance cameras
- Motion or thermal alarm systems
- Security guards
- Picture IDs
- Locked and dead-bolted steel doors
- Network segregation
- Work area separation

Technical Controls

The Technical control uses technology as a basis for controlling the access and usage of sensitive data throughout a physical structure and over a network.

- Encryption
- Smart cards
- Network authentication
- Access control lists (ACLs)
- File integrity auditing software

Administrative Controls

Administrative controls define the human factors of security. It involves all levels of personnel within an organization and determines which users have access to what resources and information by such means as:

- Training and awareness
- Disaster preparedness and recovery plans
- Personnel recruitment and separation strategies
- Personnel registration and accounting
- Policy and procedures

Controls categorized by their functionality

- Preventive Controls
- Detective Controls
- Deterrent Controls
- Corrective Controls
- Recovery Controls
- Compensating Controls

Preventive Controls

Designed to discourage errors or irregularities from occurring. They are proactive controls that help to ensure departmental objectives are being met.

- Separation of duties
- Security of Assets (Preventive and Detective)
- Planning/testing
- Proper hiring practices
- Proper processing of terminations
- Approvals, Authorizations, and Verifications

Detective Controls

Designed to find errors or irregularities after they have occurred.

- Monitoring Systems
- Log reviews
- Bugler Alarm
- File Integrity checkers
- Security reviews and audits
- Performance evaluations

Deterrent Controls

Intended to discourage potential attackers and send the message that it is better not to attack, but even if you decide to attack we are able to defend ourselves.

- Notices of monitoring logging
- Visible practice of sound information security management.

Corrective Controls

Designed to correct the situation after a security violation has occurred. Although a violation occurred, not all is lost, so it makes sense to try and fix the situation.

- Procedure to clean a virus from an infected system
- A guard checking and locking a door left unlocked by a careless employee
- Updating firewall rules to block an attacking IP address

Recovery Controls

Somewhat like corrective controls, but they are applied in more serious situations to recover from security violations and restore information and information processing resources.

- Disaster recovery and business continuity mechanisms
- Backup systems and data
- Emergency key management arrangements and similar controls.

Compensating Controls

Intended to be alternative arrangements for other controls when the original controls have failed or cannot be used.

When a second set of controls addresses the same threats that are addressed by another set of controls, the second set of controls are referred to as compensating controls.

Risk Management

What is risk?

- Life is full of risk. We all manage risk consciously or automatically in life.
- Risk is the possibility of damage happening, and the ramifications of such damage should it occur.

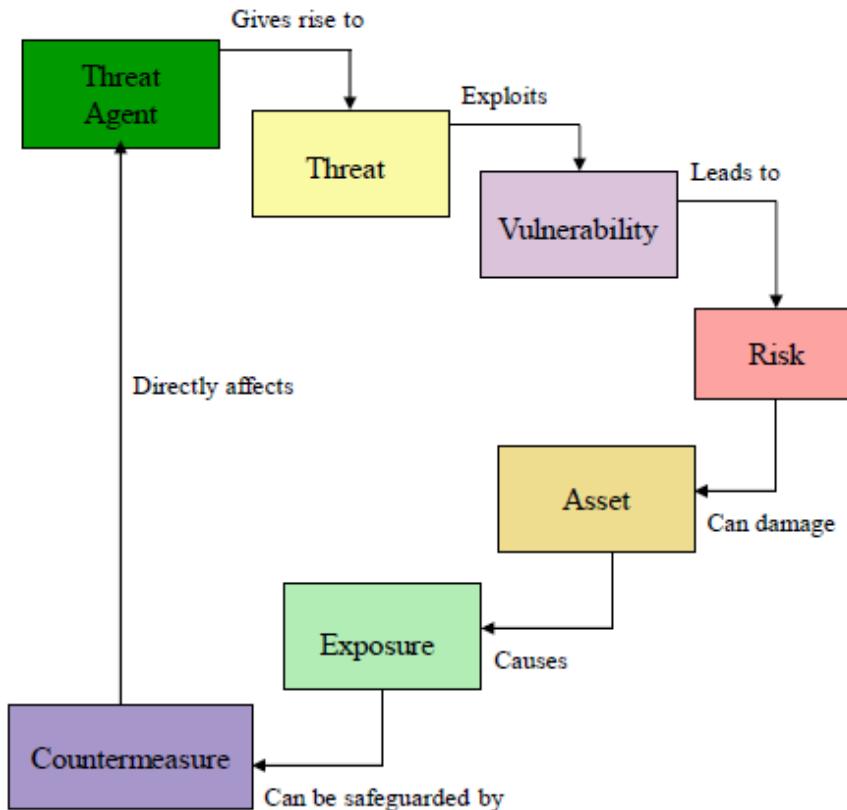
Information Risk Management (IRM) is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level.

- Risk can be mitigated, but cannot be eliminated (which is usually not an option in the commercial world, where controlled (managed) risk enables profits)

Risk Management Terms

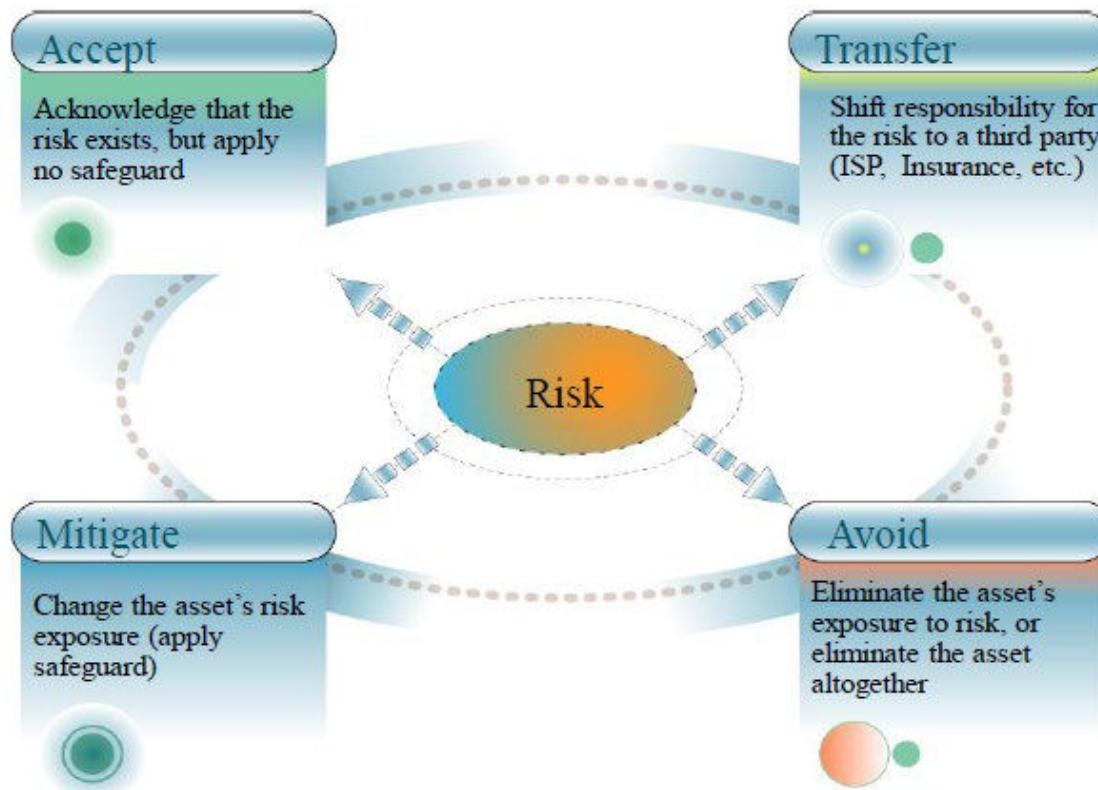
- Vulnerability – a system, network or device weakness
- Threat – potential danger posed by a vulnerability
- Threat agent – the entity that identifies a vulnerability and uses it to attack the victim
- Risk – likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact
- Exposure – potential to experience losses from a threat agent
- Countermeasure – put into place to mitigate the potential risk

Understanding Risk

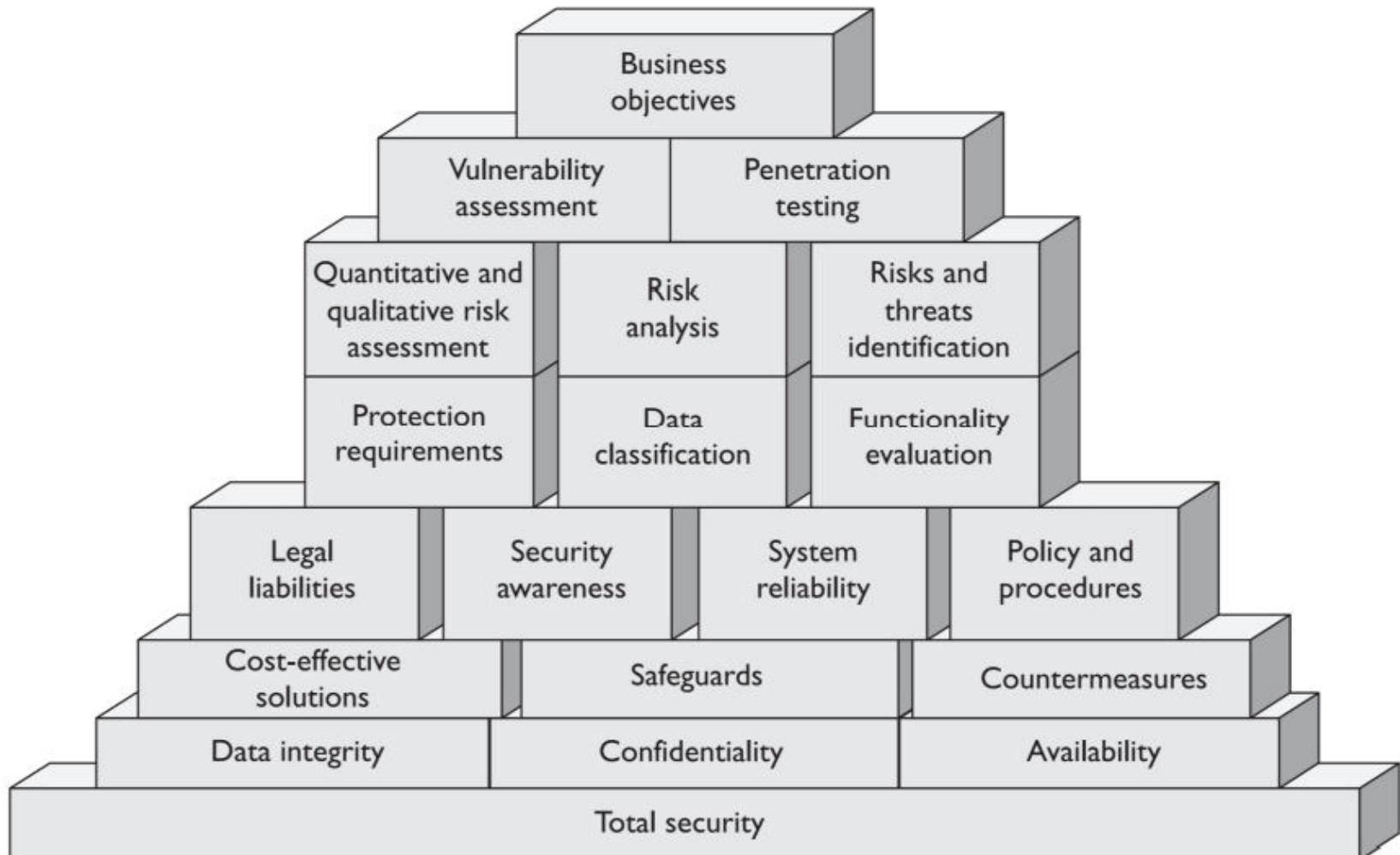


A **threat agent** gives rise to a **threat** that exploits a **vulnerability** and can lead to a **security risk** that can damage your **assets** and cause an **exposure**. This can be counter-measured by a safeguard that directly affects the threat agent.

Managing Risks



Comprehensive Security Model



Data Loss

Data loss or data exfiltration is when data is intentionally or unintentionally lost, stolen, or leaked to the outside world.

Data is likely to be an organization's most valuable asset.

Organizational data can include

- Research and development data
- Sales data
- Financial data
- Human resource and legal data
- Employee data
- Contractor data
- Customer data.

Data Loss can result in:

- Brand damage and loss of reputation
- Loss of competitive advantage
- Loss of customers
- Loss of revenue
- Litigation/legal action resulting in fines and civil penalties
- Significant cost and effort to notify affected parties and recover from the breach

Vectors of Data Loss

- Unencrypted Devices
- Cloud Storage Devices
- Removable Media
- Hard Copy
- Improper Access Control
- Email
- Social Networking

BYOD (Bring Your Own Device)

- **BYOD** is the emerging trend of employees using their personal devices, like smartphones, tablets, laptops etc, to remotely access any organizational network to carry out office work.
- Employees can thus access official mail on their smartphone, connect to office and work using their laptop even while they are traveling and use tablets to be part of conferences that happen at their office when they are away.
- BYOD is important today since employees would want to deliver their best in today's competitive world and companies too would want to make the most of the manpower they have at hand.

BYOD Benefits

- Boosts productivity. Employees can always work by accessing work using their personal devices and they can even check emails and update presentations while on vacation or while traveling back home.
- Employees work with devices that they are more comfortable with and are hence happier when they work in places where BYOD is encouraged.
- The money that needs to be invested on buying hardware, software etc can be utilized for other things even as employees use their own personal devices for work. Thus SMBs can benefit out of BYOD in a very direct manner.
- BYOD helps companies stay abreast of changing technology as employees using personal devices for work would stay up-to-date as regards technology and would use the same for the company as well.

BYOD Drawbacks

- The security threats arise due to the increased number of people who would be accessing a company's data using other devices and also due to the fact that malware could get in through any BYOD device that isn't properly secured.
- Company files and data, which are free to be accessed by employees using their personal devices, could also end up in wrong hands. Such data can be easily seen or stolen by outsiders with malicious intentions.
- BYOD devices might also get stolen or they may get lost, which would also cause data breaches.
- The IT departments in companies where BYOD is practiced would have to undergo tremendous pressure support, managing and securing all BYOD devices.

COPE (corporate-owned, personally enable)

- COPE is a business model in which an organization provides its employees with mobile computing devices and allows the employees to use them as if they were personally-owned notebook computers, tablets or smartphones.
- The COPE model provide the organization with greater power to protect the organization's data both technically and legally.
- Corporate-owned device policies provide several benefits, such as:
 - The ability to actively manage and control if and when a device can access particular apps, sites, services, networks and solutions.
 - The opportunity to wipe a device of any corporate data when an employee loses his or her device or parts ways with the organization.
 - The chance to incorporate controls on the device that determine how applications, networks and IT systems can be utilized remotely, and whether specific information can be retrieved in certain scenarios.

Security measures for COPE/BYOD

Mobile Device Management (MDM) features secure, monitor, and manage mobile devices, including corporate-owned devices and employee-owned devices.

- Data Encryption
- PIN enforcement / Strong Authentication Mechanisms
- Remote Date Wipe of stolen/misplaced devices
- Data Loss Prevention (DLP) options
- Jailbreak/Root detection
- Remotely locating devices
- Security assessments (Vulnerability assessments/ Pen testing/ Audits)

The Hacker

Hacker is a common term used to describe a network attacker.

However, the term “hacker” has a variety of meanings:

- A clever programmer capable of developing new programs and coding changes to existing programs to make them more efficient.
- A network professional that uses sophisticated programming skills to ensure that networks are not vulnerable to attack.
- A person who tries to gain unauthorized access to devices on the Internet.
- Individuals who run programs to prevent or slow network access to a large number of users, or corrupt or wipe out data on servers.

White Hat Hackers

- Ethical Hackers Who use their hacking skills for good, ethical and legal purposes
- May perform Security assessments such as vulnerability assessment penetration tests to discover vulnerabilities.
- Security vulnerabilities are reported to developers for them to fix before the vulnerabilities can be exploited.
- Some organizations award prizes or bounties to white hat hackers when they report vulnerabilities

Gray Hat Hackers

These are the individuals who commit crimes and do arguably unethical things, but not for personal gain or cause serious damage.

Example:

Someone who compromise a system without permission and then disclose the vulnerabilities publically.

However, by publicizing a vulnerability, the gray hat hacker may give other hackers the opportunity to exploit it.

Black Hat Hackers

These are unethical criminals who violate computer and network security for personal gain or for malicious reasons.

Black hat hackers exploit vulnerabilities to compromise computer and network systems.

Modern Hacking Titles

- Script Kiddies
- Vulnerability Brokers
- Cyber Criminals
- Hacktivists
- State-Sponsored Hackers

Script Kiddies

- Inexperienced hackers running existing scripts, tools and exploits developed by skillful hackers to cause harm but typically not for profit.
- It is generally assumed that most script kiddies are juveniles who lack the ability to write sophisticated programs or exploits on their own
- Their objective is to try to impress their friends or gain credit in computer-enthusiast communities.
- However, the term does not relate to the actual age of the participant.

Vulnerability Brokers

They are usually gray hat hackers who attempt to discover exploits and report them to vendors, sometime for prize or rewards.

Cyber Criminals

- Cyber criminals are black hat hackers with the motive to make money using any means necessary.
- Self employed (working independently) or working for criminal organizations.
- It is estimated that globally, cyber criminals steal billions of dollars from consumers and businesses.
- Cyber criminals operate in an underground economy where they buy, sell, and trade attack toolkits, zero day exploit code, botnet services, banking Trojans, keyloggers, and much more.
- They also buy and sell the private information and intellectual property they steal from victims.
- Cyber criminals target small businesses and consumers, as well as large enterprises and industry verticals.

Hacktivists

- Grey hat hackers who rally and protest against different social and political ideas.
- Hacktivists do not hack for profit, they hack for attention.
- Hacktivists publically protest against organization or governments by posting articles, videos. Leaking sensitive information and performing distributed denial of service attacks.

Examples of hacktivist groups

- Anonymous Hackers
- Syrian Electronic Army.

State-Sponsored Hackers

- These are government-funded and guided attackers.
- State-sponsored hackers create advanced and customized attack code, often using previously undiscovered software vulnerabilities, Steal government secrets , gather intelligence and sabotage networks and systems.
- Their targets are foreign governments, terrorist groups and corporations.
- Most countries in the world participate to some degree in state-sponsored hacking.
- Nations hire the best talent to create the most advanced and stealthy threats.
- **An example :** Stuxnet malware that was created to damage Iran's nuclear enrichment capabilities.

Information Risk Management: GRC & COBIT

By Kavinga Yapa Abeywardena

Sri Lanka Institute of Information Technology (SLIIT)



Governance, Risk Management, Compliance (GRG)

- An ‘umbrella term’ that covers these three areas of enterprise activities (Not just IT)
- Constantly reviewed and analysed to enhance the organisations performances and efficient delivery of stakeholder needs.
- GRC activities are typically based on principles, policies, models, frameworks, organisational structures. Etc.

Governance, Risk Management, Compliance (GRC)

- **Governance:** Exercise of authority; control; government; arrangement.
- **Risk (management):** Hazard; danger; peril; exposure to loss, injury, or destruction (The act or art of managing; the manner of treating, directing, carrying on, or using, for a purpose; conduct; administration; guidance; control)
- **Compliance:** The act of complying; a yielding; as to a desire, demand, or proposal; concession; submission

Governance, Risk Management, Compliance (GRC)

Simpler Definitions

- **Governance:** Effective management of a company by executives & senior management
- **Risk (management):** Ability to effectively mitigate risks that deter company's success
- **Compliance:** Abiding by rules, regulations, laws and industrial ethics & standards

Governance, Risk Management, Compliance (GRC)

- Different types of GRC
 - Corporate GRC
 - Project GRC
 - Information Technology GRC
 - Environmental GRC
 - Economic and financial GRC

IT GRC

- **IT Governance:** Establishes decision structures and tracking mechanisms.
- **IT Risk Management:** Helps mitigate adverse effects and identifies opportunities.
- **IT Compliance:** Ensure that an organization is not only adhering to laws and regulations, but is also taking into account corporate responsibilities and industry standards.

What's New in IT GRC ?

- IT GRC initiatives have traditionally been scattered across organizations without any coordination or synchronization.
- Need a unified approach for better results and efficiency. ‘Holistic Approach’ is the buzz word used in the industry.
- High demand for products that help organizations effectively break down scattered initiatives & create a centralized approach to managing **RISK** and **COMPLIANCE** while simultaneously ensuring good **GOVERNANCE**.

COBIT for IT GRC

- COBIT is a framework that guides IT professionals and enterprise leaders to fulfill their IT governance responsibilities while delivering value to the business.
- Developed and maintained by ISACA (Information Systems Audit and Control Association), COBIT 5 is the latest version.



AUDIT & ASSURANCE

Manage vulnerabilities and ensure compliance.



RISK MANAGEMENT

Evaluate and optimize enterprise risk.



INFORMATION SECURITY

Oversee and manage information security.



REGULATORY & COMPLIANCE

Keep ahead of rapidly changing regulations.



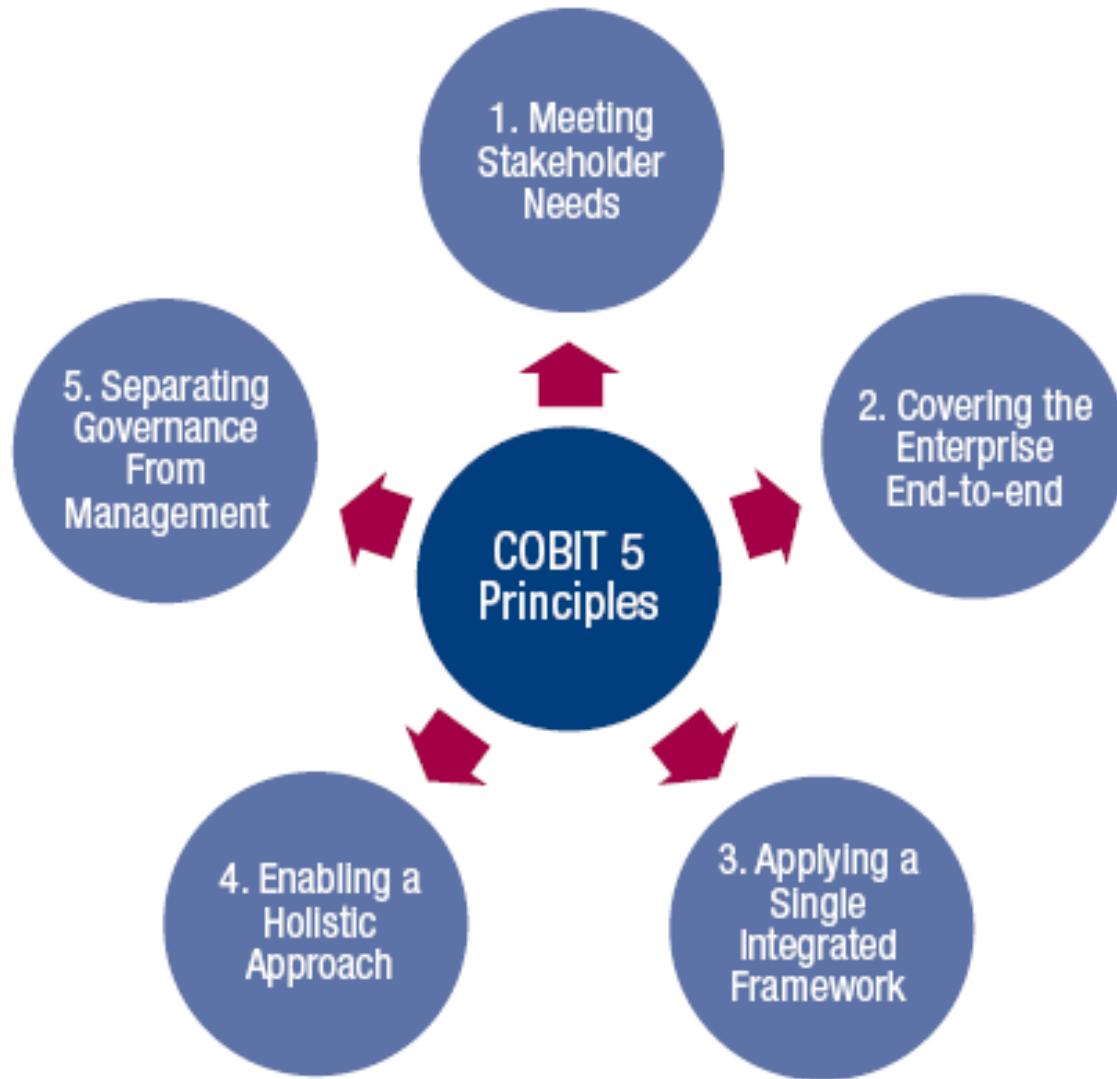
GOVERNANCE OF ENTERPRISE IT

Align IT goals and strategic business objectives.

The COBIT 5 Framework

- Helps enterprises to create optimal value from IT by maintaining a **balance between realising benefits and optimising risk levels** and resource use.
- Enables **IT to be governed and managed in a holistic manner** for the entire enterprise, taking in the full end-to-end business and functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.
- The **COBIT 5 principles** and **enablers** are generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

COBIT 5 Principles



Source: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved.

Meeting Stakeholder Needs

Principle 1. Meeting Stakeholder Needs:

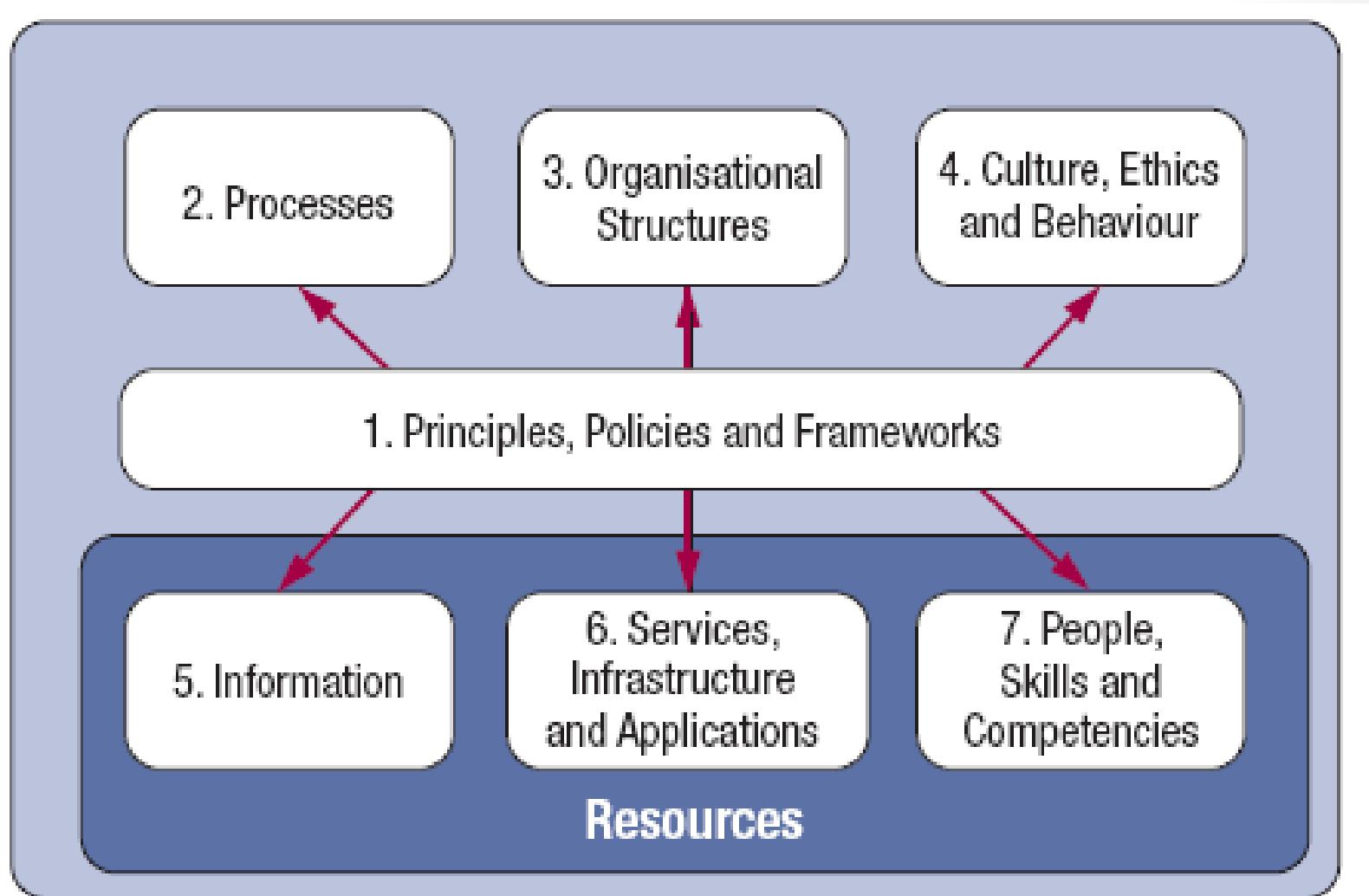
- Enterprises have **many** stakeholders, and ‘creating value’ means different—and sometimes conflicting—things to each of them.
- Governance is about negotiating and deciding amongst different stakeholders’ value interests.
- The governance system should consider all stakeholders when making benefit, resource and risk assessment decisions.
- For each decision, the following can and should be asked:
 - Who receives the benefits?
 - Who bears the risk?
 - What resources are required?

1. Meeting Stakeholder Needs



- Stakeholder needs transformed into an actionable enterprise strategy.
- The COBIT 5 '**goals cascade**' translates stakeholder needs into specific, practical and customised goals within the context of the enterprise, IT-related goals and enabler goals.

COBIT 5 Enablers



Source: COBIT® 5, figure 12. © 2012 ISACA® All rights reserved.

QUESTIONS ?



Thank
You



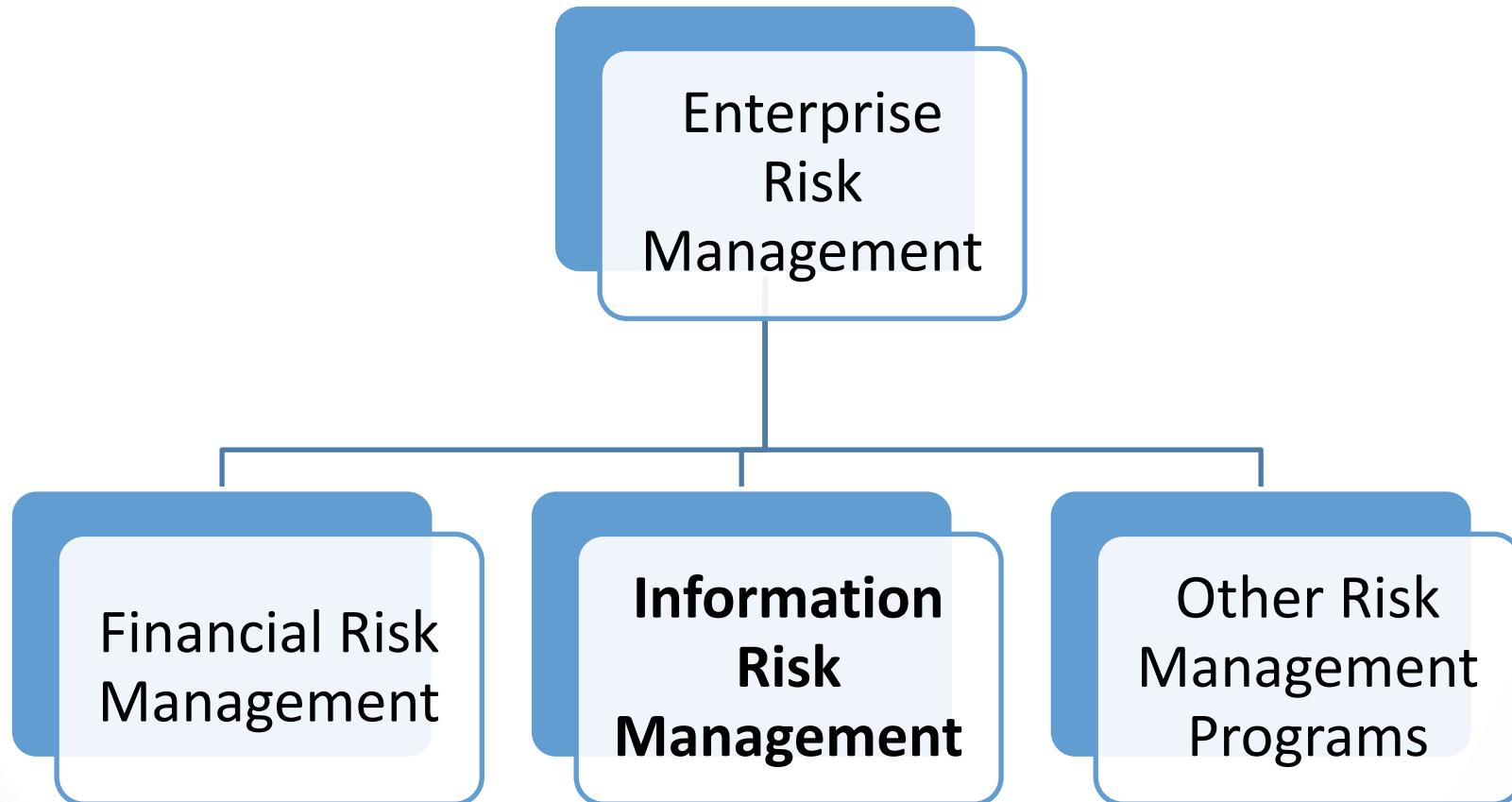
Information Risk Management: An Introduction

By Kavinga Yapa Abeywardena

Sri Lanka Institute of Information Technology (SLIIT)

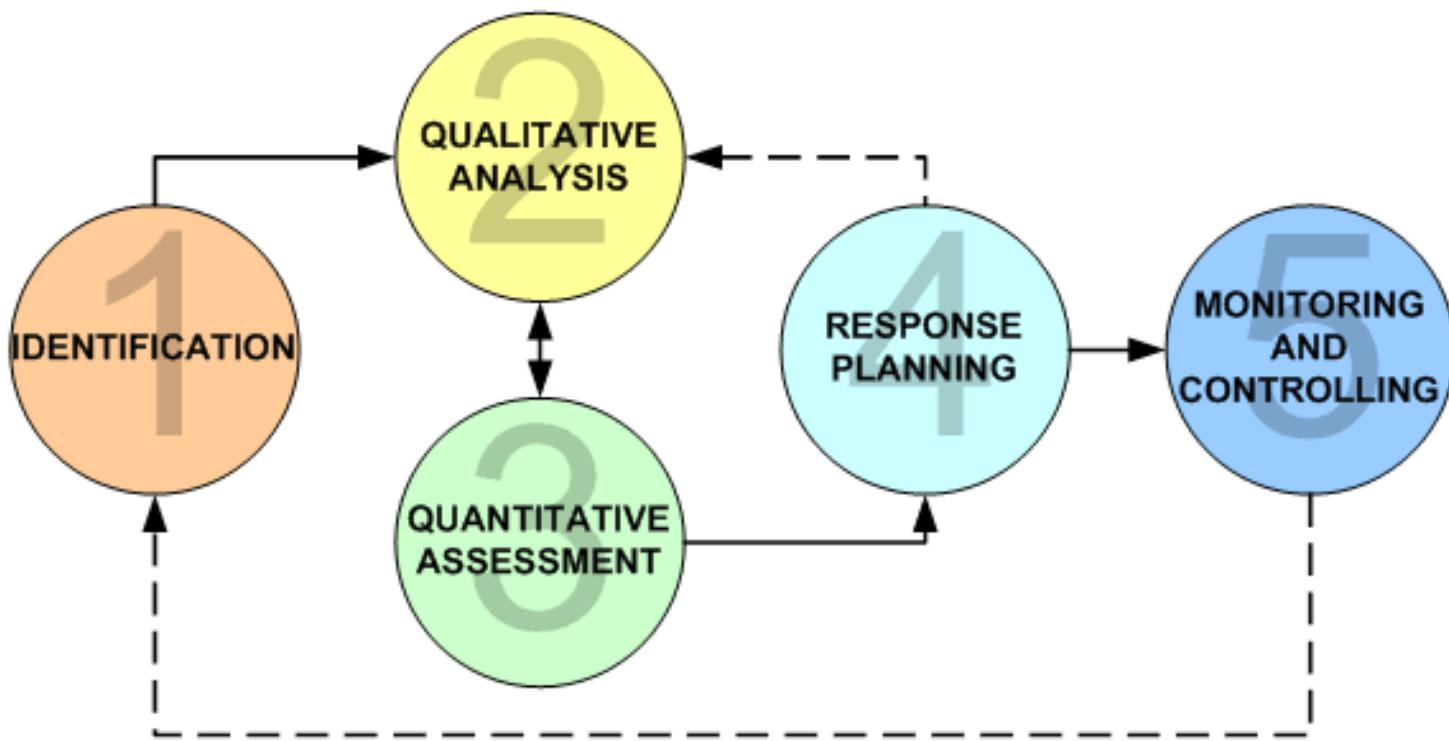


THE BIG PICTURE



Risk Management Process

5-step Risk Management Approach



Risk Management Process

Step 1 : Risk Identification

- Consider internal & external factors
- Use expert knowledge (Penetration Testing?)
- Involve every department
- Creativity & Imagination is the KEY!
- Risk identification and review is an ongoing process throughout the project's lifetime.

Risk Management Process

Step 2 : Qualitative Analysis

- Identifies the most critical risks and focus the attention
- Impact rating depend on company's business goals & objectives
 - Reputation/customer confidence
 - Life/health of customer
 - Fines/Legal penalties
 - Financial
 - Other

Risk Management Process

Step 2 : Qualitative Analysis

- Use expert knowledge & judgment
- Probability of an event occurring identified
- Risk = Impact x Probability
- Example Case Study:
 - <https://www.dropbox.com/s/k0i1d104ihfi5go/LCS%20-%20IT%20Security%20Report.pdf?dl=0>
- Discussion!

Risk Management Process

Step 2 : Qualitative Analysis (Example)

| PROBABILITY | | |
|-------------------|---------------|------------------------------|
| Qualitative Scale | Numeric Scale | Description |
| Very Low | 1 | Unlikely to occur |
| Low | 4 | May occur occasionally |
| Medium/Moderate | 6 | Is as likely as not to occur |
| High | 8 | Is likely to occur |
| Very High | 10 | Is almost certain to occur |

Risk Management Process

Step 2 : Qualitative Analysis (Example)

| IMPACT | | |
|-------------------|---------------|---|
| Qualitative Scale | Numeric Scale | Description |
| Very Low | 1 | Negligible impact |
| Low | 2 | Minor impact on time, cost or quality |
| Medium/Moderate | 4 | Notable impact on time, cost or quality |
| High | 8 | Substantial impact on time, cost or quality |
| Very High | 16 | Threatens the success of the company |

Risk Management Process

| IMPACT | COST | TIME | QUALITY |
|-----------|---|---|---|
| Very low | Manageable by fund transfer from another sector | Slight slippage against internal targets | Slight reduction in quality/scope with no overall impact on usability/standards |
| Low | Additional Funding required | Slight slippage against key milestones or published targets | Failure to include certain 'nice to have' elements promised to stakeholders |
| Moderate | Significant additional Funding required | Delay affects key stakeholders and causes loss of confidence in the project | Significant elements of scope or functionality will be unavailable |
| High | Significant reallocation of owner's funds (or borrowing) required to achieve business goals | Failure to meet key deadlines in relation to the strategic plan | Failure to meet the needs of a large proportion of stakeholders |
| Very high | Threaten the existence of the business (Can be beyond recovery) | Delay jeopardizes the existence of the business | Products or services become effectively unusable |

Risk Management Process

Step 2 : Qualitative Analysis (Example)

| Risk | Probability | Impact | Rating |
|------|-------------|--------|--------|
| A | 4 | 8 | 32 |
| B | 6 | 2 | 12 |
| C | 1 | 16 | 16 |

Risks sorted according to rating : A > C > B

Proximity: Immediate nature of the risk to be taken into consideration. How to incorporate?

Risk Management Process

Step 3 : Quantitative Analysis

- Qualitative analysis is only useful as long as the management agrees on ratings & what they actually mean. (E.g. What is a rating of 16? in \$?)
- In order to analyse risks in a meaningful way it is necessary to define the impacts in relation to company's business goals.
- What's the difference of 'very low' & 'moderate' ?

Quantitative Risk Analysis

- So far we have focused on ‘Qualitative Risk Analysis’.
- We have noticed that Qualitative methods are scenario based.
- ‘**Quantitative Risk Analysis**’ attempts to assign independent monetary values to system components.
- Quantitative methods tend to be more resource consuming, however they come with few distinct **advantages** over qualitative methods.

Quantitative Risk Analysis: Key Variables

- **Exposure Factor (EF)** = Percentage of asset loss caused by identified threat (0-100%)
 - **Single Loss Expectancy (SLE)** = Asset Value x EF
 - e.g. Rs. 50,000 x 20% = Rs. 10,000
 - **Annualized Rate of Occurrence (ARO)** = Frequency a threat will occur within a year
 - **Annualized Loss Expectancy (ALE)** = SLE x ARO
- **Safeguard Cost/Benefit** = ALE before Safeguard - ALE After Safeguard - Annual Cost of Safeguard

Determining Asset Values [2]

- **Tangible Assets**
 - Ask the **IT manager** for cost information regarding existing equipment, hardware & software
 - Internet **research** on exact or comparable systems
 - Look at **previous projects**, adjust according to depreciation
 - Overall **replacement cost** due to failure (installation, troubleshooting, 10% for contingency, temporary loss of services)
- **Intangible Assets**
 - Measure asset's fair market value (depreciation!) e.g. Trade Secrets
 - Focus on the income producing capability of the intangible asset
 - Involve senior management to conduct final valuation

Risk Management Process

Step 4 : Response Planning

- Individual risks to be treated according to the impact rating from previous analysis
- Different responses for different risks
- All responses carry a cost (time, money & labor)
- Use expert knowledge & judgment
- Involve company's stakeholders

Risk Management Process

Step 4 : Response Planning: Standard Levels of Response

| RESPONSE | DESCRIPTION |
|----------|--|
| Avoid | Risk Removal and Risk Prevention. Altering the plan so that the circumstances which may give rise to the risk no longer exist. |
| Mitigate | Risk Reduction. Reducing the probability or impact of the risk. |
| Transfer | Moving the impact (and ownership) of the risk to a third party. |
| Defer | Deferring aspects of the plan to a date when the risk is less likely to occur. |
| Accept | Dealing with the risk via contingency rather than altering the plan. |

Risk Management Process

Step 5 : Monitor & Control Risks

- Keep track of the identified risks, monitor the **effectiveness** of risk responses
- Identify new or changed risks (Back to Step 2 - 4)
- A regular review & updating process is required
- Communication with all the stakeholders
- Phase out or release of contingency responses if risks no longer exist

Risk Management Methodologies

- There are variety of methodologies available for Information Risk Management. Some are well documented, others not so much.
- We will specifically look at **OCTAVE / OCTAVE-Allegro**
- **Next Lecture!**

QUESTIONS ?



Thank
You



OCTAVE

Risk Evaluation

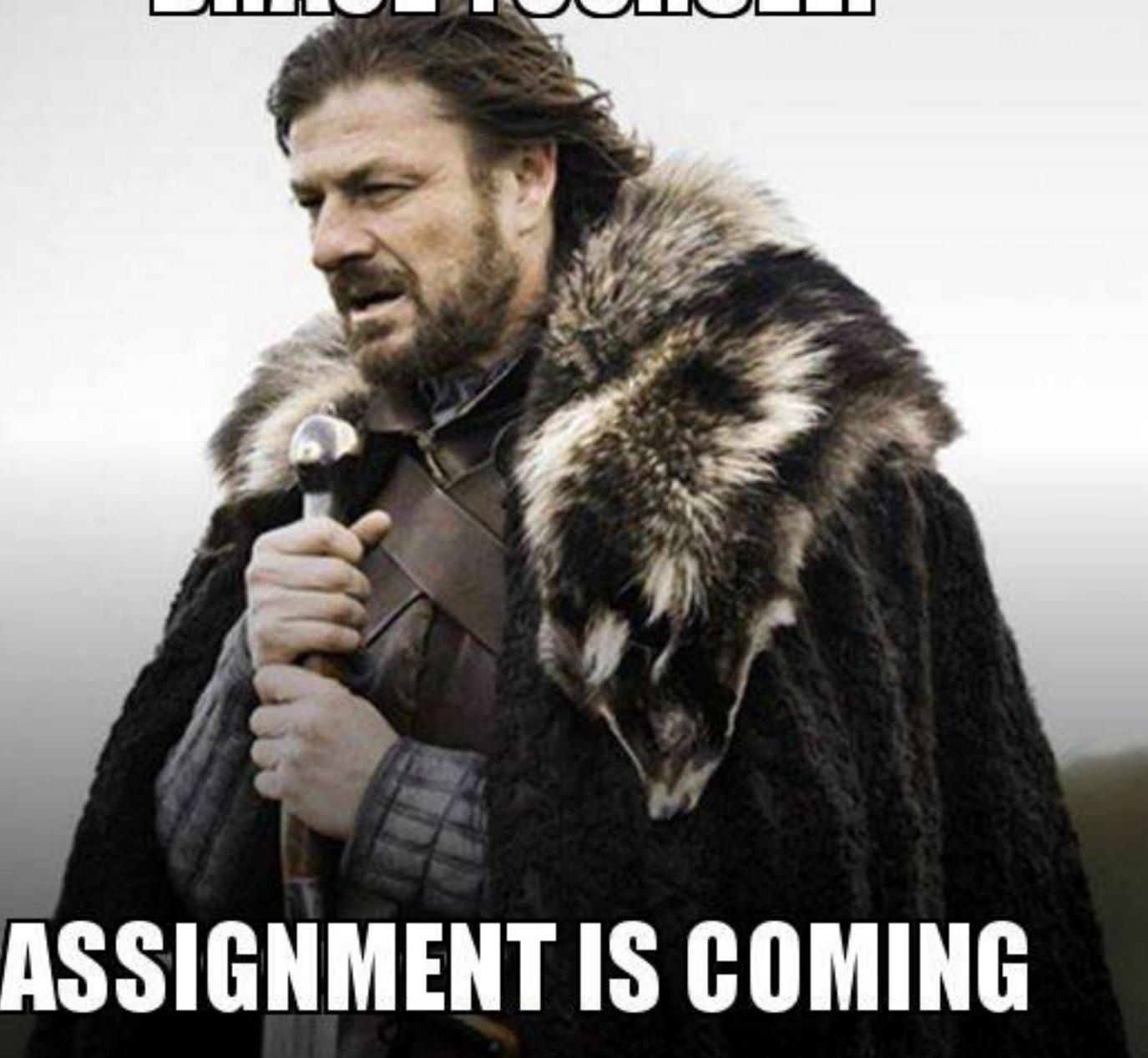
Framework

By Kavinga Yapa Abeywardena

Sri Lanka Institute of Information Technology (SLIIT)



BRACE YOURSELF

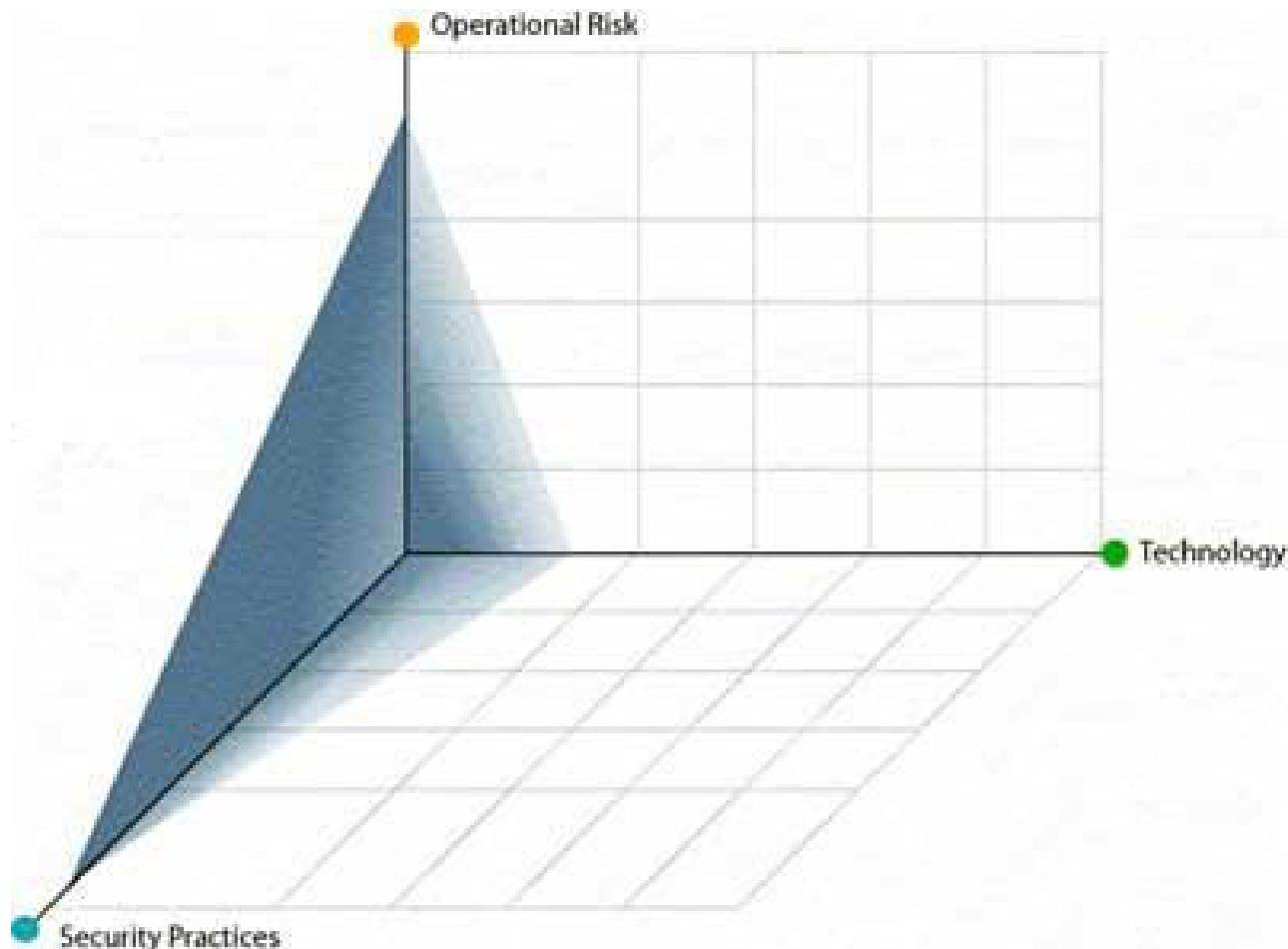


ASSIGNMENT IS COMING

Operationally Critical Threat Asset & Vulnerability Evaluation

- OCTAVE is a methodology for identifying and evaluating information security risks to an asset
- Set of tools, techniques and methods for risk-based information security strategic assessment and planning.
- Developed by Christopher Alberts; a scientist at Carnegie Mellon University (CMU)

OCTAVE - Big Picture



Not Technology Focused!

OCTAVE – Big Picture

- **Philosophy/Vision**

- Focuses on strategy
- Take into account the organization's needs

- **Risk Assessment:**

- Top-down approach
- Threat-per-asset based
- Qualitative approach

- **Implementation:**

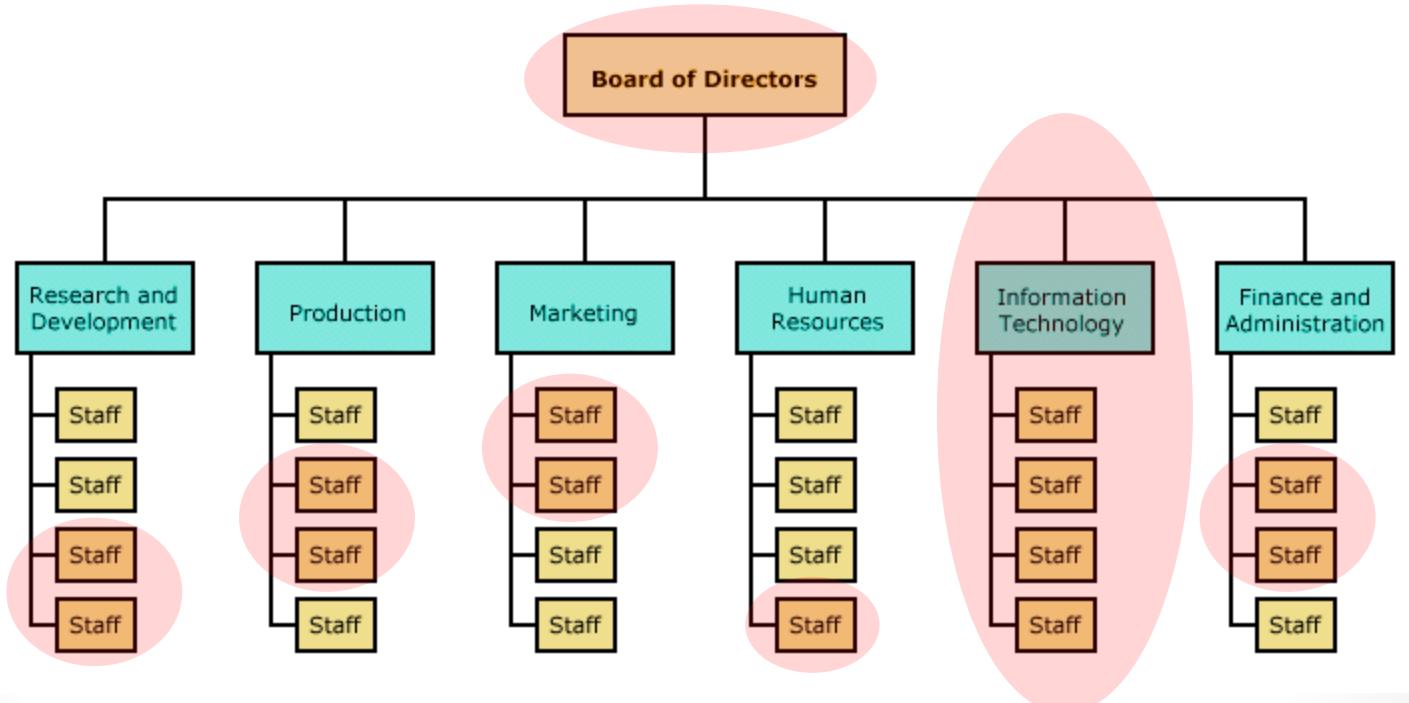
- Process-driven
- Flexible: Can be customized
- Self-directed: led by organization's employee

OCTAVE – What's Different ?

| OCTAVE | Other Frameworks |
|------------------------------|-------------------------|
| Strategic Focus | Tactical Focus |
| Focus on Security Practices | Focus on Technology |
| Organization-wide evaluation | System based evaluation |
| Self Directed | Expert led |
| Top - Down | Bottom - Up |

OCTAVE – Team

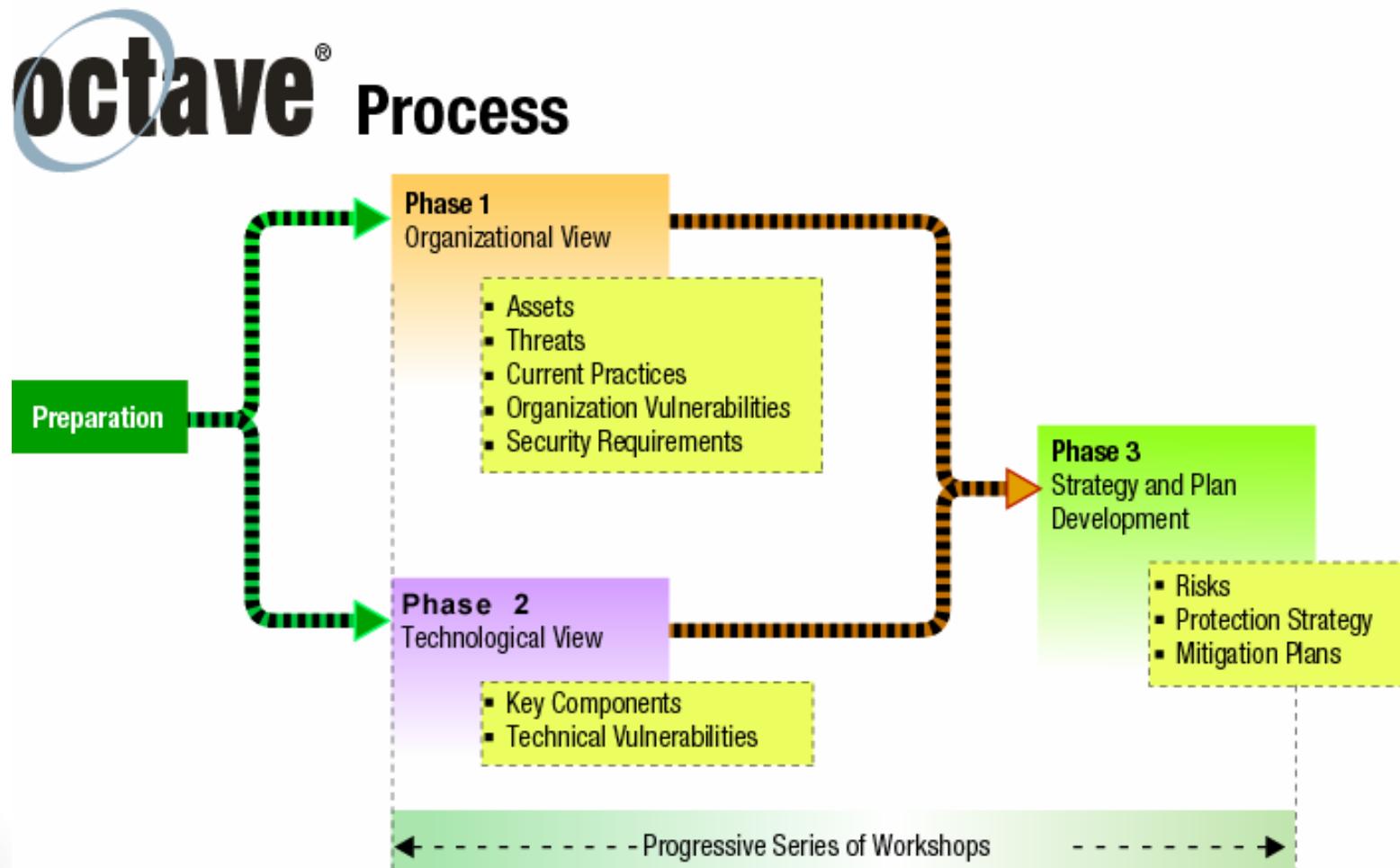
- **Consists of:**
 - Operational (Business) units
 - IT department



OCTAVE – Functionality

- **Functionality:**
 - Identify critical assets that are important to the organization
 - Focus risk analysis on the most important organizational assets
 - Consider:
 - Relationship between critical assets
 - Threats to assets
 - Vulnerabilities that can expose assets to threats
 - Evaluate risks in an operational context
 - Create practice-based protection strategy and risk mitigation plans to reduce risk

OCTAVE Phases - Overview



OCTAVE Phases - Overview

- Uses three-phase approach to examine organisational and technology issues
- Three Phases of OCTAVE
 - Phase 1: Build **Asset-Based Threat Profiles**
 - Phase 2: Identify Infrastructure **Vulnerabilities**
 - Phase 3: Develop **Security Strategy** and Plan
- Three phases are a composition of sub processes with each achieving a specific objective
- We will examine few important sub processes!

OCTAVE Phases & Processes

- Phase 1: Build asset-based **threat profiles**
 - Process 1: Determine **critical assets** and how they are currently protected
 - Process 2: Identify **security requirements** for each critical asset.
 - Process 3: Identify organisational **vulnerabilities** within **existing** practices
 - Process 4: Create **threat profile** for each critical asset
- Phase 2: Identify infrastructure **vulnerabilities**
 - Process 5: Identify network **access paths** and **IT components** related to critical assets
 - Process 6: **Evaluate** identified IT components
- Phase 3: Develop **security strategy** and mitigation plans
 - Process 7: Conduct **risk analysis**
 - Process 8: Develop protection **strategy and mitigation plan**

Process 4 : Threat Profile

A threat profile has the following characteristics:

- **Asset**
- **Access:** how the asset will be accessed by the actor:
network or physical access (Optional)
- **Actor:** a person or natural occurrence with an undesirable outcome
- **Motive:** Actor's intentions: deliberate or accidental
(Optional)
- **Outcome:** the immediate outcome of violating the security requirements of an asset
 - **Disclosure:** unauthorized access to asset
 - **Modification:** tampering with an asset
 - **Interruption** (loss/destruction): Unavailability of an asset
 - **Fabrication** (other): Creation of new objects in a system

Process 4 : Threat Profile

Example: SLIIT student records in the ‘S01’ server has been identified as a critical assets by Process 1.

| Area of Concern | Threat Profile |
|--|--|
| People are accidentally entering the wrong data into system S01. This results in incorrect records on that system. | <ul style="list-style-type: none">· Asset – system S01 records· Access – network (The data are entered into records on a system.)· Actor – insiders (The concern implies staff with legitimate access.)· Motive – accidental· Outcome – modification (Inconsistent data) |
| Someone could use the records from system S01 for personal gain. | <ul style="list-style-type: none">· Asset – system S01 records· Access – network (The actor gets the records from the system.)· Actor – insiders and outsiders (implies staff with legitimate access as well as outsiders.)· Motive – deliberate· Outcome – disclosure (The actor is viewing information that he/she shouldn’t be viewing.) |

Phase 3: Risk Analysis & Security Strategy/Mitigation

- Information generated by Phases 1 and 2 are analysed to:
 - **Identify risks** to critical assets - prioritize
 - Develop **protection strategies**
 - Develop **mitigation plans**
 - Propose **next steps**
 - Senior **Management approval**
- Process 7(Risk Analysis) plays a major role. You already know how to do this!

Process 7 : Risk Analysis

- Identify & evaluate the impact of threats to critical assets
- This will form Risk Profiles: Threat profile + description of impact + impact values + Probability values
- Based on the following evaluation criteria:
 - Only focuses on **important and relevant risks**
 - **Qualitative** impact values/measures: high, medium and low
 - **Impact Areas:**
 - Reputation/customer confidence
 - Life/health of customer
 - Fines/Legal penalties
 - Financial
 - Other

OCTAVE Variants

- OCTAVE
 - large organizations \geq 300 employees
- OCTAVE-S
 - organizations \leq 300 employees
- OCTAVE-Allegro
 - Focuses on information assets

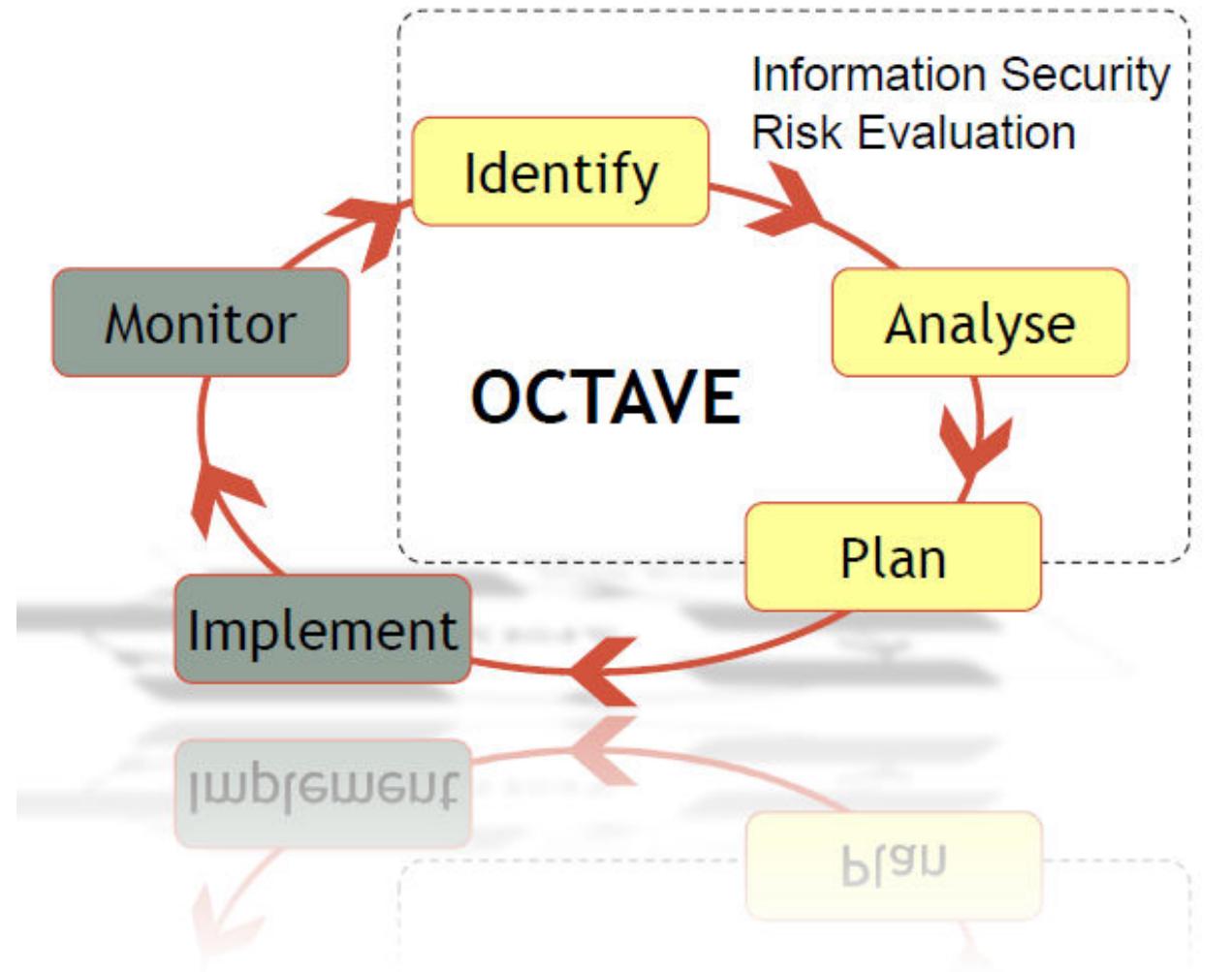
OCTAVE-S

- Developed in 2003 to cater smaller organization
- Includes a limited exploration of the computing infrastructure during Phase 2
- Requires:
 - Small organisation with a simple hierarchical structure
 - Small interdisciplinary analysis team (3-5 employees)
 - Understanding of organization's business & security processes

OCTAVE-S Deliverables

- **Organization-wide protection strategy** – strategy outlines direction with respect to information security practice
- **Risk mitigation plans** – are intended to mitigate risks to critical assets by improving selected security practices
- **Action list** – includes short-term action items needed to address specific weaknesses
- A listing of important **information-related assets** supporting the organization's business goals and objectives
- Survey results showing the extent to which the organization is following **good security practice**
- **A risk profile** for each critical asset depicting a range of risks to that asset

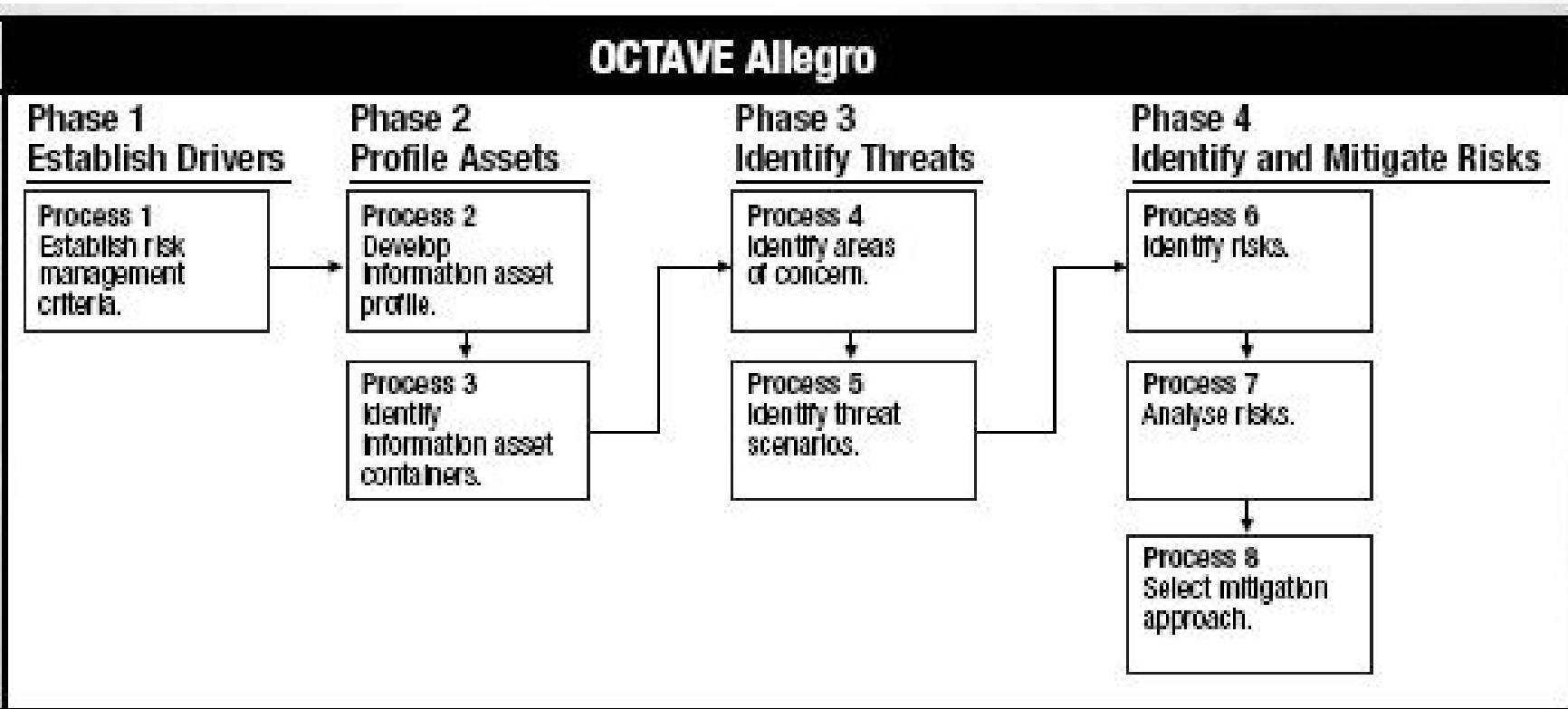
OCTAVE-S Scope



OCTAVE-Allegro

- Developed in 2007
- Unlike previous OCTAVE approaches, it focuses on information assets (e.g. data, hardware and software)
 - How they are used
 - Where they are stored, transported, and processed
 - How they are exposed to threats, vulnerabilities, and disruptions as a result
- Suitable to perform risk assessment without extensive organizational involvement , expertise, or input.

OCTAVE-Allegro



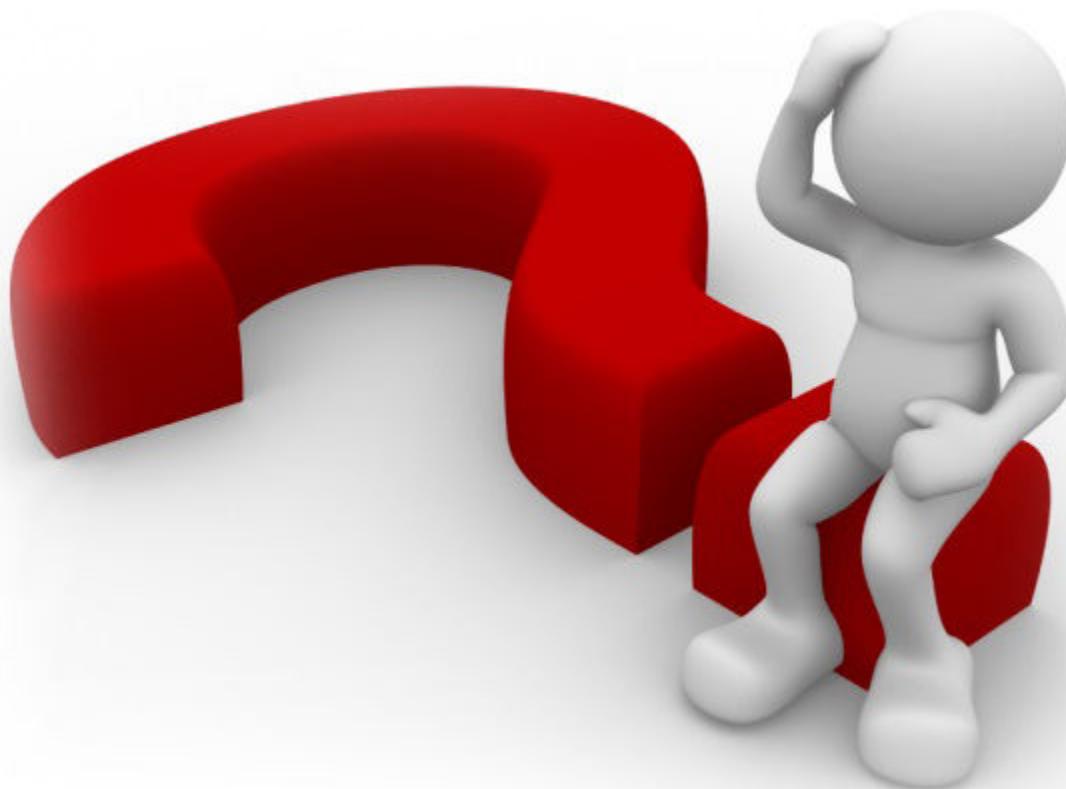
OCTAVE-Allegro Pros & Cons

- **Pros:**
 - Well-documented through published academic papers
 - Flexible: Organisations choose to implement portions that they find appropriate for them
 - Comprehensive
 - Focuses on important and relevant risks
 - Cheap: it is self-led
- **Cons:**
 - Needs extensive preparation
 - Complexity – exhausting processes
 - Qualitative methodology– OCTAVE does not allow organizations to mathematically model risks
 - Risk Analysis is done on a single asset– slower results which affects organizations
 - Difficult to capture futuristic threats & risks

OCTAVE – Discussion

- Flexible
- OCTAVE provides organizations an option to only choose required parts from the framework. On one hand, this might be good in terms of reducing cost, time and effort while on the other hand, some misinterpreted required parts might be missed!
- Risk analysis is performed using internal staff – not suitable for organizations interested in expertise more than lower cost
- Uses no mathematical calculations
- Uses Expected Value Matrix to determine a risk's expected value
- Values simplicity over accuracy

QUESTIONS ?



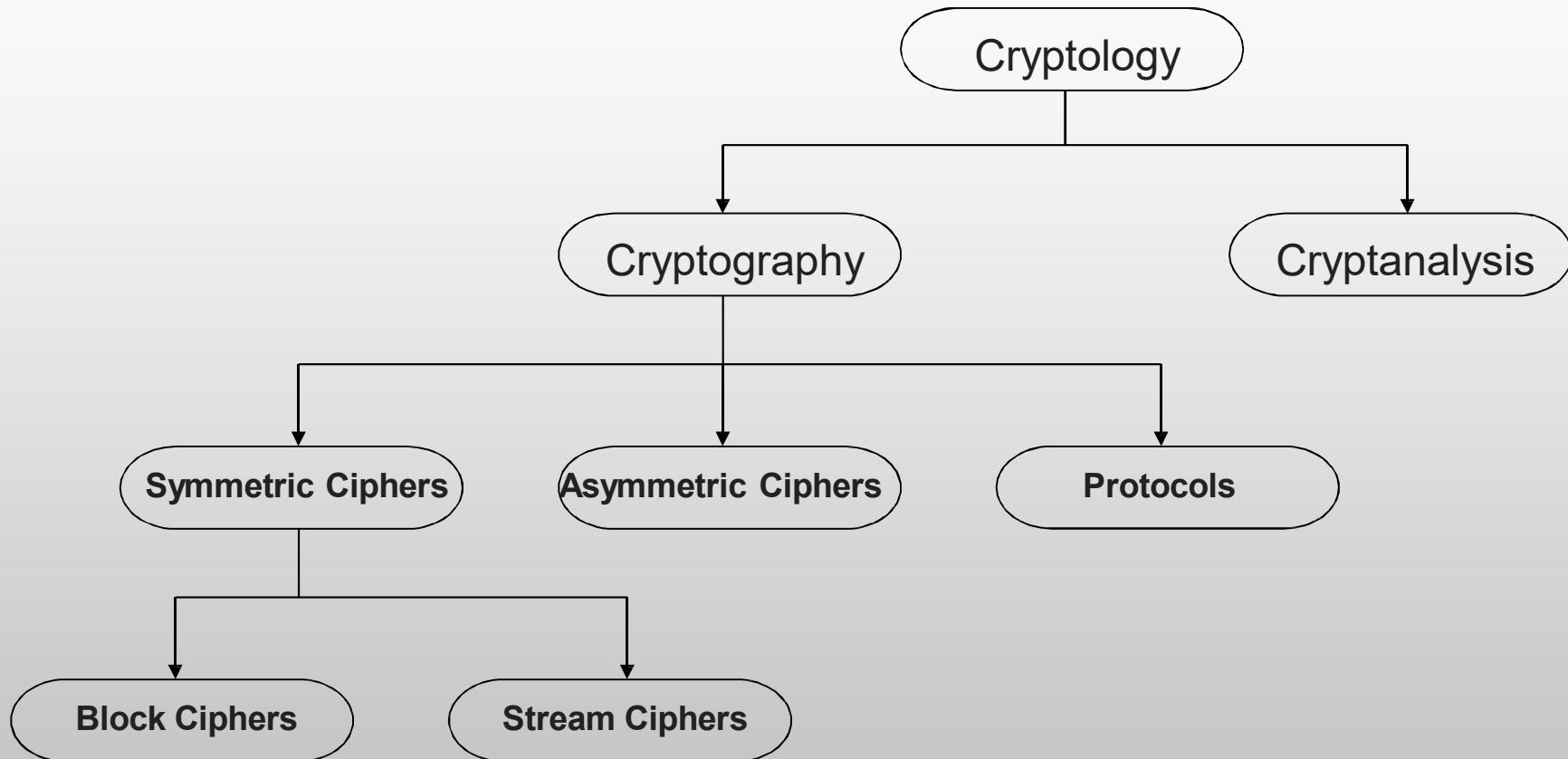
Thank
You



INTRODUCTION TO CRYPTOGRAPHY



🚩 Classification of the Field of Cryptology

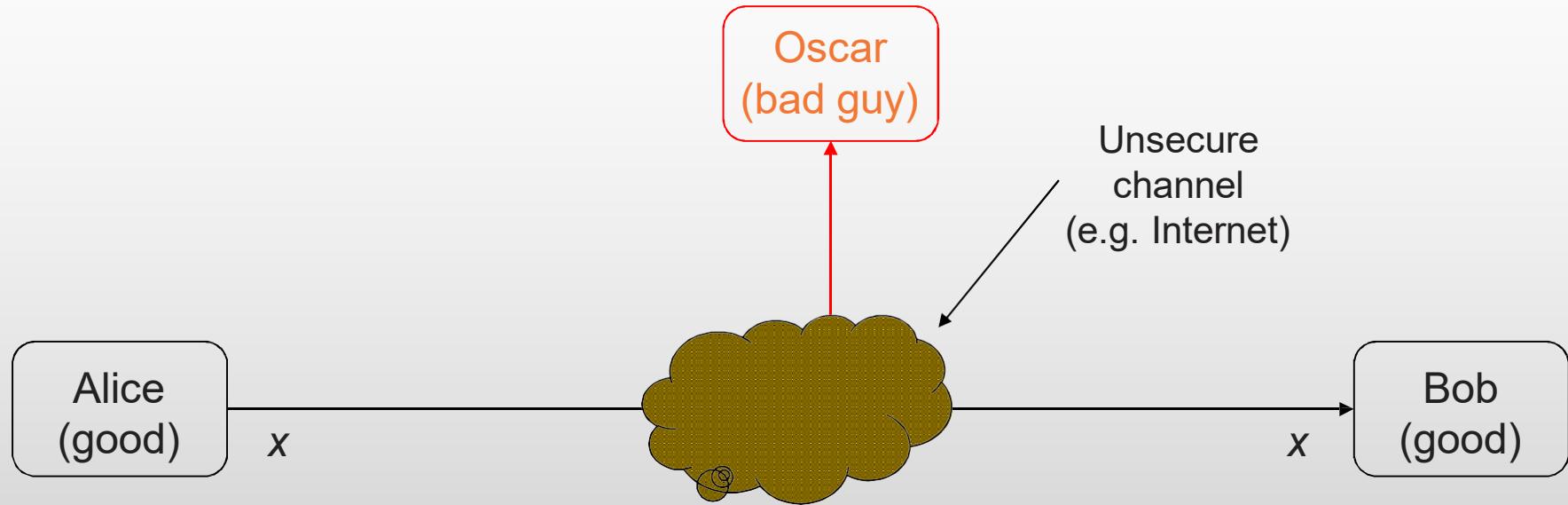


Some Basic Facts

- **Ancient Crypto:** Early signs of encryption in Egypt in ca. 2000 B.C. Letter-based encryption schemes (e.g., Caesar cipher) popular ever since.
- **Symmetric ciphers:** All encryption schemes from ancient times until 1976 were symmetric ones.
- **Asymmetric ciphers:** In 1976 public-key (or asymmetric) cryptography was openly proposed by Diffie, Hellman and Merkle.
- **Hybrid Schemes:** The majority of today's protocols are hybrid schemes, i.e., they use both
 - symmetric ciphers (e.g., for encryption and message authentication) and
 - asymmetric ciphers (e.g., for key exchange and digital signature).

💡 Symmetric Cryptography

- Alternative names: **private-key**, **single-key** or **secret-key** cryptography.

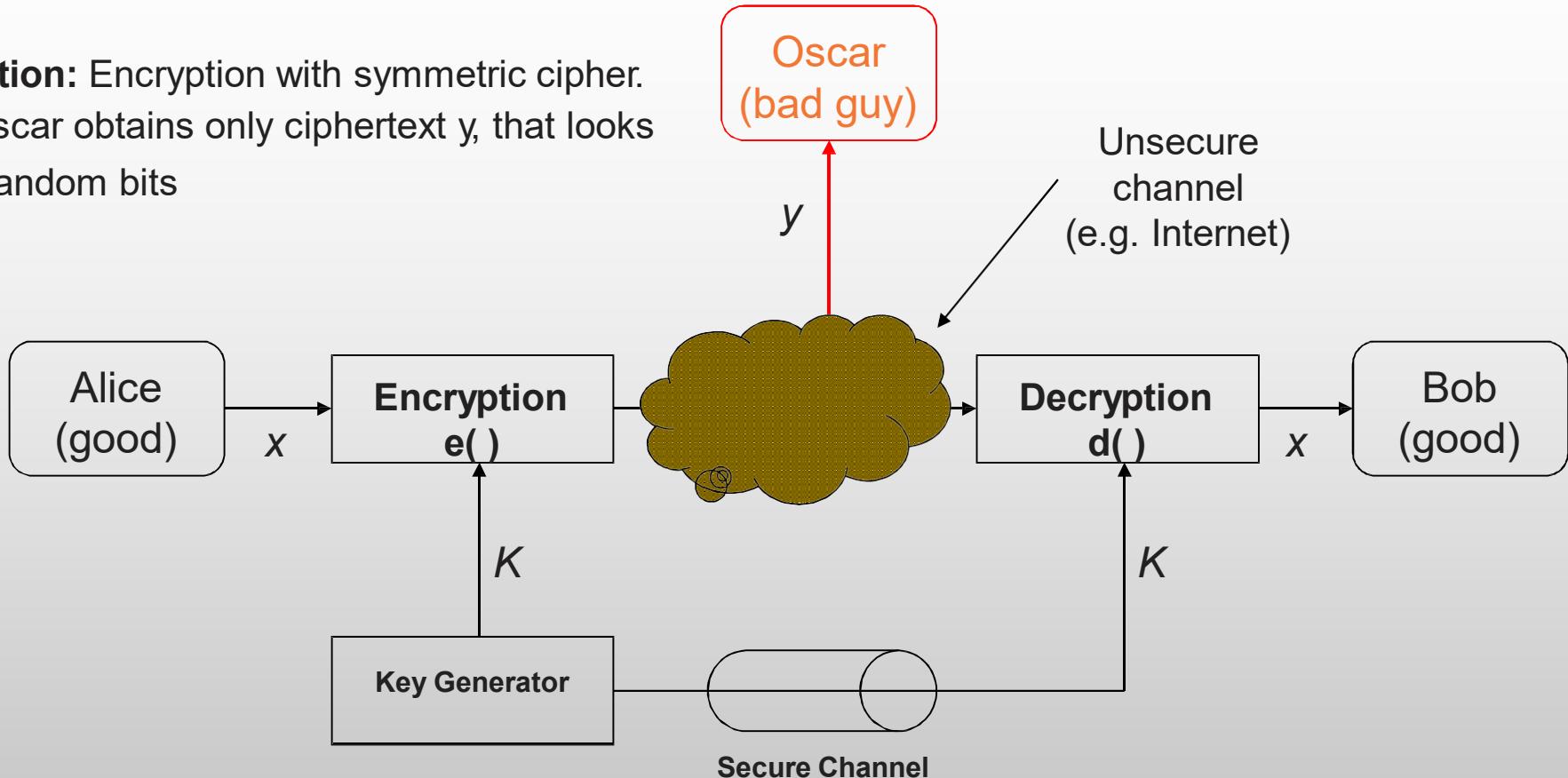


- **Problem Statement:**

- 1) Alice and Bob would like to communicate via an unsecure channel (e.g., WLAN or Internet).
- 2) A malicious third party Oscar (the bad guy) has channel access but should not be able to understand the communication.

💡 Symmetric Cryptography

Solution: Encryption with symmetric cipher.
⇒ Oscar obtains only ciphertext y , that looks like random bits



- x is the **plaintext**
- y is the **cipher-text**
- K is the **key**
- Set of all keys $\{K_1, K_2, \dots, K_n\}$ is the **key space**

▀ Symmetric Cryptography

- Encryption equation
- Decryption equation

$$y = e_K(x)$$

$$x = d_K(y)$$

- Encryption and decryption are inverse operations if the same key K is used on both sides:

$$d_K(y) = d_K(e_K(x)) = x$$

- Important: The key must be transmitted via a **secure channel** between Alice and Bob.
- The secure channel can be realized, e.g., by manually installing the key for the Wi-Fi Protected Access (WPA) protocol or a human courier.
- However, the system is only secure if an attacker does not learn the key K!

⇒ **The problem of secure communication is reduced to secure transmission and storage of the key K.**

Cryptanalysis

- There is no *mathematical proof of security* for any practical cipher
- The only way to have assurance that a cipher is secure is to try to break it (and fail) !

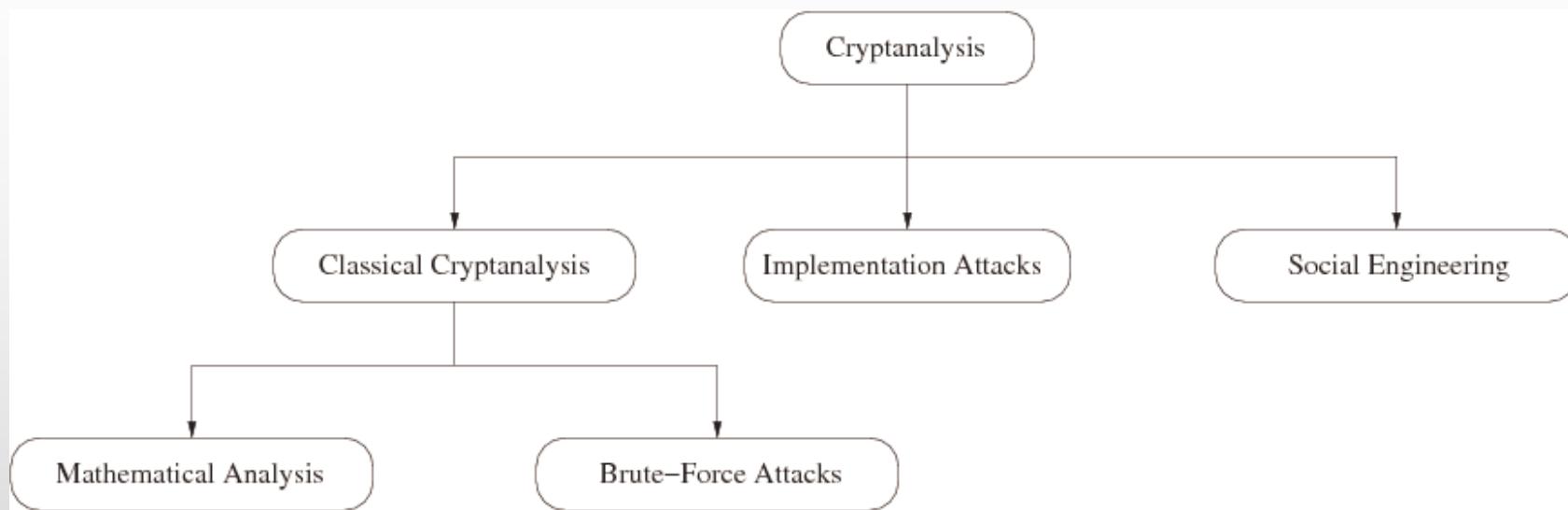
Kerckhoff's Principle is paramount in modern cryptography:

A cryptosystem should be secure even if the attacker (Oscar) knows **all details** about the system, with the exception of the **secret key**.

- In order to achieve Kerckhoff's Principle in practice:
Only use widely known ciphers that have been cryptanalyzed for several years by good cryptographers!

Remark: It is tempting to assume that a cipher is „more secure“ if its details are kept secret. However, history has shown time and again that secret ciphers can almost always been broken once they have been reversed engineered. (Example: Content Scrambling System (CSS) for DVD content protection.)

CRYPTANALYSIS: ATTACKING CRYPTOSYSTEMS



- **Classical Attacks**
 - Mathematical Analysis
 - Brute-Force Attack
- **Implementation Attack:** Try to extract key through reverse engineering or power measurement, e.g., for a banking smart card.
- **Social Engineering:** E.g., trick a user into giving up her password

✿ Brute-Force Attack (or Exhaustive Key Search) against Symmetric Ciphers

- Treats the cipher as a black box
- Requires (at least) 1 plaintext-ciphertext pair (x_0, y_0)
- Check all possible keys until condition is fulfilled:

$$d_K(y_0) = x_0^?$$

- How many keys do we need ?

| Key length in bit | Key space | Security life time (assuming brute-force as best possible attack) |
|----------------------|-----------|---|
| 64 | 2^{64} | Short term (few days or less) |
| 128 | 2^{128} | Long-term (several decades in the absence of quantum computers) |
| 256 | 2^{256} | Long-term (also resistant against quantum computers – note that QC do not exist at the moment and might never exist) |

/Substitution Cipher

- Historical cipher
- Great tool for understanding brute-force vs. analytical attacks
- Encrypts letters rather than bits (like all ciphers until after WW II)

Idea: replace each plaintext letter by a fixed other letter.

| Plaintext | | Ciphertext |
|-----------|---|------------|
| A | → | k |
| B | → | d |
| C | → | w |
| | | |

for instance, ABBA would be encrypted as kddk

- Example (ciphertext):

iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnb hcc
hwwhbsqvqbrevhwqvhlg

- How secure is the Substitution Cipher? Let's look at attacks...

_ATTACKS AGAINST THE SUBSTITUTION CIPHER

1. Attack: Exhaustive Key Search (Brute-Force Attack)

- Simply try every possible substitution table until an intelligent plaintext appears (note that each substitution table is a key)..
- How many substitution tables (= keys) are there?

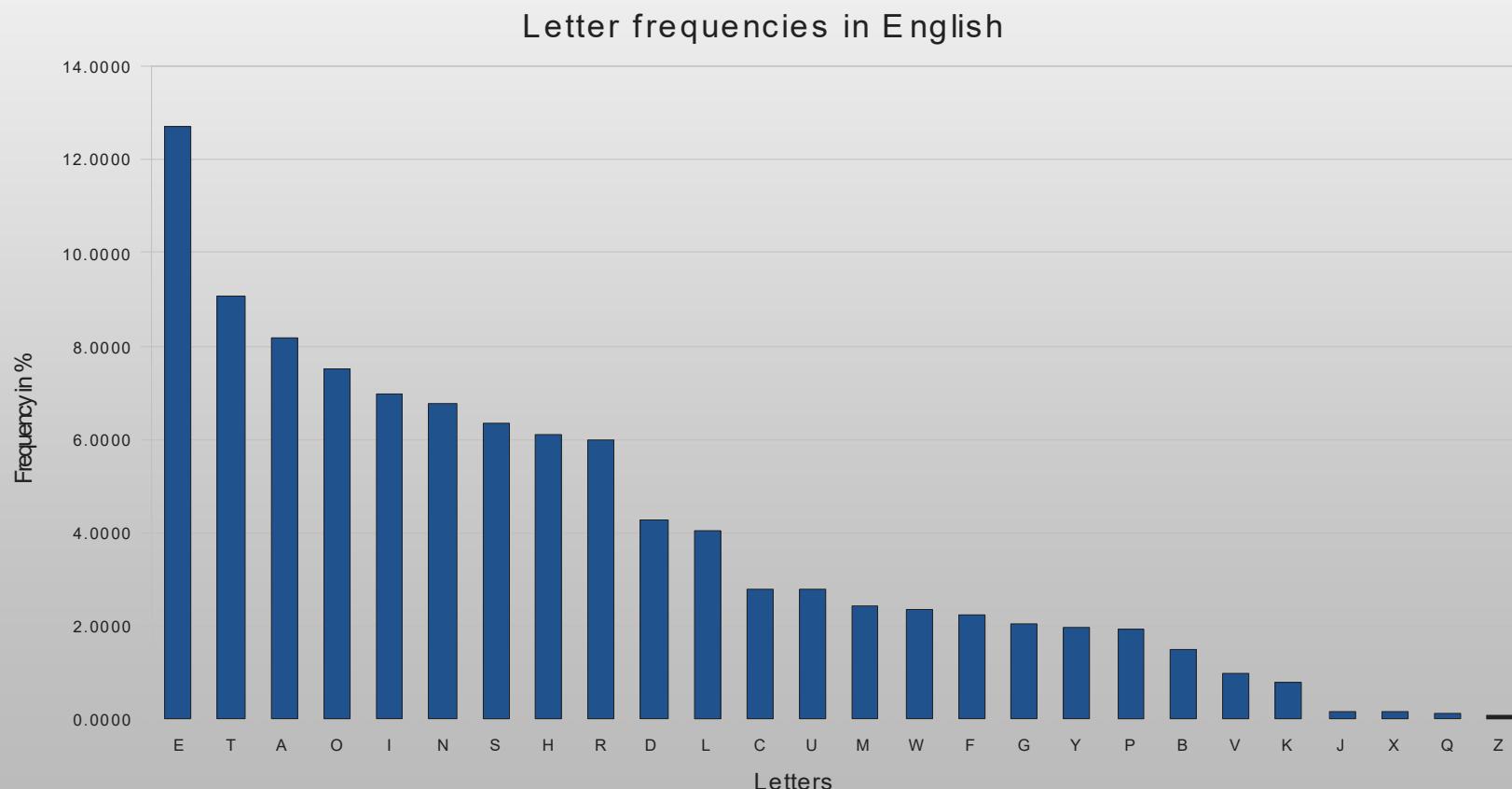
$$26 \times 25 \times \dots \times 3 \times 2 \times 1 = 26! \approx 2^{88}$$

Search through 2^{88} keys is completely infeasible with today's computers!
(cf. earlier table on key lengths)

- Q: Can we now conclude that the substitution cipher is secure since a brute-force attack is not feasible?
- A: No! We have to protect against **all** possible attacks...

💡 2. Attack: Letter Frequency Analysis (Brute-Force Attack)

- Letters have very different frequencies in the English language
- Moreover: the frequency of plaintext letters is preserved in the ciphertext.
- For instance, „e“ is the most common letter in English; almost 13% of all letters in a typical English text are „e“.
- The next most common one is „t“ with about 9%.



▀ Breaking the Substitution Cipher with Letter Frequency Attack

- Let's return to our example and identify the most frequent letter:

i~~q~~ ifcc v~~qq~~r fb rd~~q~~ vfllc~~q~~ na rd~~q~~ cfjwhwz hr bnnb hcc
hwwhbs~~q~~v~~q~~bre hw~~q~~ vh~~l~~~~q~~

- We replace the ciphertext letter ~~q~~ by ~~E~~ and obtain:

i~~E~~ ifcc v~~EE~~r fb rd~~E~~ vfllc~~E~~ na rd~~E~~ cfjwhwz hr bnnb hcc
hwwhbs~~E~~v~~E~~bre hw~~E~~ vh~~l~~~~E~~

- By further guessing based on the frequency of the remaining letters we obtain the plaintext:

WE WILL MEET IN THE MIDDLE OF THE LIBRARY AT NOON ALL
ARRANGEMENTS ARE MADE

- In practice, not only frequencies of individual letters can be used for an attack, but also the frequency of letter pairs (i.e., „th“ is very common in English), letter triples, etc.

CAESAR CIPHER

- WHEN JULIUS CAESAR SENT MESSAGES TO HIS GENERALS, HE DIDN'T TRUST HIS MESSENGERS.
- HE ENCRYPTED HIS MESSAGES BY REPLACING EVERY LETTER:
 - A WITH A D
 - B WITH AN E
 - AND SO ON
- HIS GENERALS KNEW THE "SHIFT BY 3" RULE AND COULD DECIPHER HIS MESSAGES.
- SHIFT BY 'N' = SHIFT CIPHER.



▀ Vigenere Table (Tabula recta)

| | Plain Text | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |



Blaise de Vigenère

Plaintext: ATTACKATDAWN

Key: LEMONLEMONLE

Ciphertext: LXFOPVEFRNHR

Period: ?

Columnar Transposition

- This method rearranges plaintext by rows/columns
- Example: THIS IS A SECRET MESSAGE
- Arranged in rows (ignoring word separations):

THIS

ISAS

ECRE

TMES

SAGE

- Reading by columns, the resulting ciphertext is

TIETSHSCMAIAREGSSESE

- Omitting spaces makes ciphertext even less readable

ENIGMA MACHINE

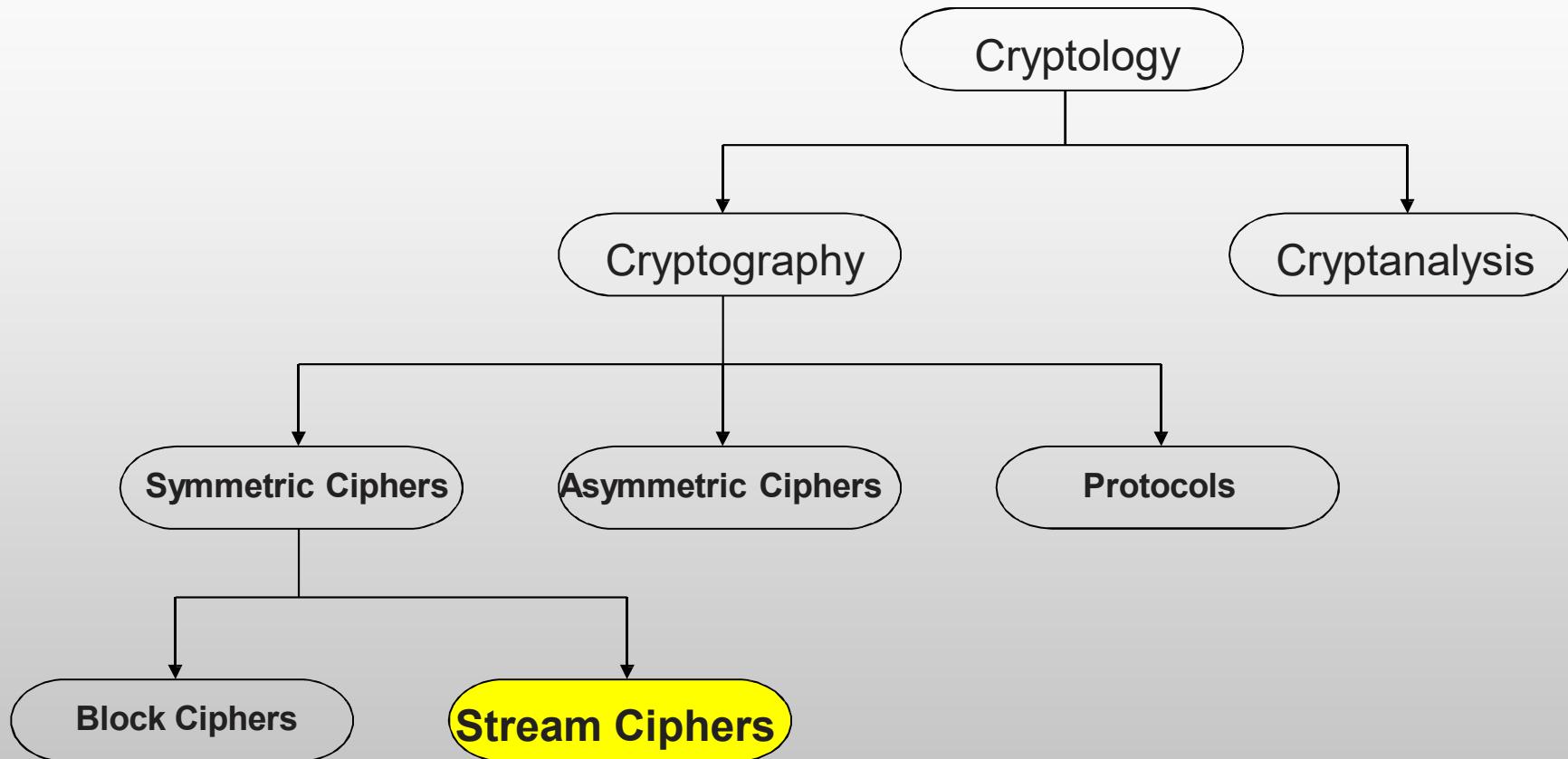
- Is an electric-mechanical machine generating ciphers
- Commercially available first in 1920
- Adopted by a number of nations for government/military purposes
- Most famous use by Nazi Germany
- Was cracked by Allied cryptologists
- Fascinating history (Bletchley Park) – ‘The Imitation Game’
- Designed in 1918, adapted and improved by German army by 1928
- Allies managed to get hold of one machine
 - This helped to break code (and probably helped finishing off the war earlier)



The ENIGMA Machine

- Combination of mechanical and electrical systems
- Keyboard is used to type plain text message
- Rotating discs (“rotors”) form varying electrical circuits
- Electrical current flows to output lamp
- This indicates resulting ciphertext
- High security because of constant change of rotor positions
- [ENIGMA Explained](#)

💡 Stream Ciphers in the Field of Cryptology

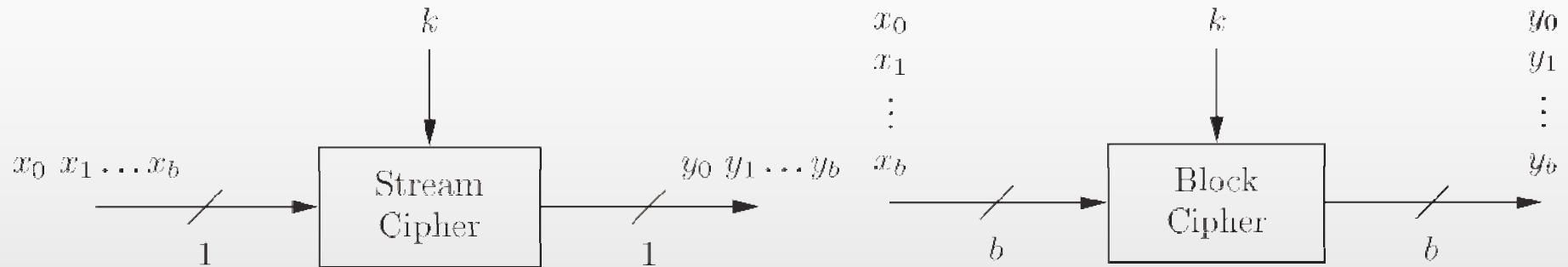


Stream Ciphers were invented in 1917 by Gilbert Vernam

STREAM CIPHERS



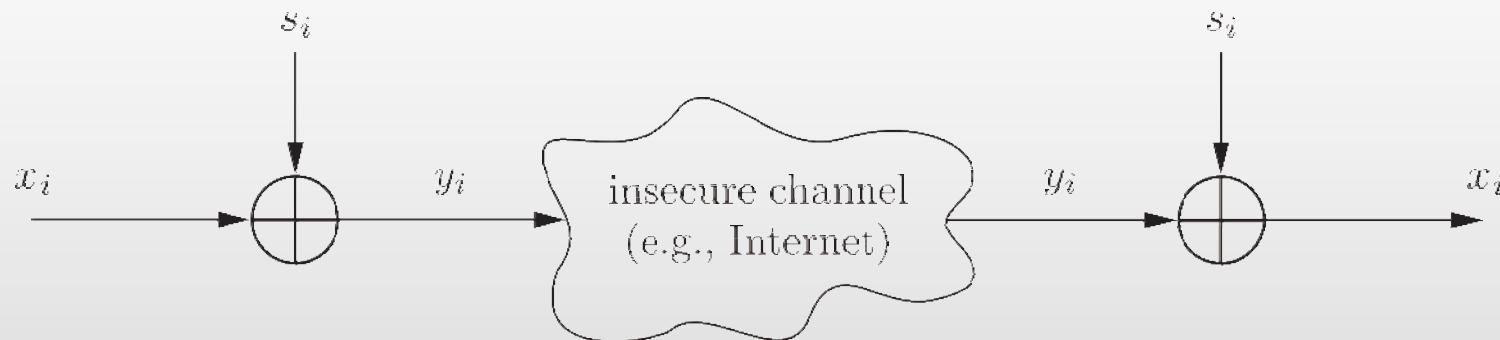
Stream Cipher vs. Block Cipher



- **Stream Ciphers**
 - Encrypt bits individually
 - Usually small and fast common in embedded devices (e.g., A5/1 for GSM phones)
- **Block Ciphers:**
 - Always encrypt a full block (several bits)
 - Are common for Internet applications

Encryption and Decryption with Stream Ciphers

Plaintext x_i , ciphertext y_i and key stream s_i consist of individual bits



- Encryption and decryption are simple additions modulo 2 (aka XOR)
- Encryption and decryption are the same functions
- **Encryption:** $y_i = e_{s_i}(x_i) = x_i + s_i \text{ mod } 2$ $x_i, y_i, s_i \in \{0,1\}$
- **Decryption:** $x_i = e_{s_i}(y_i) = y_i + s_i \text{ mod } 2$

💡 Why is Modulo 2 Addition a Good Encryption Function?

- Modulo 2 addition is equivalent to XOR operation
- For perfectly random key stream s_i , each ciphertext output bit has a 50% chance to be 0 or 1

Good statistic property for ciphertext
- Inverting XOR is simple, since it is the same XOR operation

| x_i | s_i | y_i |
|-------|-------|-------|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

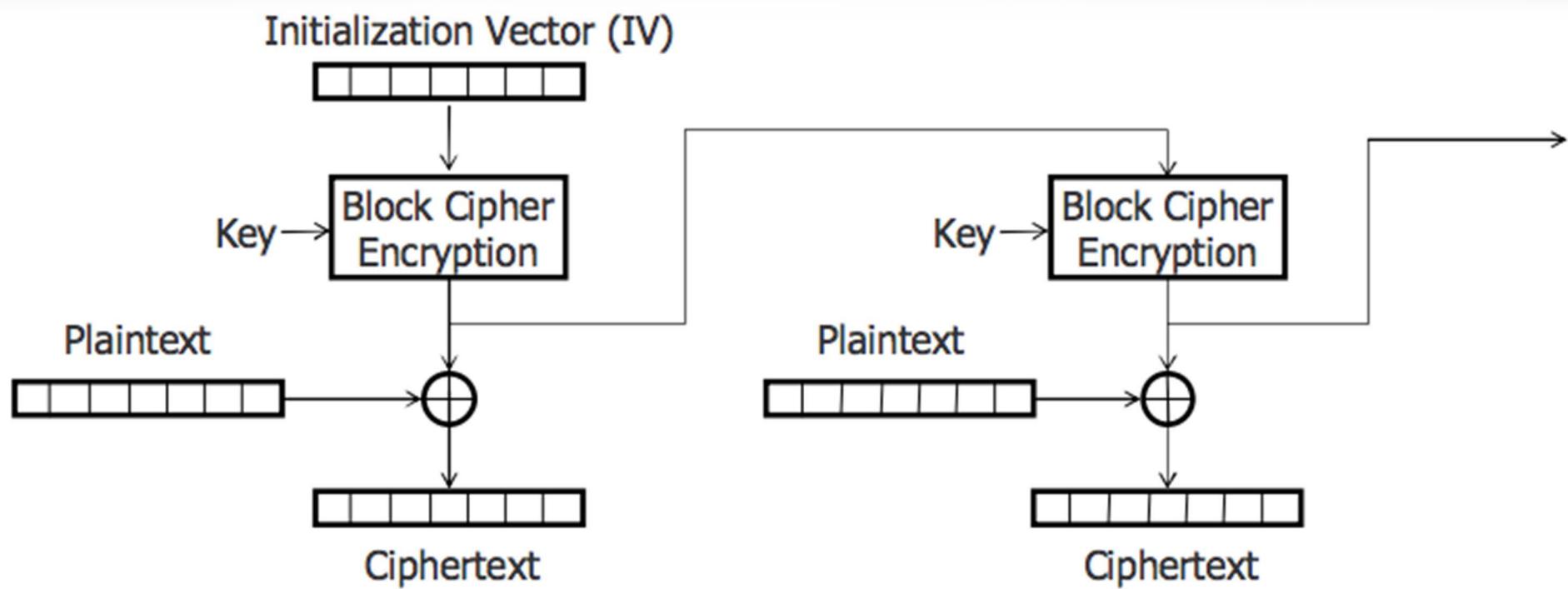
💡 Stream Cipher: Throughput

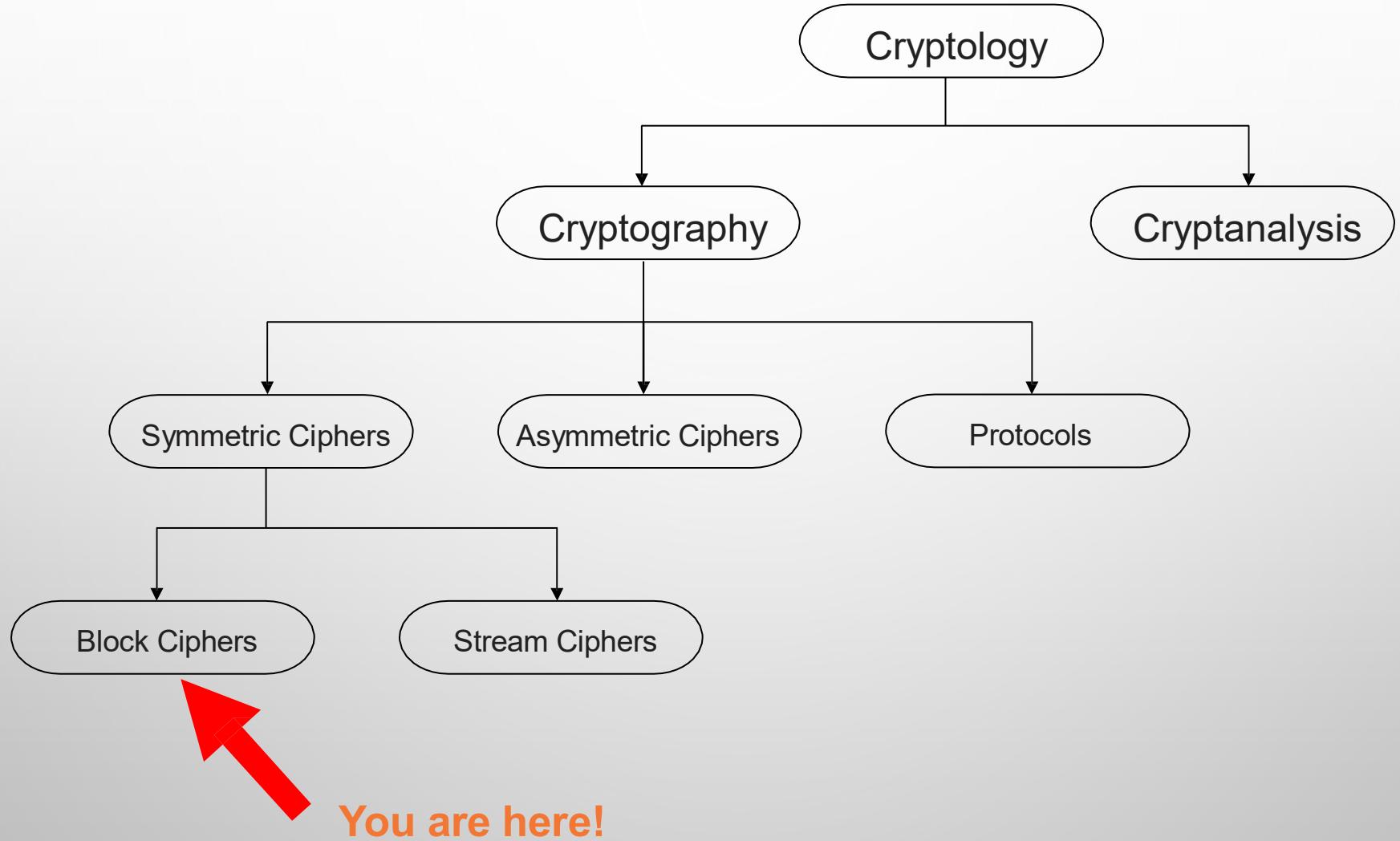
Performance comparison of symmetric ciphers (Pentium4):

| Cipher | Key length | Mbit/s |
|---------------------|-------------|--------|
| DES | 56 | 36.95 |
| 3DES | 112 | 13.32 |
| AES | 128 | 51.19 |
| RC4 (stream cipher) | (choosable) | 211.34 |

Source: Zhao et al., Anatomy and Performance of SSL Processing, ISPASS 2005

BLOCK CIPHERS



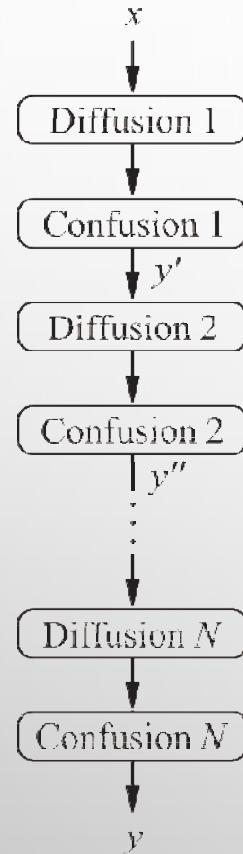




Block Cipher Primitives: Confusion and Diffusion

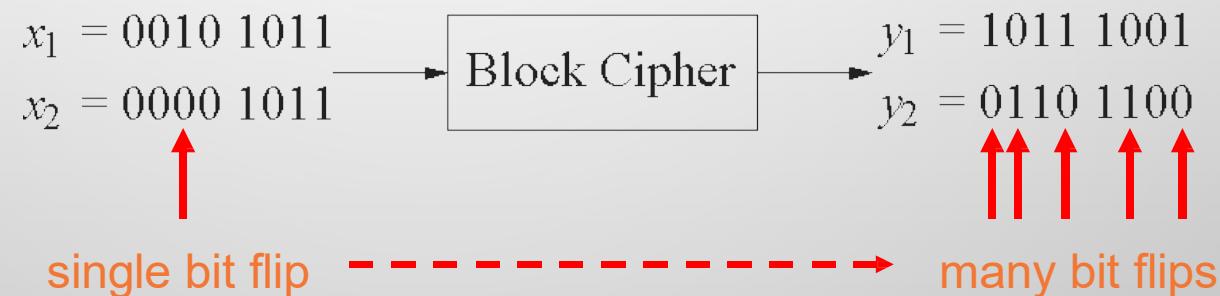
- Claude Shannon: There are two primitive operations with which strong encryption algorithms can be built:
 1. **Confusion:** An encryption operation where the **relationship between key and ciphertext is obscured.**
Today, a common element for achieving confusion is **substitution**, which is found in both AES and DES.
 2. **Diffusion:** An encryption operation where the **influence of one plaintext symbol is spread over many ciphertext symbols** with the goal of hiding statistical properties of the plaintext.
A simple diffusion element is the **bit permutation**, which is frequently used within DES.
- Both operations by themselves cannot provide security. The idea is to concatenate confusion and diffusion elements to build so called *product ciphers*.

Product Ciphers



- Most of today's block ciphers are *product ciphers* as they consist of rounds which are applied repeatedly to the data.
- Can reach excellent diffusion: **changing of one bit of plaintext results on average in the change of half the output bits.**

Example:



HOW TO CHOOSE AN ENCRYPTION ALGORITHM?

| | DES | 3DES | AES |
|--|-----------------------|------|----------------------|
| Is the algorithm trusted by the cryptographic community? | Been replaced by 3DES | Yes | Verdict is still out |
| Does the algorithm adequately protect against brute-force attacks? | No | Yes | Yes |

DATA ENCRYPTION STANDARD (DES)

- The most popular symmetric encryption standards.
 - Developed by IBM
 - Thought to be unbreakable in the 1970s
 - Shared keys enable the encryption and decryption
- DES converts blocks of 64-bits of clear text into ciphertext by using an encryption algorithm.
 - The decryption algorithm on the remote end restores ciphertext to clear text.

DES SCORECARD

| Description | Data Encryption Standard |
|----------------------|---|
| Timeline | Standardized 1976 |
| Type of Algorithm | Symmetric |
| Key size (in bits) | 56 bits |
| Speed | Medium |
| Time to crack | The EFF's DES cracker (Deep Crack) breaks a DES key in 56 hours |
| Resource Consumption | Medium |

DES SECURITY RATING

- Because of its short key length, DES is considered a good protocol to protect data for a very short time.
 - **3DES** is a better choice to protect data because it has an algorithm that is very trusted and has higher security strength.
- Recommendations:
 - Change keys frequently to help prevent brute-force attacks.
 - Use a secure channel to communicate the DES key from the sender to the receiver.

Alternatives to DES

| Algorithm | I/O Bit | key lengths | remarks |
|----------------|---------|-----------------|---|
| AES / Rijndael | 128 | 128/192/256 | DES "replacement", worldwide used standard |
| Triple DES | 64 | 112 (effective) | conservative choice |
| Mars | 128 | 128/192/256 | AES finalist |
| RC6 | 128 | 128/192/256 | AES finalist |
| Serpent | 128 | 128/192/256 | AES finalist |
| Twofish | 128 | 128/192/256 | AES finalist |
| IDEA | 64 | 128 | patented |

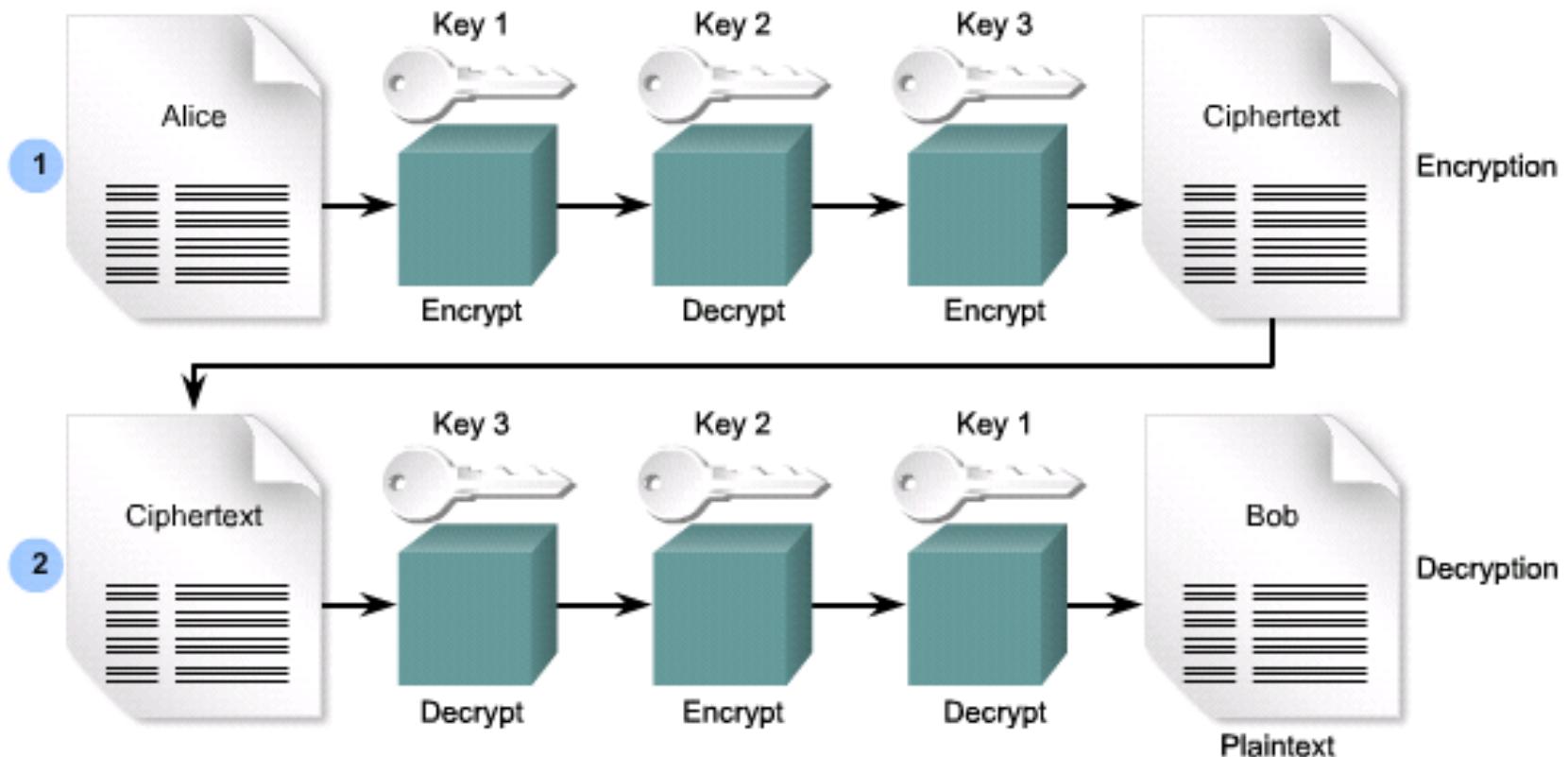
TRIPLE DES (3DES OR TDES)

- 2DES is not recommended. Find out why?
- 3DES is 256 times stronger than DES.
- It takes a 64-bit block of data and performs three des operations in sequence:
 - Encrypts, decrypts, and encrypts.
 - Requires additional processing time.
 - Can use 1, 2, or 3 different keys (when used with only one key, it is the same as des).

3DES SCORECARD

| | |
|---|---|
| Description | Triple Data Encryption Standard |
| Timeline | Standardized 1977 |
| Type of Algorithm | Symmetric |
| Key size (in bits) | 112 and 168 bits |
| Speed | Low |
| Time to crack <small>(Assuming a computer could try 255 keys per second)</small> | 4.6 Billion years with current technology |
| Resource Consumption | Medium |

Symmetric Key (triple DES) Encryption



1. The clear text from Alice is encrypted using Key 1. That ciphertext is decrypted using a different key, Key 2. Finally that ciphertext is encrypted using another key, Key 3.
2. When the 3DES ciphered text is received, the process is reversed. That is, the ciphered text must first be decrypted using Key 3, encrypted using Key 2, and finally decrypted using Key 1.

ADVANCED ENCRYPTION STANDARD (AES)

- AES is an extremely secure Federal Information Processing Standard (FIPS)-approved cryptographic algorithm.
 - Based on the RIJNDAEL algorithm.
 - It uses keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits.
 - All 9 combinations of key length and block length are possible.
- AES is the world standard for block encryption.

AES SCORECARD

| | |
|---|------------------------------|
| Description | Advanced Encryption Standard |
| Timeline | Official Standard since 2001 |
| Type of Algorithm | Symmetric |
| Key size (in bits) | 128, 192, and 256 |
| Speed | High |
| Time to crack <small>(Assuming a computer could try 255 keys per second)</small> | 149 Trillion years |
| Resource Consumption | Low |

RC ALGORITHMS

- The RC algorithms were designed all or in part by Ronald Rivest, who also invented MD5.
- The RC algorithms are widely deployed in many networking applications because of their favorable speed and variable key-length capabilities.
- There are several variation of RC algorithms including:
 - RC2
 - RC4
 - RC5
 - RC6

RON'S CODE OR RIVEST CODES SCORECARD

| Description | RC2 | RC4 | RC5 | RC6 |
|--------------------|--|--|---|---|
| Timeline | 1987 | 1987 | 1994 | 1998 |
| Type of Algorithm | Block cipher | Stream cipher | Block cipher | Block cipher |
| Key size (in bits) | 40 and 64 | 1 - 256 | 0 to 2040 bits (128 suggested) | 128, 192, or 256 |
| Use | Variable key-size block cipher that was designed as a "drop-in" replacement for DES. | Most widely used stream cipher based on a variable key-size Vernam stream cipher. It is often used in file encryption products and secure communications, such as within SSL. The cipher can be expected to run very quickly in software and is considered secure. | A fast block cipher that has a variable block size and key size. It can be used as a drop-in replacement for DES if the block size is set to 64-bit. | An AES finalist (Rijndael won). A 128-bit to 256- bit block cipher that was designed by Rivest, Sidney, and Yin and is based on RC5. Its main design goal was to meet the requirement of AES. |



Public Key Cryptography

Kavinga Yapa Abeywardena



AGENDA

- Symmetric Cryptography Revisited
- Principles of Asymmetric Cryptography
- Public-Key Cryptography : Limitations
- Hybrid Cryptography
- Digital Signatures
- Certificates & PKI

Symmetric Cryptography Revisited

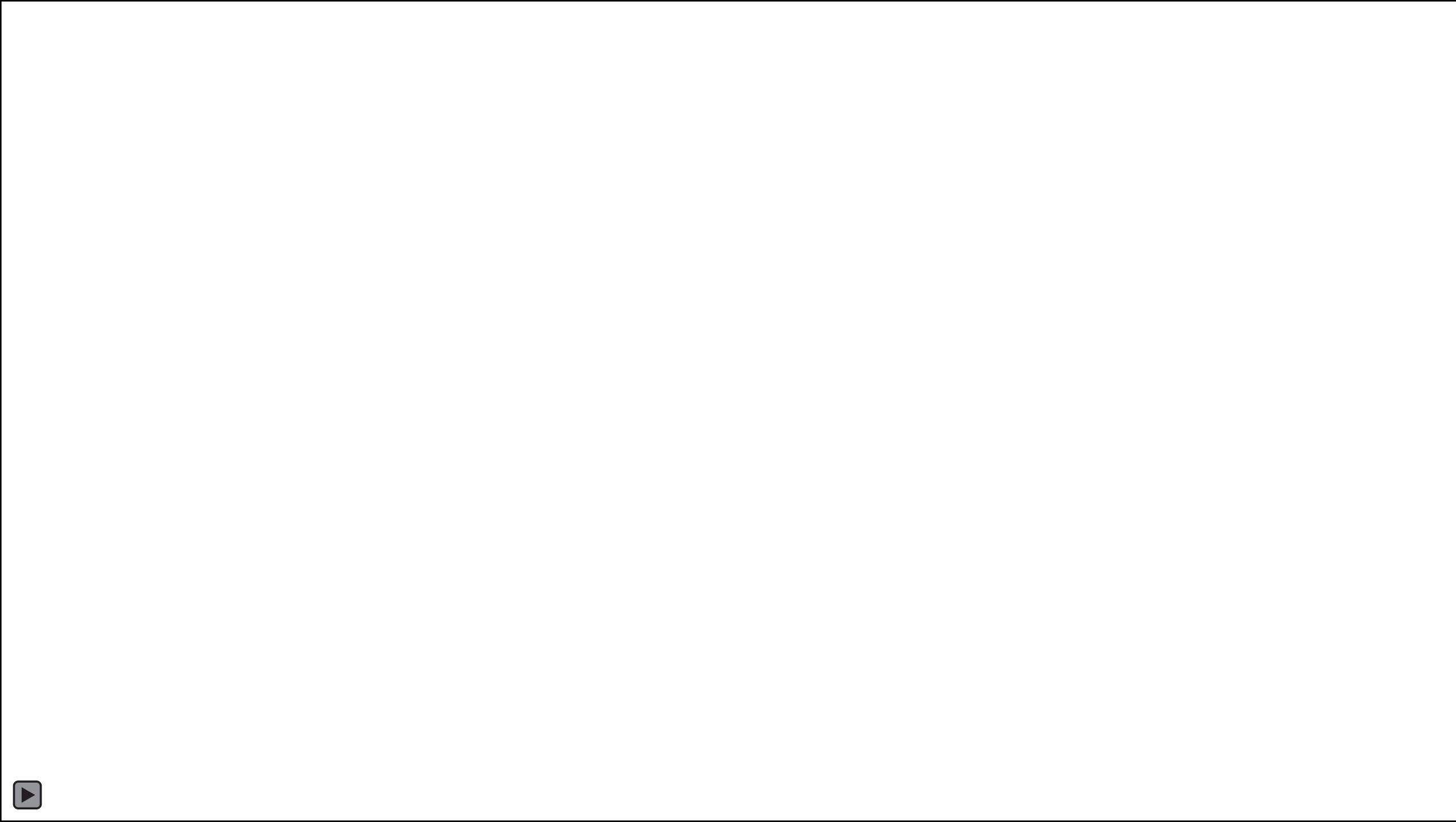
- Same **secret key** K is used for encryption and decryption



Symmetric Cryptography - Limitations



- Safe with a **STRONG** lock
- Only Alice and Bob should have the key
- **Key distribution problem:** Secret key must be transported securely
- Another problem?



Public Key Cryptography (Asymmetric)

- New idea proposed in 1976 by Whitfield **Diffie** and Martin **Hellman**.



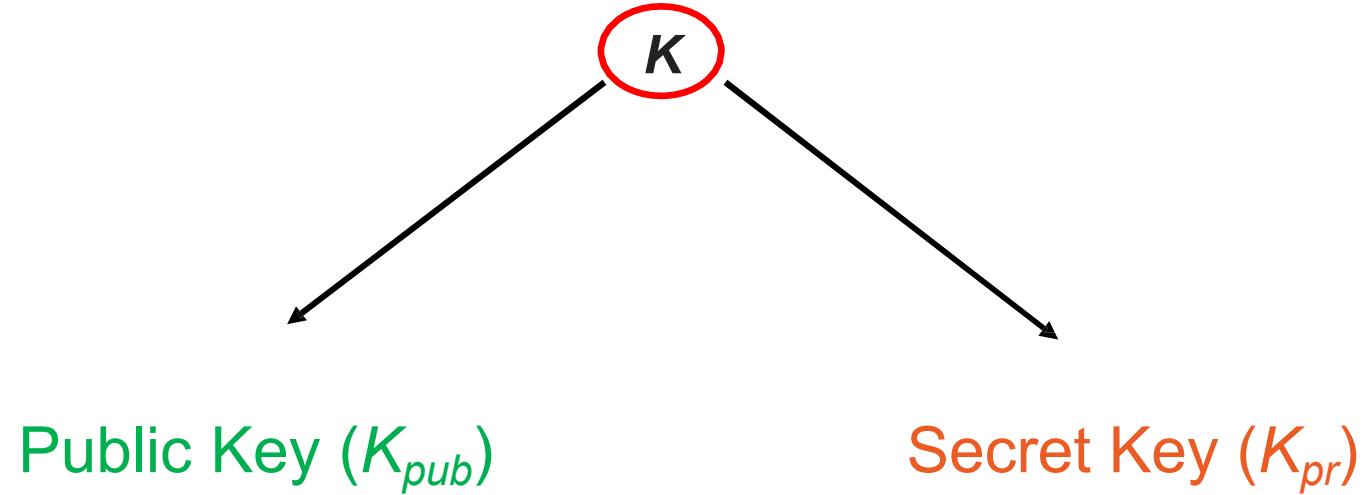
Everyone can drop a letter



Only the owner has the correct key to open the box

Public Key Cryptography

- **Principle:** Split up the key.
- During the key generation, a key pair K_{pub} and K_{pr} is computed



Public Key Cryptography

Alice

Bob

$$\xleftarrow{\hspace{1cm}} (\textcolor{green}{K_{pubB}}, \textcolor{red}{K_{prB}}) = K$$



Public Key Cryptography : Limitation

- 1000 times **SLOWER** than Symmetric Encryption!
- Can only encrypt a small amount of data

Solution : A Hybrid system

- Use both asymmetric and symmetric algorithms
- **Key Exchange** (for symmetric) using Public Key Encryption
- **Encryption of Messages** (faster) using Symmetric Encryption

A Hybrid Protocol : Key Exchange

Alice

Bob

$$\xleftarrow{\hspace{1cm}} (\textcolor{green}{K_{pubB}}, \textcolor{red}{K_{prB}}) = K$$



Key distribution problem Solved!

A Hybrid Protocol : Encryption of Messages



How to build a Public Key Algorithm?

Asymmetric schemes are based on a '**one-way function**'

- Computing $y = f(x)$ is computationally easy
- Computing $x = f^{-1}(y)$ is computationally infeasible

One way functions are based on **mathematically hard problems**.

Three main families:

- **Factoring integers** (RSA, ...):
Given a composite integer n , find its prime factors (Multiply two primes: easy)
- **Discrete Logarithm** (Diffie-Hellman, Elgamal, DSA, ...): Given a , y and m , find x such that $a^x \equiv y \pmod{m}$
(Exponentiation a^x : easy)
- **Elliptic Curves (EC)** (ECDH, ECDSA): Generalization of discrete logarithm
Note: The problems are considered mathematically hard, but no proof exists (so far).

The RSA Cryptosystem

- Martin Hellman and Whitfield Diffie published their landmark public-key paper in 1976
- Ronald Rivest, Adi Shamir and Leonard Adleman proposed the asymmetric RSA cryptosystem in 1977
- Until now, RSA is the most widely used asymmetric cryptosystem although elliptic curve cryptography (ECC) becomes increasingly popular (Faster)
- RSA is mainly used for two applications
 - Transport of (i.e., symmetric) keys
 - Digital signatures

Diffie–Hellman Key Exchange



- Proposed in 1976 by **Whitfield Diffie and Martin Hellman**
- **Widely used**, e.g. in Secure Shell (SSH), Transport Layer Security (TLS), and Internet Protocol Security (IPSec)
- The Diffie–Hellman Key Exchange (DHKE) is a key exchange protocol and **not** used for encryption
(For the purpose of encryption based on the DHKE, ElGamal can be used.)



DIGITAL SIGNATURES



Motivation for Digital Signatures

- Alice orders a pink car from the car salesmen Bob
 - After seeing the pink car, Alice states that she has never ordered it:
 - How can Bob prove towards a judge that Alice has ordered a pink car? (And that he did not fabricate the order himself)
- ⇒ Symmetric cryptography fails because both Alice and Bob can be malicious
- ⇒ Can be achieved with public-key cryptography

Digital Signatures : Basic Principle



Digital Signatures

- For a given message ' x ', a digital signature is appended to the message (just like a conventional signature).
- Only the **person with the private key** should be able to **generate** the signature.
- The signature must change for every document.
 - ⇒ The signature is realized as a function with the message ' x ' and the private key as input.
 - ⇒ The public key and the message ' x ' are the inputs to the verification function.

CERTIFICATES

- In order to authenticate public keys, all public keys are digitally signed by a central trusted authority.
- Such a construction is called *certificate*

certificate = public key + ID(user) + digital signature over public key and ID

- In its most basic form, a certificate for the key k_{pub} of user Alice is:

$$\mathbf{Cert(Alice)} = (k_{pub}, \mathbf{ID(Alice)}, \mathbf{sig}_{KCA}(k_{pub}, \mathbf{ID(Alice)}))$$

- Certificates bind the identity of user to his/her public key
- The trusted authority that issues the certificate is referred to as ***certifying authority (CA)***
- "Issuing certificates" means in particular that the CA computes the signature $\mathbf{sig}_{KCA}(k_{pub})$ using its **(super secret!)** private key k_{CA}
- The party who receives a certificate, e.g., Bob, verifies Alice's public key using the public key of the CA

CERTIFICATES IN REAL WORLD

- In real world certificates contain much more information than just a public key and a signature.
- X509** is a popular signature standard. The main fields of such a certificate are shown to the right.

| |
|--|
| Serial Number |
| Certificate Algorithm: - Algorithm - Parameters |
| Issuer |
| Period of Validity: - Not Before Date - Not After Date |
| Subject |
| Subject's Public Key: - Algorithm - Parameters - Public Key |
| Signature |

REMAINNING ISSUES WITH CERTIFICATES

There are many additional problems when certificates are to be used in systems with a large number of participants. The more pressing ones are:

1. Users communicate which other whose certificates are issued by different CAs

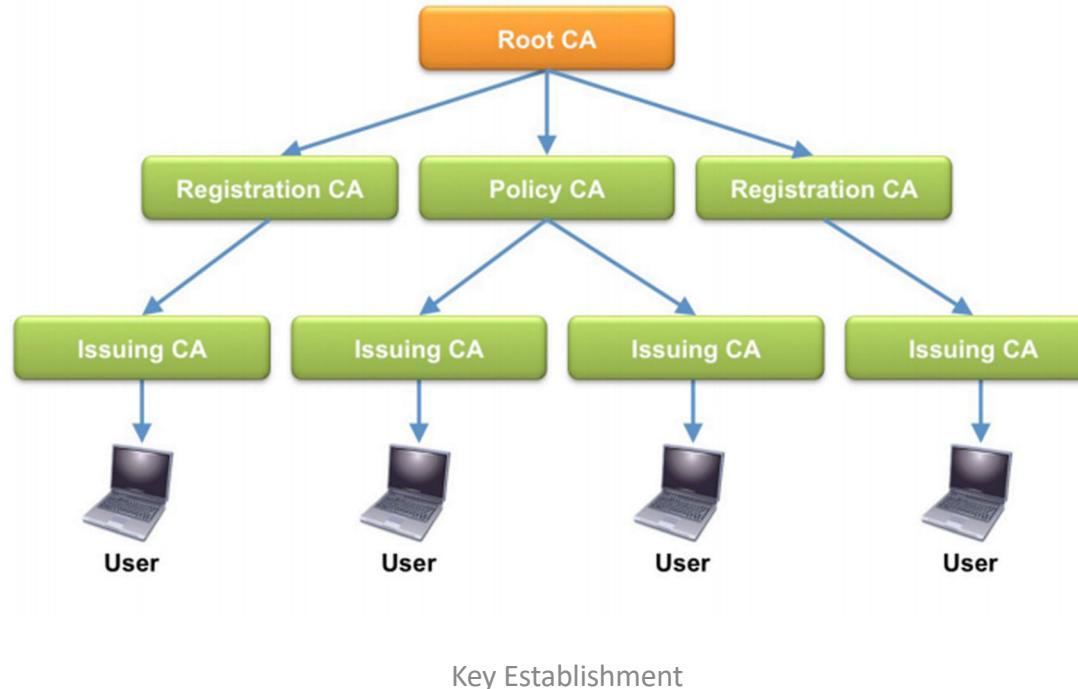
- This requires cross-certification of CAs, e.g.. CA1 certifies the public-key of CA2. If Alice trusts her CA1, cross-certification ensures that she also trusts CA2. This is called a "**chain of trust**" and it is said that trust is delegated.

2. Certificate Revocation Lists (CRLs)

- Another real-world problem is that certificates must be revoked, e.g., if a smart card with certificate is lost or if a user leaves an organization. For this, **CRLs** must be sent out periodically (e.g., daily) which is a burden on the bandwidth of the system.

Public Key Infrastructure

The entire system that is formed by CAs together with the necessary support mechanisms is called a **public-key infrastructure (PKI)**.

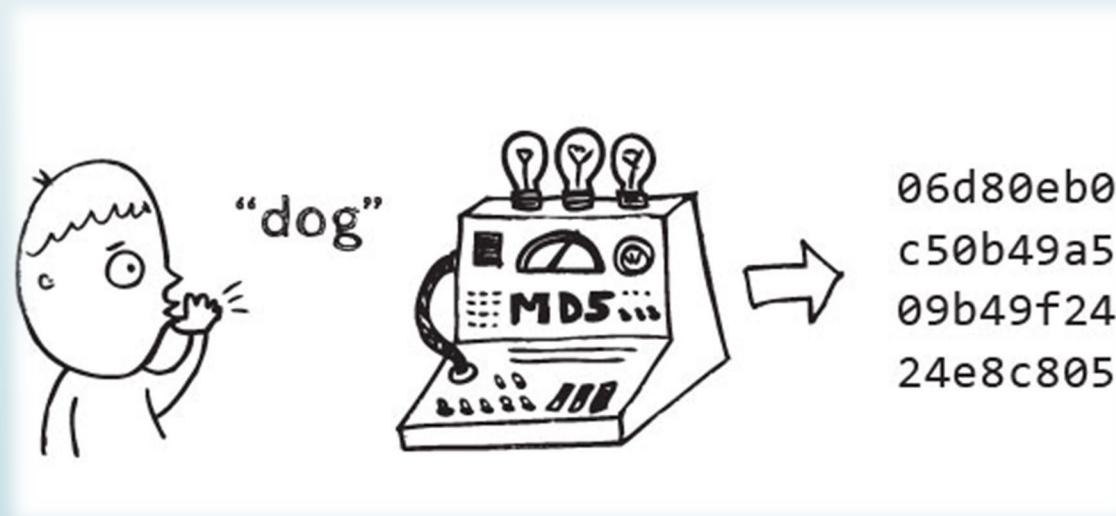


Thank
You





Cryptographic Hash Functions



Content of this Chapter

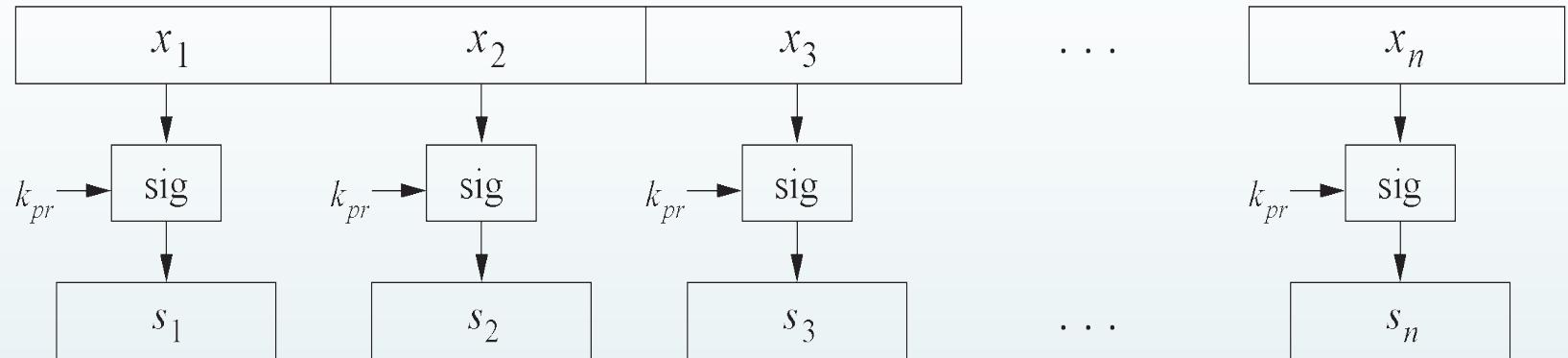
- Why we need hash functions
- How does it work
- Security properties
- Algorithms
- Example: The Secure Hash Algorithm SHA-1

Content of this Chapter

- **Why we need hash functions**
- How does it work
- Security properties
- Algorithms
- Example: The Secure Hash Algorithm SHA-1

Motivation

Naive signing of long messages generates a signature of same length.



Three Problems

- Computational overhead (256MB file need 1 Million 256bit RSA signatures) ☹
- Message overhead (256MB file, total of 512MB must be transmitted) ☹
- Security limitations (Can Replace/Remove Blocks) ☹

Solution:

Instead of signing the whole message, sign only a digest (=hash)

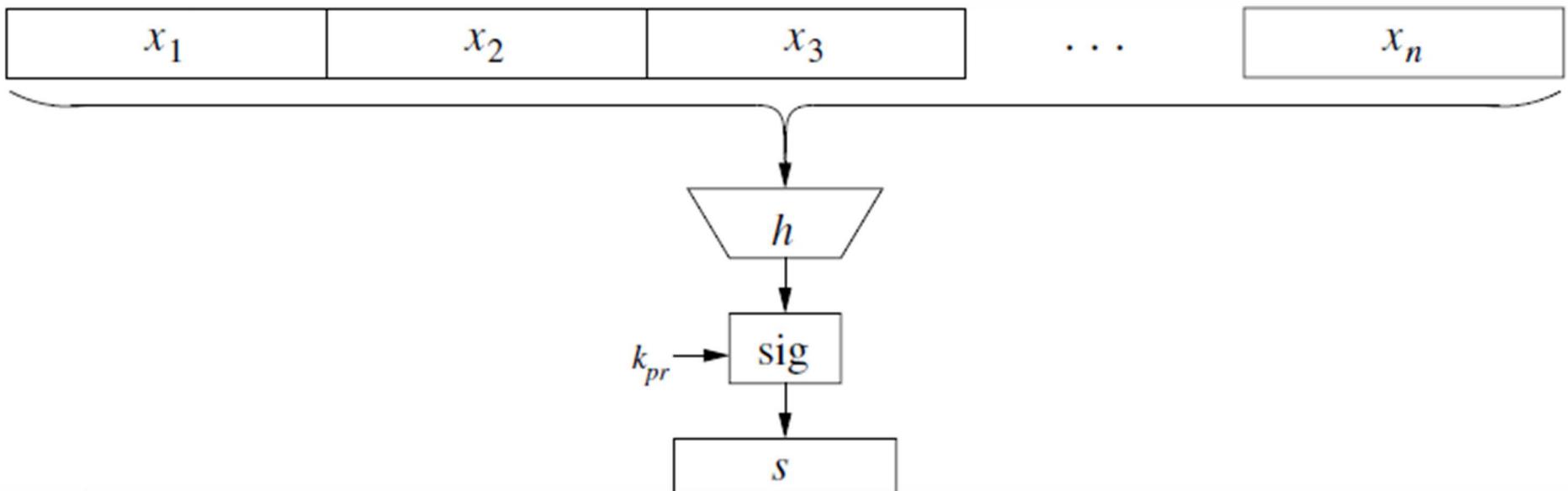
Also secure, but much faster ☺

Needed:

Hash Functions! → One short signature for an arbitrary length message



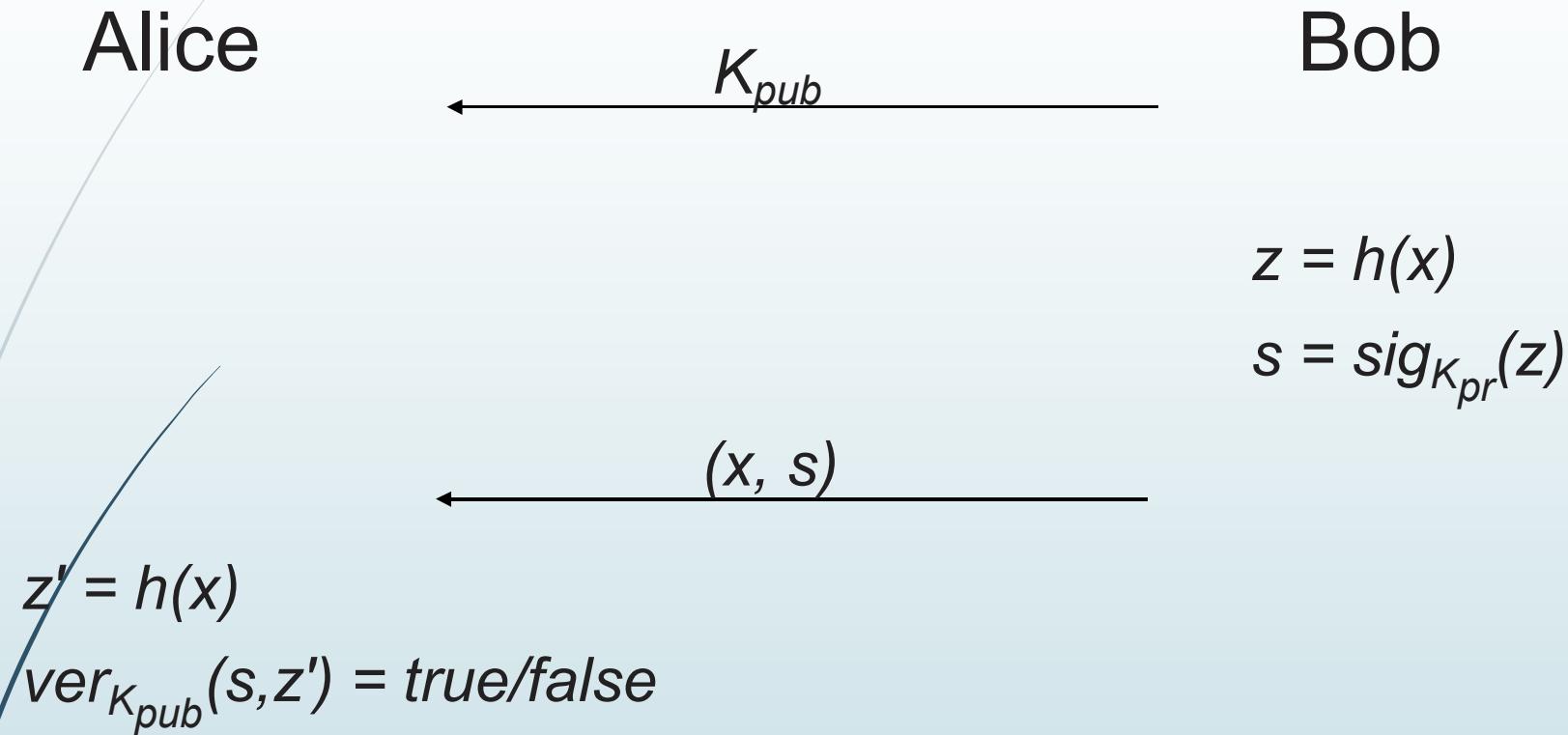
💡 Digital Signature with a Hash Function



- If we had a hash function that somehow computes a fingerprint of the message 'x' we could perform the signature operation as shown above.



Basic Protocol for Digital Signatures with a Hash Function:

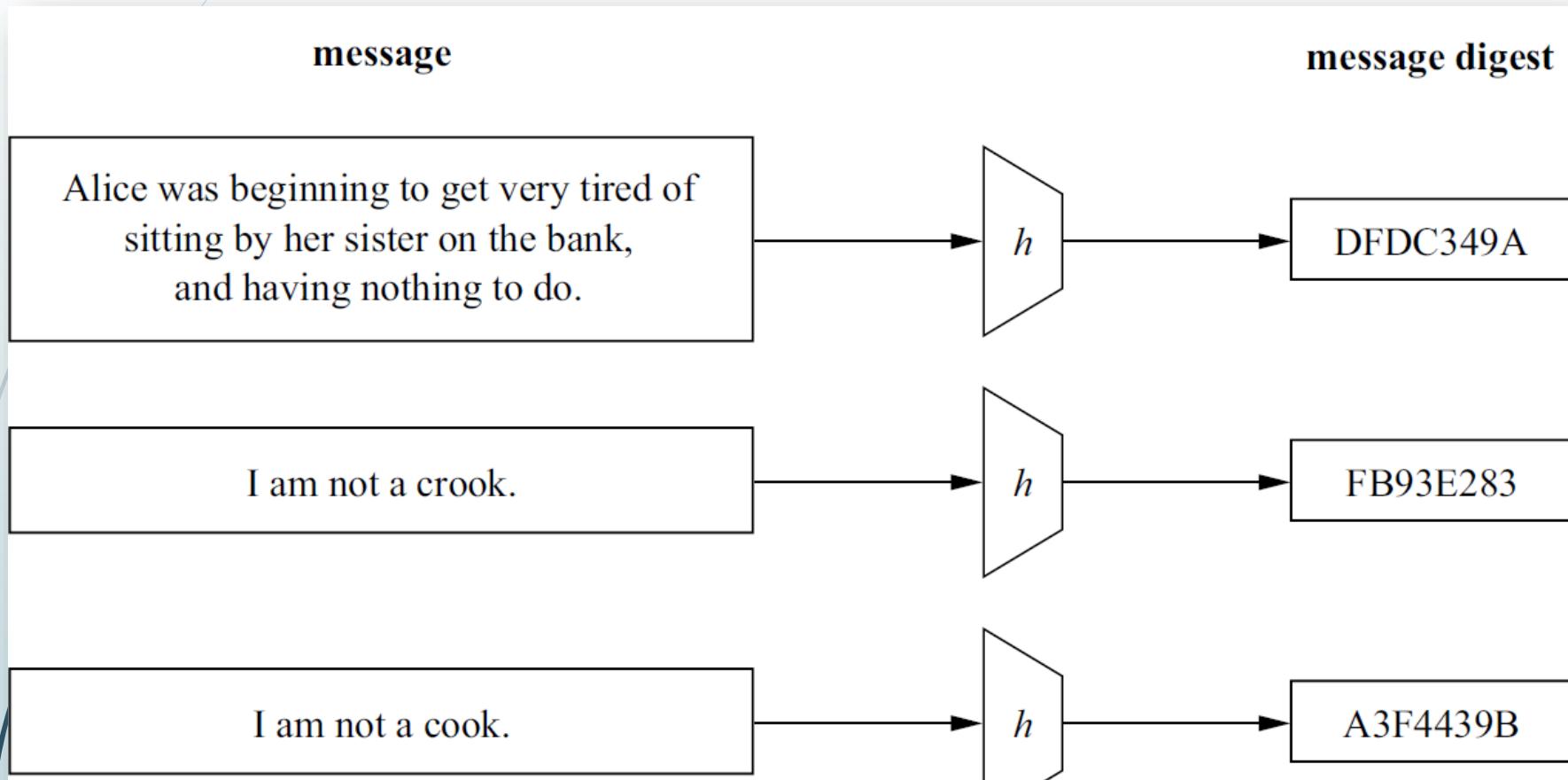


Note: Both the signature generation and the verification operate on the hash value 'z' rather than on the message itself. Hence, the hash value represents the message(Fingerprint/Digest).



Principal input–output behavior of hash functions

- Output of a hash function is of **fixed length** and independent of the input length.



- Practical hash functions have output lengths between **128–512 bits**.
- **Diffusion** property is desirable as well as **Efficiency**.



Content of this Chapter

- Why we need hash functions
- How does it work
- **Security properties**
- Algorithms
- Example: The Secure Hash Algorithm SHA-1

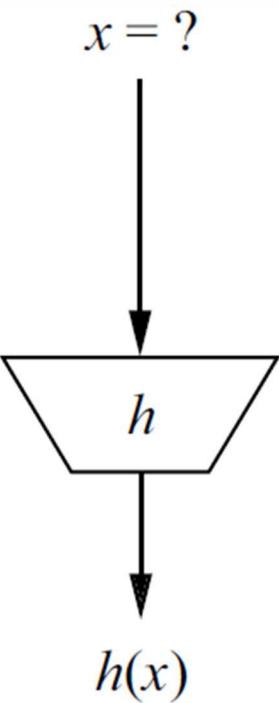


Hash Function: Security Properties

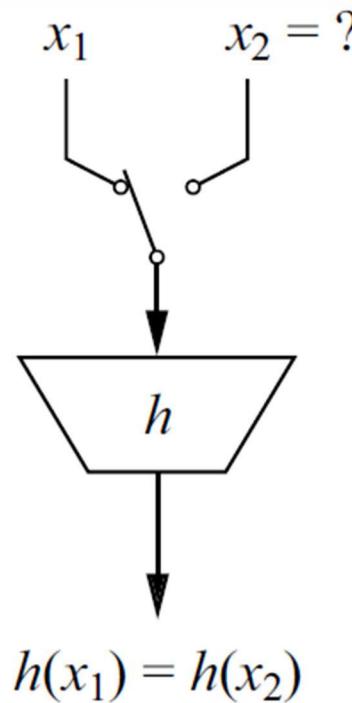
- **Preimage Resistance:** For a given output 'z', it is impossible to find any input 'x' such that $h(x) = z$, i.e., $h(x)$ is **one-way**.
- **Second Preimage Resistance:** Given x_1 , and thus $h(x_1)$, it is computationally infeasible to find any x_2 such that $h(x_1) = h(x_2)$.
- **Collision Resistance:** It is computationally infeasible to find any pairs $x_1 \neq x_2$ such that $h(x_1) = h(x_2)$.



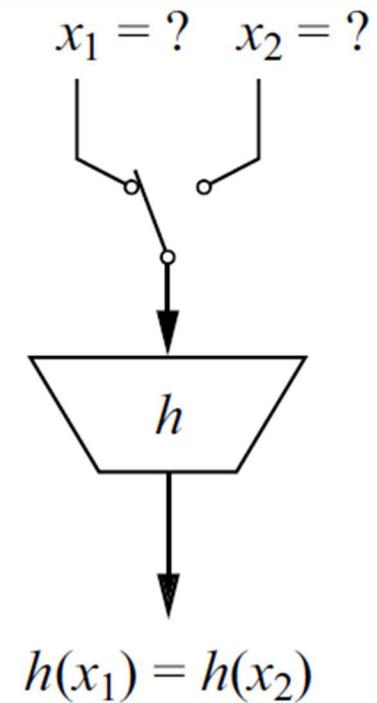
The three security properties of hash functions



preimage resistance



second preimage
resistance



collision resistance





Message Authentication Codes (MAC's)

Some other MACs!



This is Our MAC!





Content of this Chapter

- The principle behind MACs
- The security properties that can be achieved with MACs
- How MACs can be realized with hash functions and with block ciphers

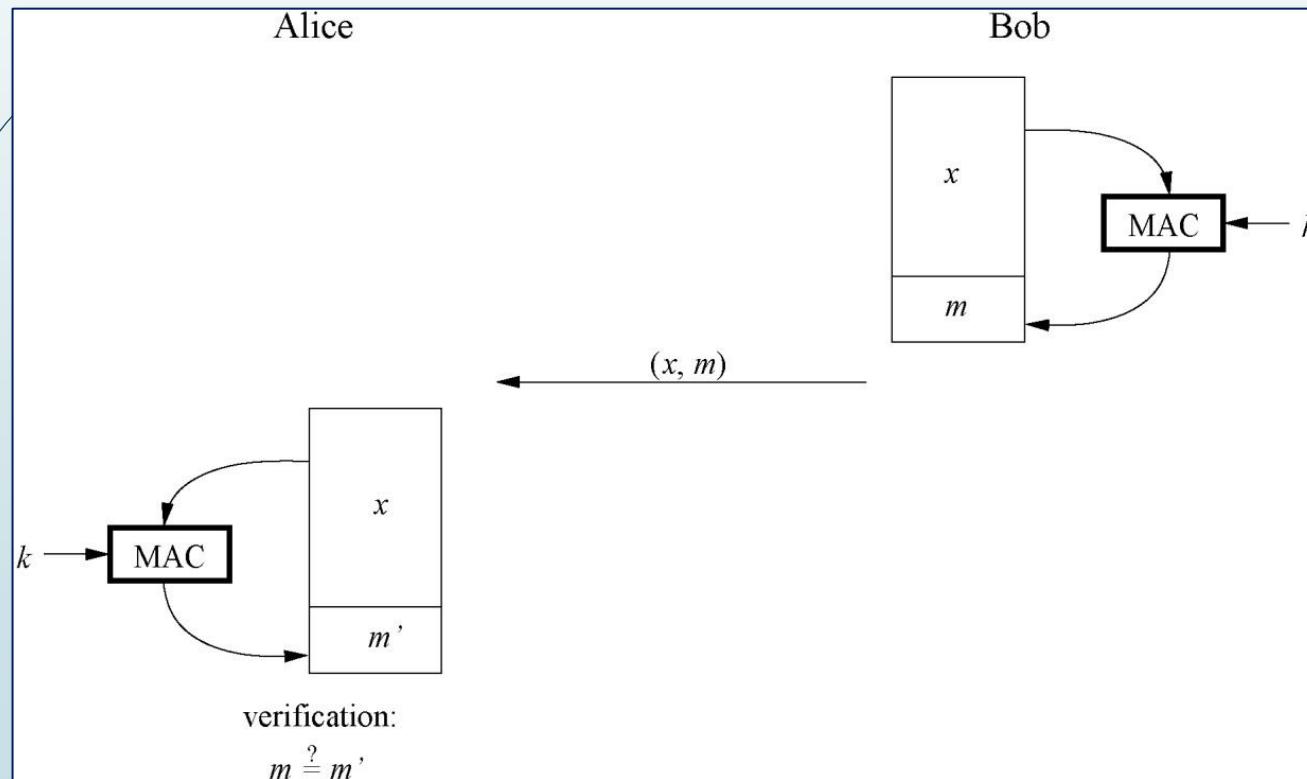


Content of this Chapter

- **The principle behind MACs**
- The security properties that can be achieved with MACs
- How MACs can be realized with hash functions and with block ciphers

💡 Principle of Message Authentication Codes

- Similar to digital signatures, MACs append an authentication tag to a message
- MACs use a **symmetric key** ' k ' for generation and verification
- Computation of a MAC: $m = \text{MAC}_k(x)$



Message Authentication Codes (MAC's)



Content of this Chapter

- 
- The principle behind MACs
 - **The security properties that can be achieved with MACs**
 - How MACs can be realized with hash functions and with block ciphers

Properties of Message Authentication Codes

1. Cryptographic checksum

A MAC generates a cryptographically secure authentication tag for a given message.

2. Symmetric

MACs are based on secret symmetric keys. The signing and verifying parties must share a secret key.

3. Arbitrary message size

MACs accept messages of arbitrary length.

4. Fixed output length

MACs generate fixed-size authentication tags.

5. Message integrity

MACs provide message integrity: Any manipulations of a message during transit will be detected by the receiver.

6. Message authentication

The receiving party is assured of the origin of the message.

7. No nonrepudiation

Since MACs are based on symmetric principles, they do not provide nonrepudiation.

Information Assurance and Security

LECTURE - 8 : ACCESS CONTROL

Reading Assignment:

- W. Stallings and L. Brown, “Computer Security, Principles and Practice,, Pearson, Chapter 4.
- Other related materials

Access Control

ITU-T Recommendation X.800's definition

Access control is the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

Access control is a critical element in computer security because the main objective of computer security is

- To prevent unauthorized users from accessing resources
- To prevent legitimate users from accessing unauthorized resources
- To enable users to access resources in an authorized way

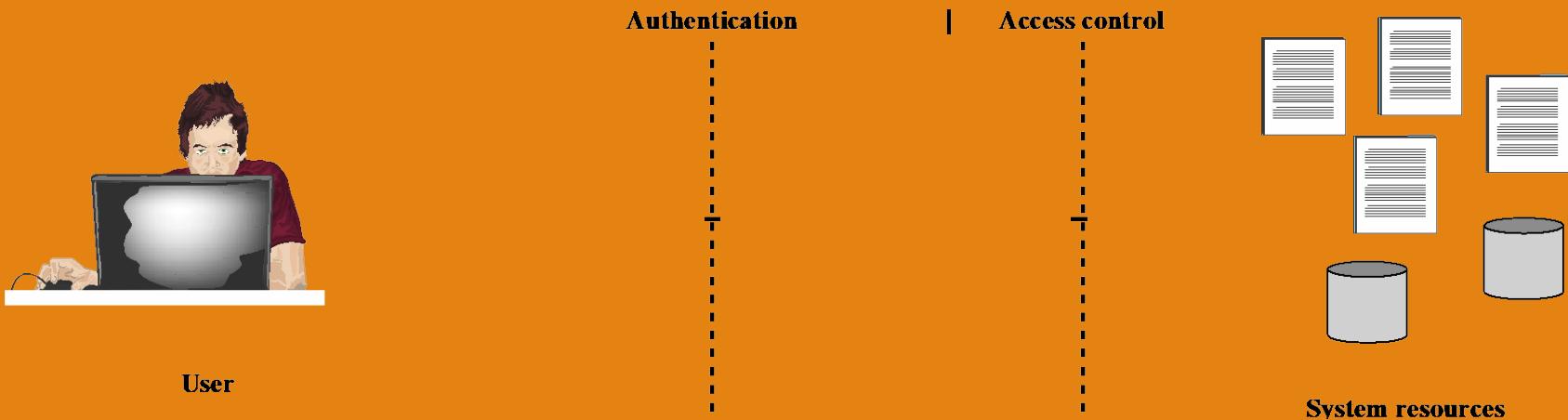


Figure 4.1 Relationship Among Access Control and Other Security Functions

Access Control Policies

An access control policy, which can be embodied in an authorization database, dictates what types of access are permitted, under what circumstances, and by whom. Access control policies are generally grouped into the following categories:

- **Discretionary Access Control (DAC)**
- **Mandatory Access Control (MAC)**
- **Role-Based Access Control(RBAC)**

Discretionary Access Control (DAC)

Controls access based on the **identity of the requestor** and on **access rules (authorizations)** stating what requestors are (or are not) allowed to do. This policy is termed discretionary because an entity might have access rights that permit the entity, by its own volition, to enable another entity to access some resource. (*E.g. UNIX RWX*)

Access Control Policies

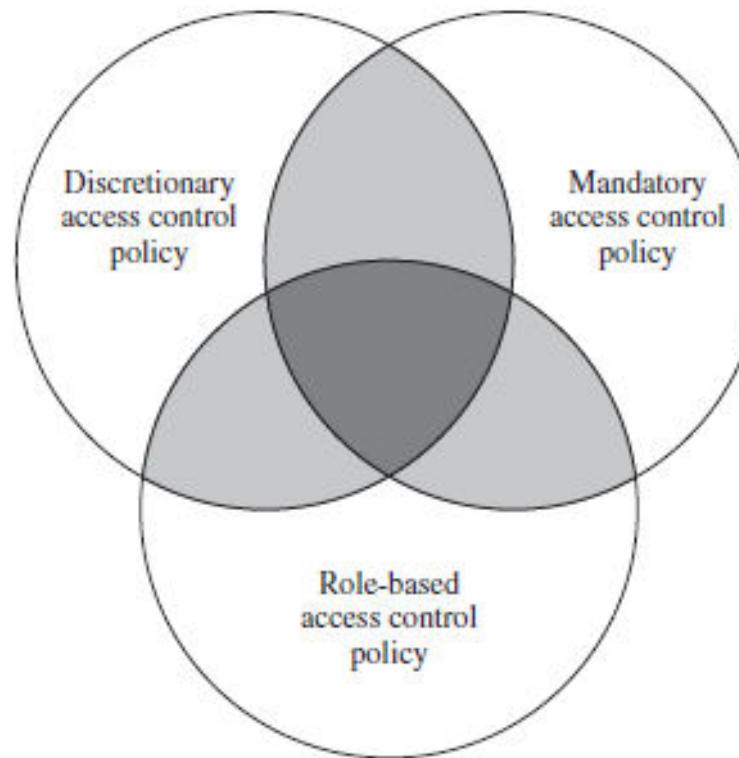
Mandatory access control (MAC):

Controls access based on comparing **Security labels** (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources). This policy is termed mandatory because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource. (*E.g. SELinux*)

Role-based access control (RBAC):

Controls access based on the **roles** that users have within the system and on rules stating what accesses are allowed to users in given roles. (*E.g. Github*)

Access Control Policies



DAC, MAC, and RBAC are not mutually exclusive. A system may implement two or even three of these policies for some or all types of access.

Elements of Access Control

- **Subject: an entity that accesses object**

A subject is a application or a user that is represented by a process in the system that takes on the user's attribute, e.g., access right

Three classes of subject: owner, group, world

- **Object: the resource which access is to be controlled**

Example: records, files, mailbox, program, messages

- **Access Right: the way a subject may access an object**

Access right includes: read, write, execute, delete, create, search

Discretionary Access Control

General access control in OS uses an access matrix

- One dimension (column) consists of subjects that need to access objects
- The other dimension (row) lists the objects that can be accessed
- Each entry in the matrix contains access rights of the subject in that row for the object in that column

Access Matrix

| | | OBJECTS | | | |
|----------|--------|----------------------|----------------------|----------------------|----------------------|
| | | File 1 | File 2 | File 3 | File 4 |
| SUBJECTS | User A | Own Read Write | | Own Read Write | |
| | User B | Read | Own Read Write | Write | Read |
| | User C | Read Write | Read | | Own Read Write |

(a) Access matrix

ACLs and Capability Tickets

Access matrix is usually sparse, and implemented by decomposing it into one or two ways:

- By columns resulting in Access Control Lists (ACLs) for all objects
- By rows resulting in capability list/tickets for all subjects/users

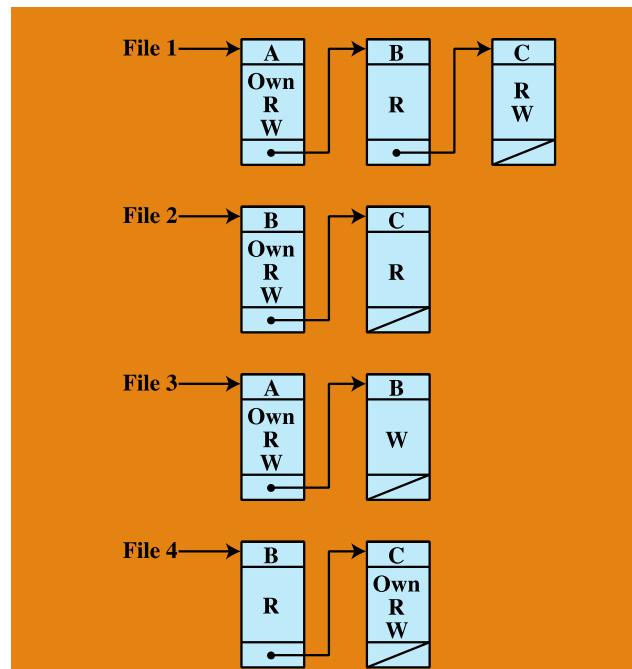
Each list for an object in ACL lists users and their access rights to access the object

- ACL may contain a default or public entry to allow users that are not explicitly listed to have a default access right
- Access rights should follow the least privilege or read-only access
- Elements in the list can be an individual or group users

Access Control Lists (ACLs)

ACL is efficient when we want to know which subjects have what access rights to a particular object

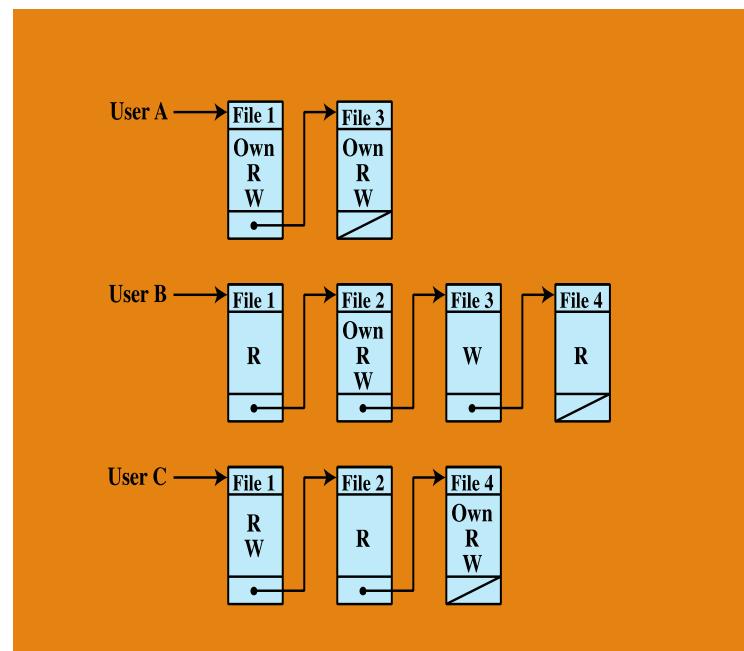
- However, it is harder to determine what access rights a specific user has on which objects



Capability Tickets

Each capability ticket refers to what access rights a particular user has on the objects in the list

- Each user has a number of tickets and they can loan or give the tickets to other users



Capability Tickets

Tickets may be spread around the system

- The tickets cause a greater security problem than ACL

The OS must protect and guarantee the integrity of each ticket; the ticket must be unforgeable

- OS keeps all tickets for the user in a memory region inaccessible by users
- Users must use a system call to request for their tickets

For distributed system, the ticket is in a form of a token

- A token can be a large random password, or a cryptographic message authentication code whose value is verified by the corresponding resource when requesting for access. (*E.g. OAuth token*)

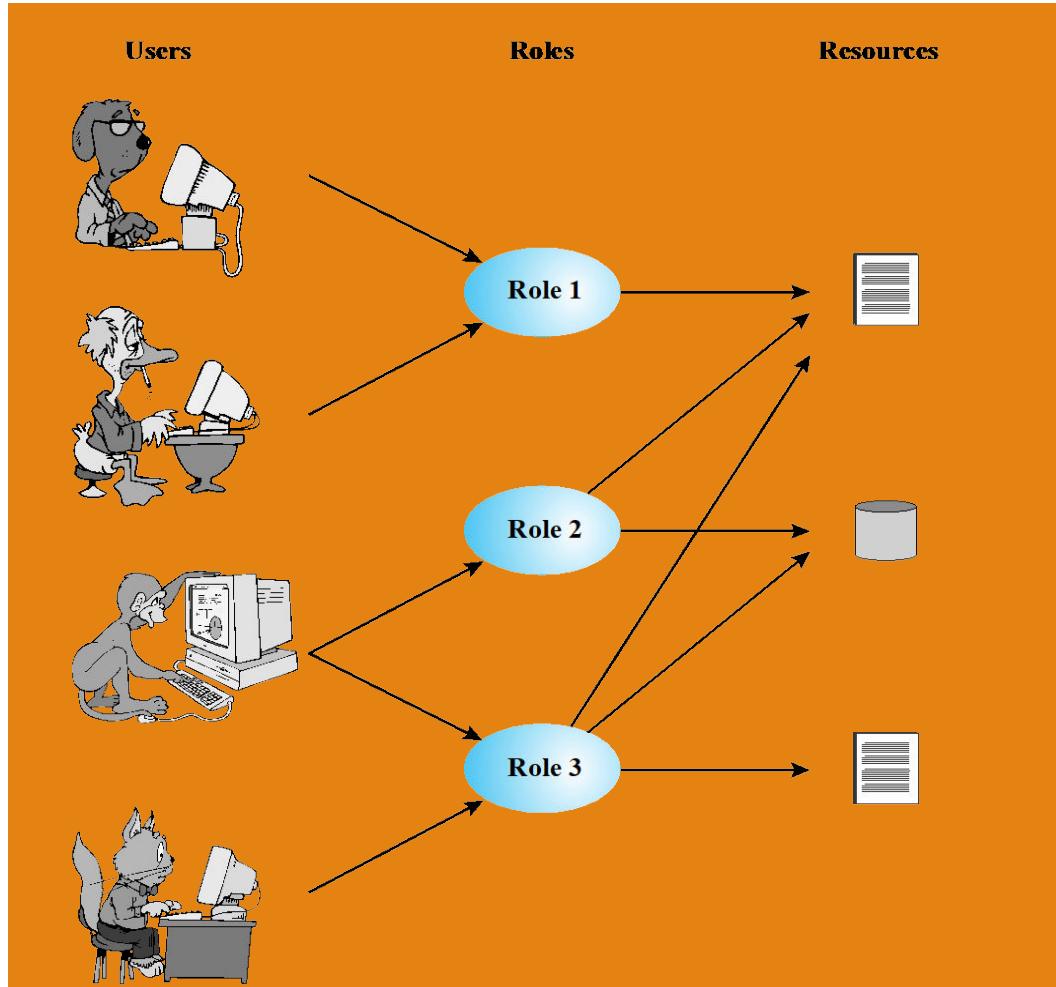


Role-based Access Control (RBAC)

RBAC defines the access rights based on the roles the users assume in the system rather than the user's identity like in DAC

- Role is a job function in the organization
- RBAC assign rights to the roles, not the users
- Users are assigned roles either statically or dynamically
- The relationship between users and roles are many-to-many

Role-based Access Control (RBAC)



Role-based Access Control (RBAC)

Access matrix representation can be used to describe the key elements of RBAC;

| | R ₁ | R ₂ | ... | R _n |
|----------------|----------------|----------------|-----|----------------|
| U ₁ | X | | | |
| U ₂ | X | | | |
| U ₃ | | X | | X |
| U ₄ | | | | X |
| U ₅ | | | | X |
| U ₆ | | | | X |
| ⋮ | | | | |
| U _n | X | | | |

| | OBJECTS | | | | | | | | |
|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
| | R ₁ | R ₂ | R _n | F ₁ | F ₁ | P ₁ | P ₂ | D ₁ | D ₂ |
| ROLES | control | owner | owner control | read * | read owner | wakeup | wakeup | seek | owner |
| R ₁ | | | | | | | | | |
| R ₂ | | control | | write * | execute | | | owner | seek * |
| ⋮ | | | | | | | | | |
| R _n | | | control | | write | stop | | | |

Access Control Requirements

Concepts and features that should be supported by an access control system

- Reliable Input
- Support for fine and coarse specifications
- Least privilege
- Separation of duty
- Open and Closed policy
- Policy combination and conflict resolution
- Administrative policy
- Dual control

Access Control Requirements

Reliable Input

An access control system assumes that a user is authentic; thus, an authentication mechanism is needed as a front end to an access control system. Other inputs to the access control system must also be reliable. For example, some access control restrictions may depend on an address, such as a source IP address or medium access control address. The overall system must have a means of determining the validity of the source for such restrictions to operate effectively.

Access Control Requirements

Support for fine and coarse specifications : The access control system should support fine-grained specifications, allowing access to be regulated at the level of individual records in files, and individual fields within records. The system should also support fine-grained specification in the sense of controlling each individual access by a user rather than a sequence of access requests. System administrators should also be able to choose coarse-grained specification for some classes of resource access, to reduce administrative and system processing burden.

Least privilege : This is the principle that access control should be implemented so that each system entity is granted the minimum system resources and authorizations that the entity needs to do its work. This principle tends to limit damage that can be caused by an accident, error, or fraudulent or unauthorized act.

Access Control Requirements

Separation of duty : This is the practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process. This is primarily a policy issue; separation of duty requires the appropriate power and flexibility in the access control system, including least privilege and fine-grained access control. Another useful tool is history-based authorization, which makes access dependent on previously executed accesses.

Open and closed policies: The most useful, and most typical, class of access control policies are closed policies. In a **closed policy**, only accesses that are **specifically authorized are allowed**. In some applications, it may also be desirable to allow an open policy for some classes of resources. In an **open policy**, authorizations **specify which accesses are prohibited; all other accesses are allowed**.

Access Control Requirements

Policy combinations and conflict resolution: An access control mechanism may apply multiple policies to a given class of resources. In this case, care must be taken that there are no conflicts such that one policy enables a particular access while another policy denies it. Or, if such a conflict exists, a procedure must be defined for conflict resolution.

Administrative policies: As was mentioned, there is a security administration function for specifying the authorization database that acts as an input to the access control function. Administrative policies are needed to specify who can add, delete, or modify authorization rules. In turn, access control and other control mechanisms are needed to enforce the administrative policies.

Dual control: When a task requires two or more individuals working in tandem.

Information Assurance and Security

LECTURE - 9 : USER AUTHENTICATION

Reading Assignment:

- W. Stallings and L. Brown, “Computer Security, Principles and Practice,, Pearson, Chapter 3.
- Other related materials

Authentication - Definition (RFC 2828)

The process of verifying an identity claimed by or for a system entity. An authentication process consists of two steps:

- **Identification step:** Presenting an identifier to the security system. (Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service.)
- **Verification step:** Presenting or generating authentication information that corroborates the binding between the entity and the identifier.

Identification

An ID provides security because

- The ID determines if the user is authorized to access the system
- The ID determines the privileges given to the user
 - e.g., superuser has the highest privilege while guest/anonymous has the least privilege
- The ID is used as discretionary access control
 - e.g., access rights (read, write, execute) to a file

Vulnerabilities of I&A

Some of I&A's more common vulnerabilities that may be exploited to gain unauthorized system access include:

- Weak authentication methods
- The potential for users to bypass the authentication mechanism
- The lack of confidentiality and integrity for the stored authentication information
- The lack of encryption for authentication and protection of information transmitted over a network
- The user's lack of knowledge on the risks associated with sharing authentication elements (e.g., passwords, security tokens)

Means of Authentication

There are four general means of authenticating a user's identity, which can be used alone or in combination:

- **Something the individual knows:** Examples includes a password, a personal identification number (PIN), or answers to a prearranged set of questions.
- **Something the individual possesses:** Examples include electronic key cards, smart cards, and physical keys. This type of authenticator is referred to as a token.
- **Something the individual is (static biometrics):** Examples include recognition by fingerprint, retina, and face.
- **Something the individual does (dynamic biometrics):** Examples include recognition by voice pattern, handwriting characteristics, and typing rhythm.

Password-Based Authentication

Most widely used means of authentication

- The system maintains a password file indexed by ID
- Typically the system stores one-way hash function of the password
- When a user enters a password, the system compares it with the password for the ID in the file

Authentication using passwords is vulnerable to attacks



Vulnerabilities of Passwords

Offline dictionary attack

- This attack is possible if the hacker can gain access to the system's password file and compares the password hash against the hashes of common words
- Countermeasures : controls to prevent unauthorized access to the password file, intrusion detection measures to identify a compromise, and rapid reissuance of passwords should the password file be compromised.

Specific account attack:

- The attacker targets a specific account and submits password guesses until the correct password is discovered.
- Countermeasures : account lockout mechanism, which locks out access to the account after a number of failed login attempts. Typical practice is no more than five access attempts.

Vulnerabilities of Passwords

Popular password attack

- Use a popular password and try it against a wide range of user IDs. A user's tendency is to choose a password that is easily remembered
- Countermeasures: Password policies and scanning the IP addresses of authentication requests and client cookies for submission patterns.

Password guessing against single user

- The attacker attempts to gain knowledge about the account holder and system password policies and uses that knowledge to guess the password.
- Countermeasures: training in and enforcement of password policies that make passwords difficult to guess. Such policies address the secrecy, minimum length of the password, character set, prohibition against using well-known user identifiers, and length of time before the password must be changed.

Vulnerabilities of Passwords

Exploiting user mistakes

- User is more likely to write it down because it is difficult to remember. A user may intentionally share a password.
- Also, attackers are frequently successful in obtaining passwords by using social engineering tactics that trick the user or an account manager into revealing a password. Many computer systems are shipped with preconfigured passwords for system administrators.
- Countermeasures: user training, intrusion detection, and simpler passwords combined with another authentication mechanism.

Workstation hijacking

- The attacker waits until a logged-in workstation is unattended.
- Countermeasures : automatically logging the workstation out after a period of inactivity and Intrusion detection schemes can be used to detect changes in user behavior.

Vulnerabilities of Passwords

Exploiting multiple password use

- Attacks can also become much more effective or damaging if different network devices share the same or a similar password for a given user.
- Countermeasures: policy that forbids the same or similar password on particular network devices.

Electronic monitoring

- Passwords communicated across a network to log on to a remote system is vulnerable to eavesdropping.
- Simple encryption will not fix this problem, because the encrypted password is, in effect, the password and can be observed and reused by an adversary

Multi-factor Authentication

Using A combination of more than one method, such as token and password (or personal identification number [PIN] or token and biometric device)

Two-factor authentication is a security process in which the user provides **two** means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code

Single Sign-On (SSO)

SSO can generally be defined as the process for consolidating all organization platform-based administration, authentication and authorization functions into a single centralized administrative function. This function would provide the appropriate interfaces to the organization's information resources, which may include:

- Client-server and distributed systems
- Mainframe systems
- Network security including remote access mechanisms

SSO Advantages

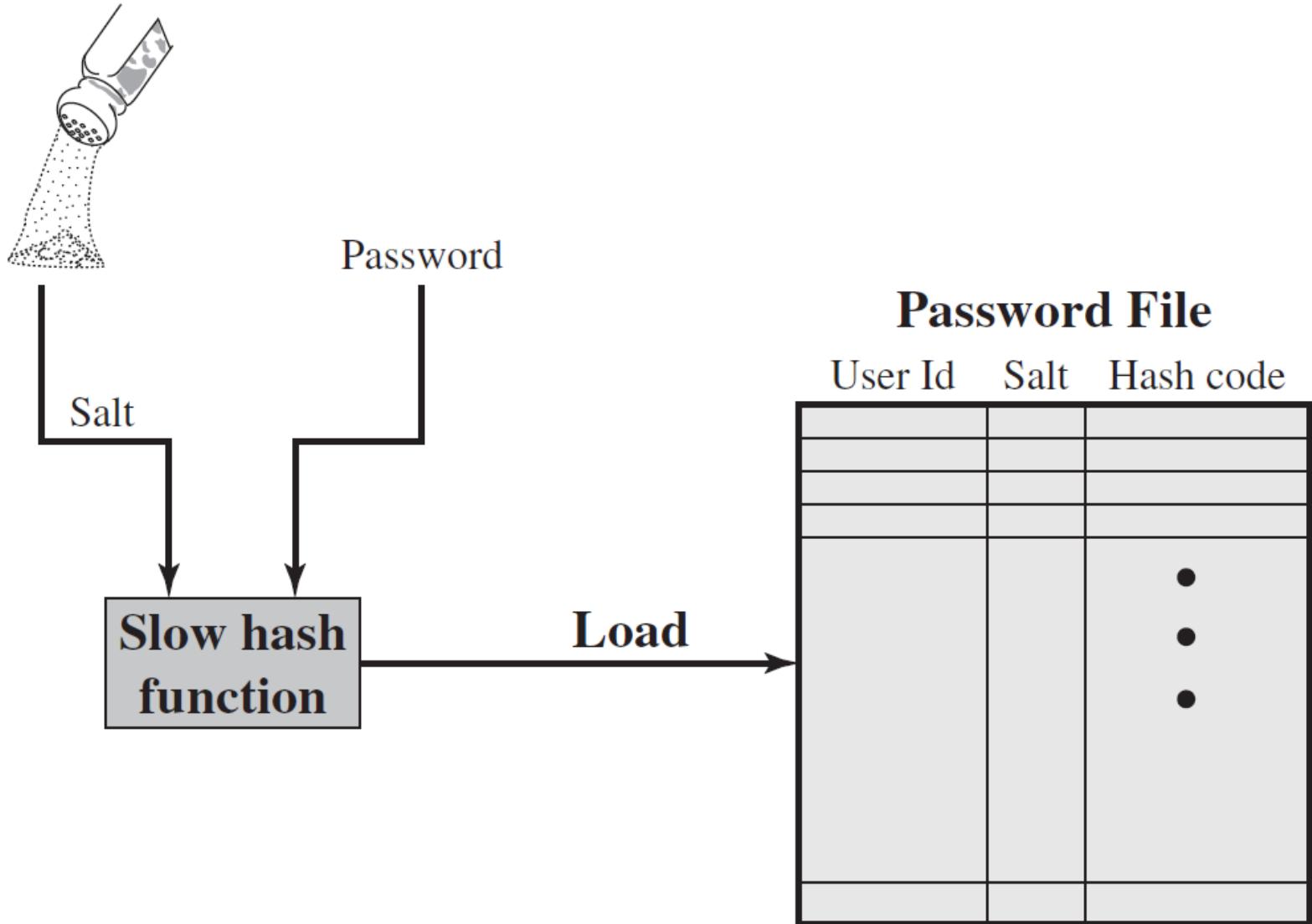
- Multiple passwords are no longer required; therefore, a user may be more inclined and motivated to select a stronger password.
- It improves an administrator's ability to manage users' accounts and authorizations to all associated systems.
- It reduces administrative overhead in resetting forgotten passwords over multiple platforms and applications.
- It reduces the time taken by users to log into multiple applications and platforms.

SSO Disadvantages

- Support for all major operating system environments is difficult. SSO implementations will often require a number of solutions integrated into a total solution for an enterprise's IT architecture.
- The costs associated with SSO development can be significant when considering the nature and extent of interface development and maintenance that may be necessary.
- The centralized nature of SSO presents the possibility of a single point of failure and total compromise of an organization's information assets. For this reason, "strong authentication" in the form of complex password requirements and the use of biometrics is frequently implemented.

Hashed passwords with salt

- Most systems, e.g., Linux, store hashed passwords and a salt value for better security
- Steps to store a password:
 - Given a password (selected by user or assigned by system), the system generates a fixed length pseudorandom/random number, called salt
 - Older system uses time when the password is created to generate the salt
 - Use hash function to generate a fixed length hashed code of the password and its salt
 - Store the hashed code and a plaintext copy of the salt in the password file



(a) Loading a new password

Hashed passwords with salt

- Steps to verify a password:
 - Given a user ID and a password, the system uses the ID to retrieve the plaintext salt and the encrypted password
 - Use the salt and the supplied password as input to the encryption function
 - If the result matches the stored encrypted value, the password is accepted

Password File

User Id

User Id Salt Hash code

| User Id | Salt | Hash code |
|---------|------|-----------|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Select

Salt

Password

**Slow hash
function**

Hashed password

Compare

(b) Verifying a password

Purposes of Using Salt

- **To prevent duplicate passwords in the password file**
Each password is assigned a different salt value. Thus even if two users use the same password, the stored hashed passwords would be different
- **To significantly increases the difficulty of offline dictionary attacks**
A b bit salt will increase the number of possible passwords by a factor of 2^b , and thus guessing password would be harder
- **To makes almost impossible to find out if a person use the same password on two or more systems**

Remote user authentication

Remote user authentication raises additional security threats such as eavesdropping and replay attack

- The counter measure generally relies on challenge-response protocol, such as Kerberos

Challenge-response protocol

- **Steps of a simple challenge-response protocol**
- User transmits his/her ID to the remote host
- The host generates a random number r , called a nonce, and returns it to the user. The host also specifies two functions, a hash function $h()$ and $f()$ to be used for the user's response
 - The host keeps function $h()$ for the password of each of its users $U \rightarrow h(P(U))$
 - This is the challenge
- The user must send a correct response $f(r', h(P'))$ to the host
 - $r'=r$ and P' is the user's password
- The host calculates $f(r, h(P(U)))$ and compares it with the received $f(r', h(P'))$

Challenge-Response Protocol

| Client | Transmission | Host |
|---------------------------------------|------------------------------|--|
| U , user | $U \rightarrow$ | |
| | $\leftarrow \{r, h(), f()\}$ | random number $h()$, $f()$, functions |
| P' password r' , return of r | $f(r', h(P')) \rightarrow$ | |
| | \leftarrow yes/no | if $f(r', h(P')) =$ $f(r, h(P(U)))$ then yes else no |

(a) Protocol for a password

- From W. Stallings and L. Brown, “Computer Security, Principles and Practice, 2nd edition

Table 3.4 Some Potential Attacks, Susceptible Authenticators, and Typical Defenses

| Attacks | Authenticators | Examples | Typical Defenses |
|-----------------------------------|----------------------------|--|--|
| Client attack | Password | Guessing; exhaustive search | Large entropy; limited attempts |
| | Token | Exhaustive search | Large entropy; limited attempts, theft of object requires presence |
| | Biometric | False match | Large entropy; limited attempts |
| Host attack | Password | Plaintext theft, dictionary/exhaustive search | Hashing; large entropy; protection of password database |
| | Token | Passcode theft | Same as password; 1-time passcode |
| | Biometric | Template theft | Capture device authentication; challenge response |
| Eavesdropping, theft, and copying | Password | "Shoulder surfing" | User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication |
| | Token | Theft, counterfeiting hardware | Multifactor authentication; tamper resistant/evident token |
| | Biometric | Copying (spoofing) biometric | Copy detection at capture device and capture device authentication |
| Replay | Password | Replay stolen password response | Challenge-response protocol |
| | Token | Replay stolen passcode response | Challenge-response protocol; 1-time passcode |
| | Biometric | Replay stolen biometric template response | Copy detection at capture device and capture device authentication via challenge-response protocol |
| Trojan horse | Password, token, biometric | Installation of rogue client or capture device | Authentication of client or capture device within trusted security perimeter |
| Denial of service | Password, token, biometric | Lockout by multiple failed authentications | Multifactor with token |

From W. Stallings and L. Brown, "Computer Security, Principles and Practice, 2nd edition

Password Selection Strategies

- User education
- Computer-generated passwords
- Reactive password checking
- Proactive password checking

Disaster Recovery & Business Continuity

By Kavinga Yapa Abeywardena

Sri Lanka Institute of Information Technology (SLIIT)



Background

- Information Systems are **vulnerable to a variety of disruptions.**
 - Mild: Temporary power outages, disk failures etc.
 - Severe: Equipment destruction, fire, natural disasters etc.
- Organizations must have the **ability to withstand hazards** and achieve business objectives through both gradual & sudden changes.
- Focus is on '**Availability**' component of the famous C.I.A
- We achieve this through '**Disaster Recovery Planning**' & '**Business Continuity Planning**'.

Background

FACT:

1 in 4 businesses never re-open their doors after a disaster



90% of businesses fail within 2 years after being struck by a disaster.



Business Continuity

When you're no longer afraid of losing everything, your focus can go back where it belongs: your business.

Background

TRENDING: Google Fi's winners & losers · New products of the week · Everest avalanche kills Google engineer · Resources/White Papers



NETWORKWORLD

Most read:



[Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Google+](#) | [RSS](#) | [Search](#)

[Home](#) > [Cloud Computing](#)

UPDATE: Amazon.com suffers outage: Nearly \$5M down the drain?

Amazon.com, the major online retailer, is down for 49 minutes



By Brandon Butler | [Follow](#)

Network World | Jan 31, 2013 4:55 PM PT

RELATED

Amazon outage started small, snowballed into 12-hour event

Amazon EBS failure brings down Reddit, Imgur, others

Definitions

- **Disaster Recovery Planning (DR)**
 - The process of rebuilding your operations or infrastructure after the disaster has passed.
- **Business Continuity Planning (BC)**
 - The activities required to keep your organization running during a period of displacement or interruption of normal operations.

NIST SP 800-34 provides guidelines for implementing DR & BC Strategies!

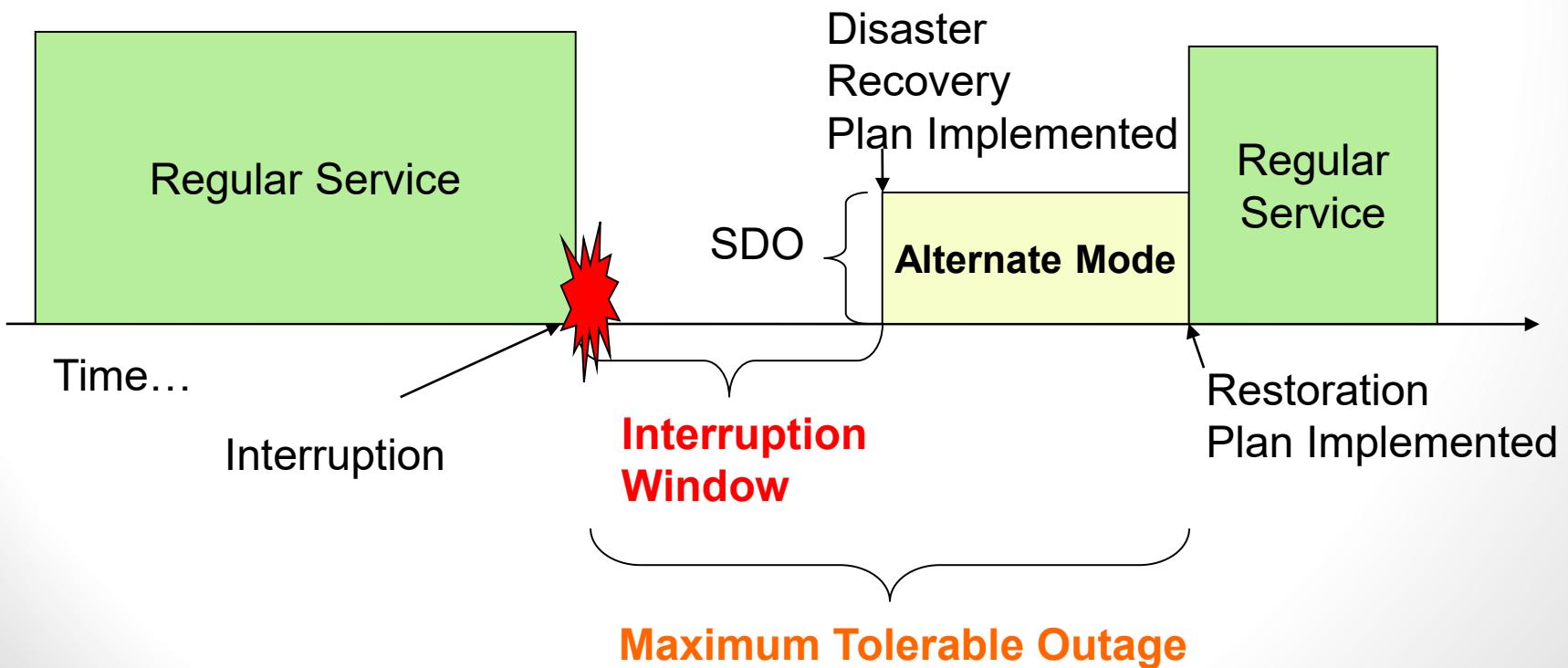
More than half of small to medium-sized enterprises affected by 9/11 did not trade again!

Recovery Time: Terms

Interruption Window: Time duration organization can wait between point of failure and service resumption

Service Delivery Objective (SDO): Level of service in Alternate Mode

Maximum Tolerable Outage: Max time in Alternate Mode



Business Continuity: Why?

- Advancement of IT means businesses nowadays depend heavily on information systems.
- Many businesses **cannot** survive without 24 x 7 operations of IS. (e.g. e-commerce)
- Therefore **traditional disaster recovery** plans which focus on restoring **centralized data & operations** center might not be sufficient.
- More comprehensive and robust **Business Continuity Plan** is needed for critical IS.

Business Continuity : When?

- Business continuity plan should exist in the event of following disruptions or disasters.
 - Equipment Failure
 - Disruption of power supply or telecommunication
 - Application failure or database corruption
 - Human error, Sabotage, Vandalism & Strikes
 - Malicious Software (Viruses, Worms, Trojan Horses) Attack
 - Hacking or any other internet attack
 - Social Unrest or Terrorism
 - Fire
 - Natural Disasters (Flood, Earthquake, Hurricanes etc.)

Business Continuity Planning : Team

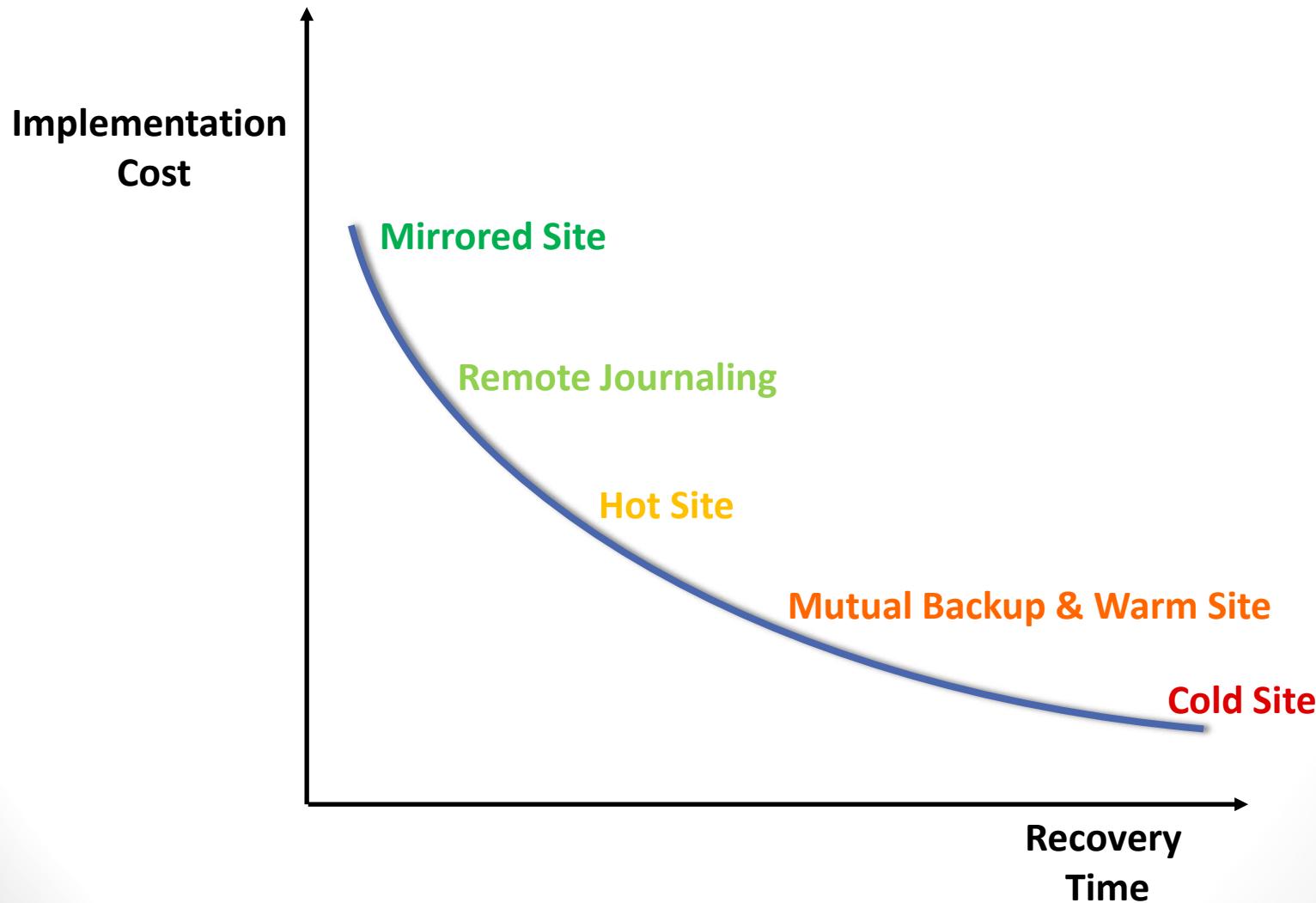
- Information systems have shifted from traditional centralized architecture to distributed and client/server architecture.
- IT department alone **cannot** achieve BCP success
- **All executives, managers, employees must participate**
- **BC/DR Coordinator** is responsible for maintaining the BCP
- He or She will carry out periodical reviews and redistribute document parts to relevant parties

Business Continuity Plan

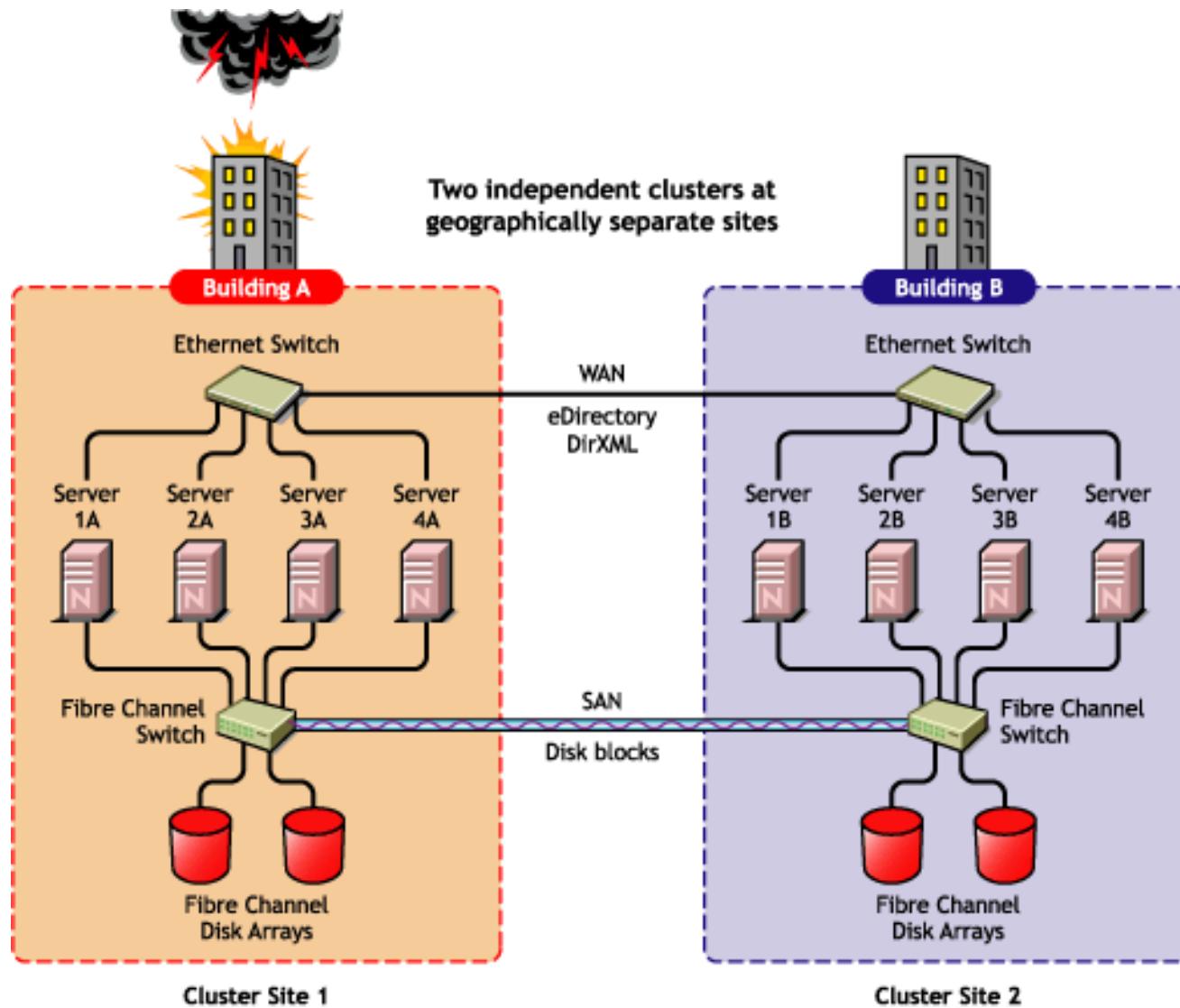
There are different methods an organization can achieve BC

- **Cold Site:** An empty facility located offsite with required infrastructure ready for installation in the event of a disaster.
- **Mutual Backup:** Two organizations with similar system configuration agreeing to serve as backup site to each other.
- **Hot Site:** A site with hardware, software & network installed and compatible to original site.
- **Remote Journaling:** Online transmission of data to backup systems periodically (every few hours) Minimizes loss of data and reduces recovery time.
- **Mirrored Site:** A site equipped with identical facilities to the original site with system mirroring capability. Data is mirrored & backed up immediately. Transparent Recovery.

Business Continuity Plan



Mirrored Site

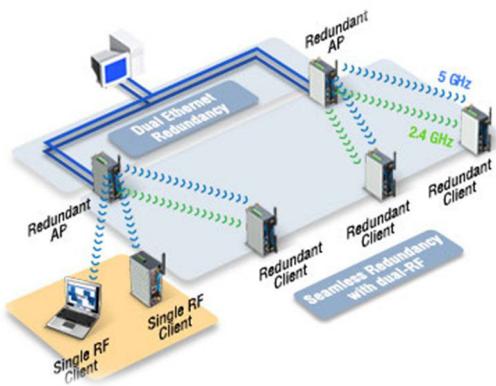


High Availability Solutions

- **RAID:** Local disk redundancy
- **Fault-Tolerant Server:** When primary server fails, backup server resumes service.
- **Distributed Processing:** Distributes load over multiple servers. If server fails, remaining server(s) attempt to carry the full load.
- **Storage Area Network (SAN):** disk network supports remote backups, data sharing and data migration between different geographical locations

Business Continuity Plan

Redundancy Vs. Cost



Vs.



- Right balance between BCP & Cost can be achieved.
- How? (Hint: You already know the answer)

DR & BC Providers

- Organizations can decide to use a facility delivered by a third party BC provider.
- However following areas of concerns should be considered.
 - Floor Space
 - Redundant Equipment
 - Redundant Network Capacity
 - Relationship with vendors to provide replacements or assistance
 - Budgetary Constraints
 - Skilled personnel availability

Preparing the BC Plan: Phases

1. Project Initiation

BC objectives are defined and the scope is identified. A committee will be appointed to draw up BC policies.

2. Business/Risk Analysis

Performing the ‘Risk Analysis’, Considering alternative BC strategies, Cost-benefit analysis, strategy selection & establish the budget.

3. Design & Development (Plan)

BC team is identified and responsibilities are assigned. Develop BC strategy and action plan and plan activation criteria.

4. Implementation (Plan)

Prepare disaster response & recovery procedures. Vendor contracts prepared and recovery resources are purchased. Ensure that recovery team on alert.

5. Testing - Exercise scenarios periodically & produce BC reports & evaluate.

6. Maintenance - Reviewing & constantly updating/improving the BC plan.

Concerns for a BCP/DR Plan

- Evacuation plan: People's lives always take **first priority**
- Disaster declaration: Who, how, for what?
- Responsibility: Who covers necessary disaster recovery functions
- Procedures for Disaster Recovery
- Procedures for Alternate Mode operation
 - Resource Allocation: During recovery & continued operation

*Copies of the plan should be off-site

Legally Obligated

- In some organizations business analysis [2] is **not** the only factor that determines BC Strategy.
- They are **legally obligated** by regulators to provide certain levels of protection to client data.
- Organizations who have direct **public interest** (such as banks) have legal obligations to implement DR & BC strategies.
- <http://www.slcert.gov.lk/> Provides consultancy on DR & BC planning.

[Click Here: Central Bank Guidelines for BC](#)

QUESTIONS ?



Thank
You





FIREWALLS, ACLS & NETWORK SECURITY

KAVINGA YAPA ABEYWARDENA



HAVE YOU EVER BEEN REFUSED ENTRY TO A PARTY?

AGENDA FOR TODAY

- Firewall
- Access Control Lists (ACLs)
 - Simple Packet Filtering
 - Stateful Packet Filtering
- Firewall Topologies

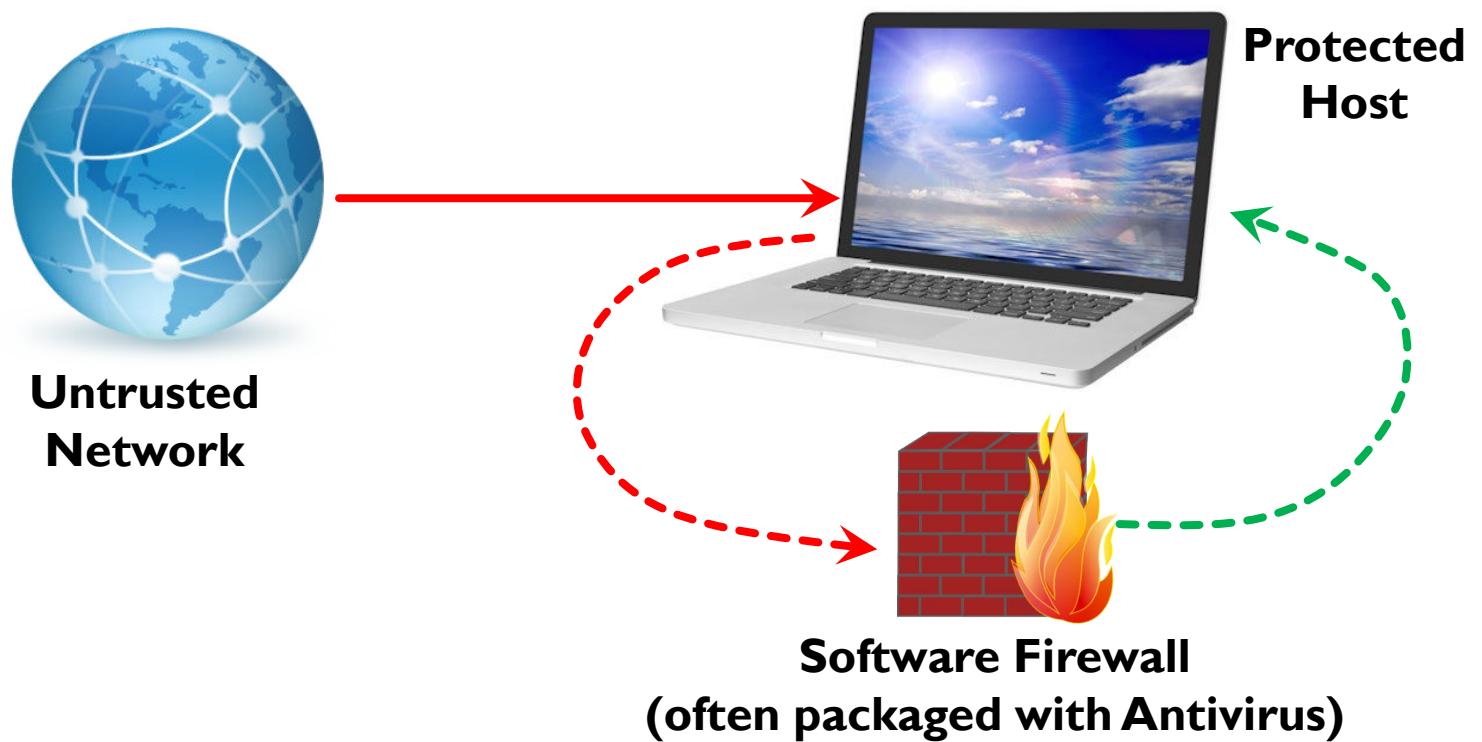


FIREWALL

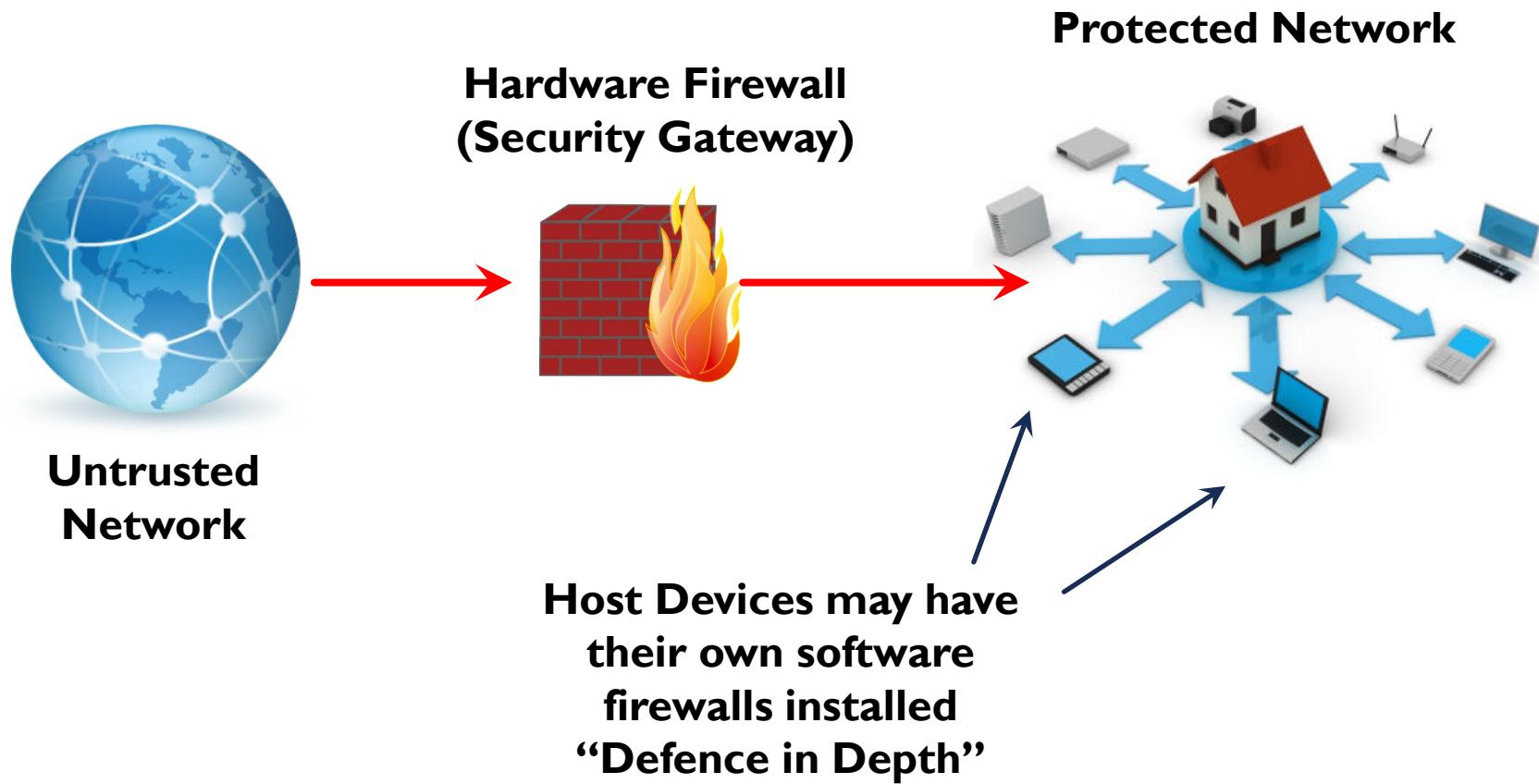
PART I

FIREWALL

- An Electronic “Checkpoint” between a (relatively) protected network/device and a (relatively) untrusted network.



FIREWALL



FIREWALL



- A system designed to prevent unauthorized access **to or from** a private network. Can be implemented in either hardware or software form, or a combination of both.
- “Setting up a firewall without a comprehensive security policy is like placing a steel door on a tent”

FIREWALL FUNCTIONS

■ “Primary” Functions

- Packet Filtering (Layers 3 and 4)
 - Stateful Inspection (Layers 3 and 4)
 - Application Layer Inspection
- 
- Using Access Control Lists (ACLs)

■ “Secondary” Functions

- Network Address Translation (NAT)
- VPN Tunnelling
- Proxy Server

PACKET FILTERING

PART 2

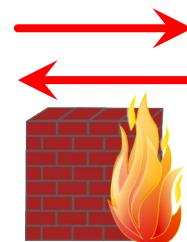


PACKET FILTERING

- Packet Filtering Firewalls can be based on
 - Source/Destination IP Address
 - Source/Destination Port Number
- Can specifically Permit/Deny
- Routers with additional functionality can also perform packet filtering
- Compares IP header with an Access Control List (ACL) to see if packet allowed to continue to next hop
- Inexpensive, flexible and fast

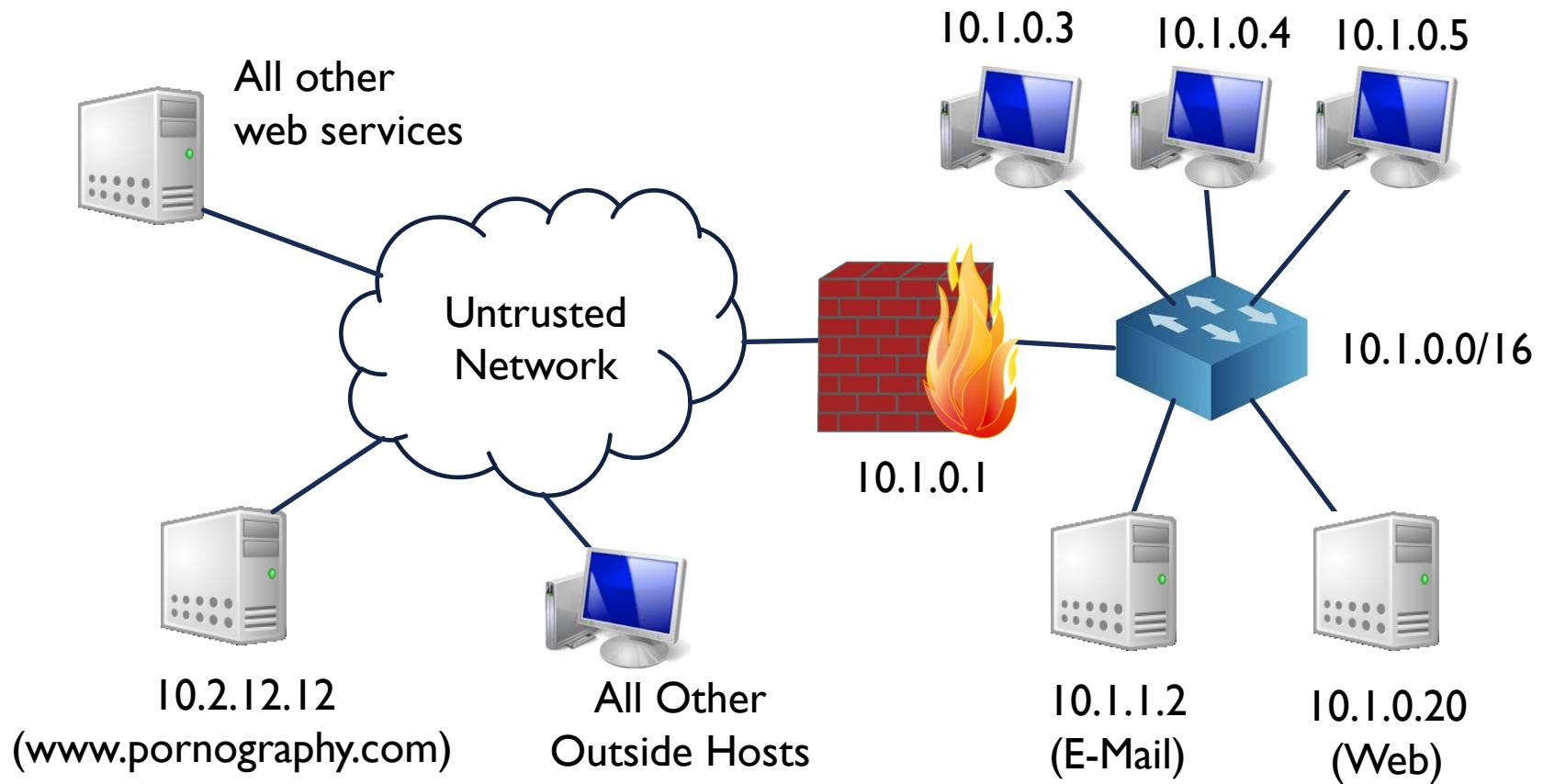
PACKET FILTERING USING ACL

- Apply an **Access Control List** to a specific interface
- Applied either **IN** or **out**
- One rule – one line
- Criteria checked sequentially
- Implicit deny at end (usually)
 - Clean Up Rule
- Protect firewall itself
 - Stealth Rule (usually first rule in list)
- Lines appear in order they are entered



CASE STUDY

The firewall protects subnet 10.1.0.0 /16. Internal hosts may access all external websites except 10.2.12.12. All external hosts may upload E-mail to 10.1.1.2 and access web pages on 10.1.0.20. All other activity is to be blocked. No connection may be made to the firewall itself.



| Rule | Source IP | Source Port | Dest. IP | Dest. Port | Protocol | Access |
|------|-----------|-------------|------------|------------|----------|--------|
| A | * | * | 10.1.0.1 | * | * | Deny |
| B | 10.1.0.0 | * | 10.2.12.12 | * | * | Deny |
| C | 10.1.0.0 | * | * | 80 | TCP | Allow |
| D | * | 80 | 10.1.0.0 | * | TCP | Allow |
| E | * | * | 10.1.1.2 | 25 | TCP | Allow |
| F | 10.1.1.2 | 25 | * | * | TCP | Allow |
| G | * | * | 10.1.0.20 | 80 | TCP | Allow |
| H | 10.1.0.20 | 80 | * | * | TCP | Allow |
| I | * | * | * | * | * | Deny |

Firewall Address (Stealth Rule)

Cleanup Rule

Port 25 – SMTP (E-Mail Upload)
Port 80 – HTTP (Web)

ACL BEST PRACTICES

- Don't forget protocols are usually bidirectional
 - Common mistakes include blocking return channel
- Reject all external packets that have internal addresses
 - Tunnelled attacks
- Reject all internal packets with external addresses
 - IP Spoofing attacks
- Log and don't respond to dropped packets
- Protect the protection system itself
 - “Stealth” rule – usually first in the list
- Deny everything that is not specifically allowed
 - “Cleanup” rule – sometimes included automatically

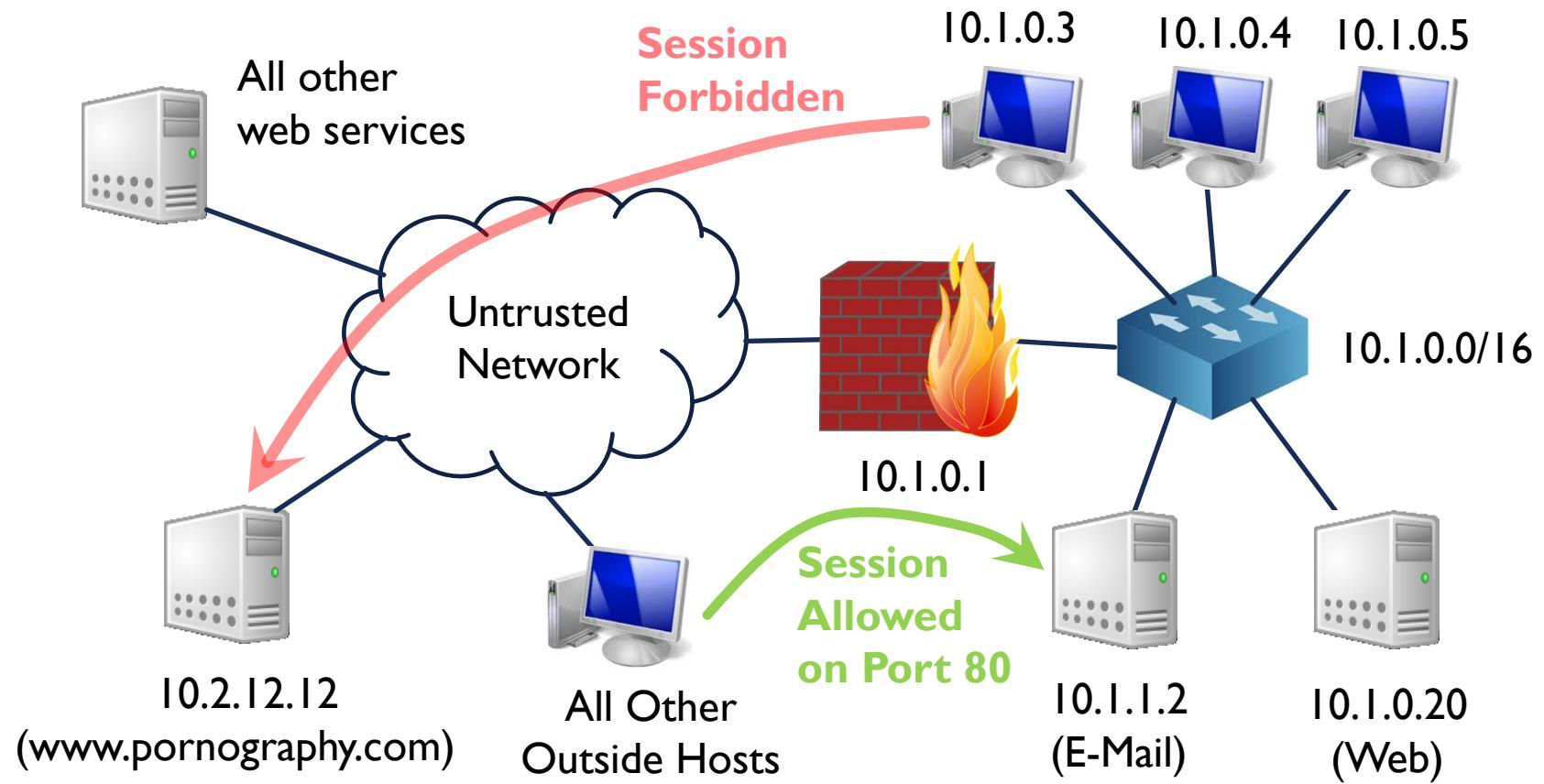
PACKET FILTERING LIMITATIONS

- Cannot keep track of sessions
- Cannot prevent IP Spoofing attacks
- A lot of applications dynamically allocate port numbers, which can cause problems
 - Both sides of a TCP connection can have random high-value port numbers.
- Although TCP traffic is difficult to deal with, UDP traffic is even harder
- Difficult and lengthy to configure
- Better Solution → Stateful Packet Inspection

STATEFUL PACKET INSPECTION

- Inspects packets and allows them if they belong to authorized sessions
 - Allowed sessions specified in stateful ACL
- Example:
 - Allow all packets belonging to “outgoing” connections
 - Sessions initiated from within the secure network
 - SYN packet allowed out but not in.
 - Returning ACK packet only allowed in response to SYN
 - Once session established, packets allowed even if server port is dynamically changed
 - Similarly incoming sessions allowed to particular hosts and ports
 - All other incoming traffic denied

STATEFUL ACL EXAMPLE



| Rule | Source IP | Source Port | Dest. IP | Dest. Port | Protocol | Access |
|------|-----------|-------------|------------|------------|----------|--------|
| A | * | * | 10.1.0.1 | * | * | Deny |
| B | 10.1.0.0 | * | 10.2.12.12 | * | * | Deny |
| C | 10.1.0.0 | * | * | 80 | TCP | Allow |
| D | * | * | 10.1.1.2 | 25 | TCP | Allow |
| E | * | * | 10.1.0.20 | 80 | TCP | Allow |
| F | * | * | * | * | * | Deny |

Firewall Address (Stealth Rule)

Cleanup Rule

Port 25 – SMTP (E-Mail)
 Port 80 – HTTP (Web)

FIREWALL BENEFITS

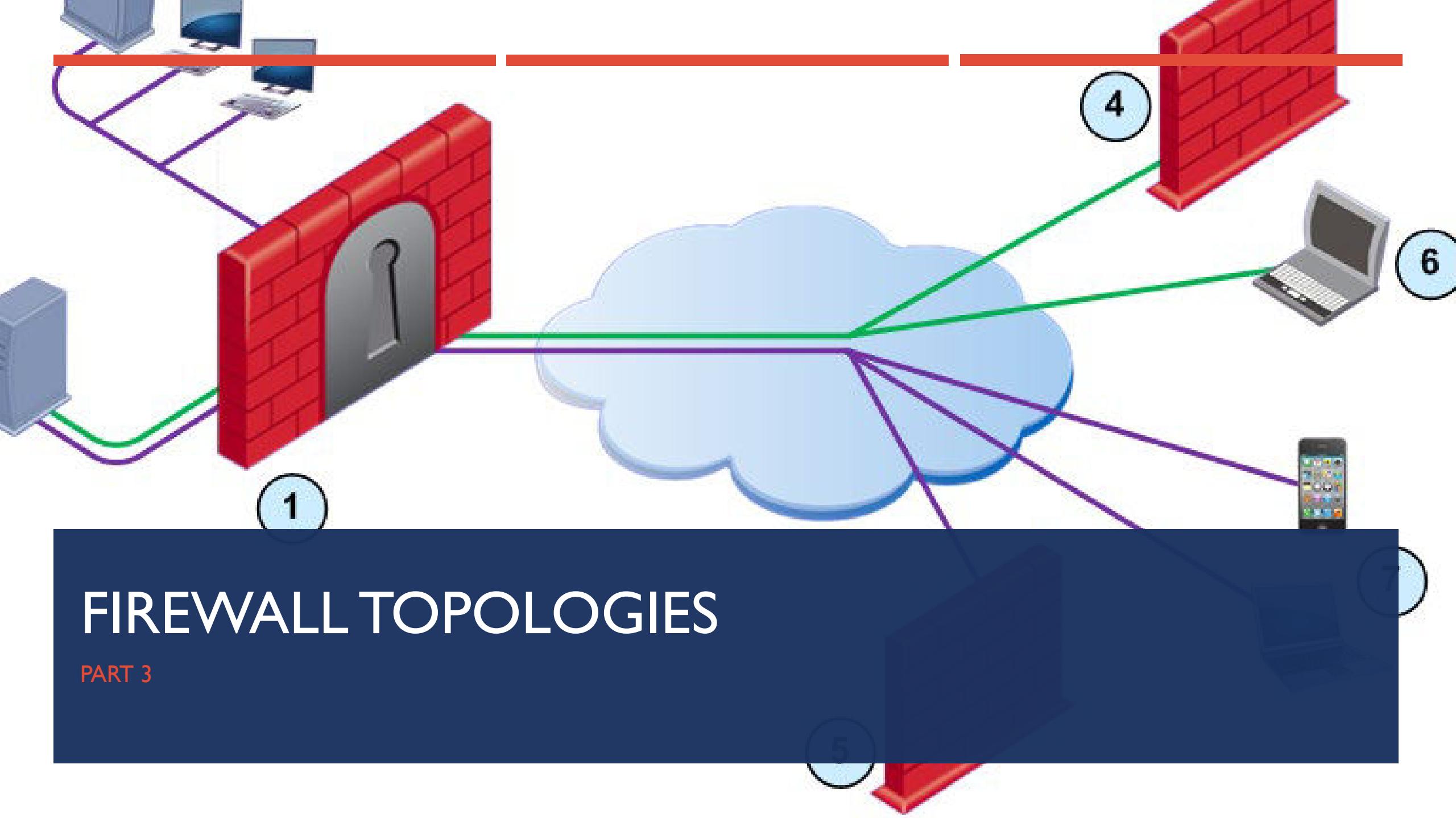
- Protect private network from outside attacks
 - Also separate departments
 - Protect connections between remote offices
- Can be used within private network
- Concentrate controls into one “choke point”
 - Like the gatehouse of a castle
- Can generate alarms when attacks are attempted
- Convenient location for other services
 - NAT
 - WWW/FTP Servers

FIREWALLS BENEFITS (CONTD.)

- DoS attack protection
 - Attack packets destined for a specific host can be stopped at the outer gateway of network
- Logging of attacks and traffic
- Blacklist maintenance
- Trace connections
 - Set maximum connections limit for single host
 - Prevents half-open connections (“SYN flood” attack)

FIREWALLS DRAWBACKS

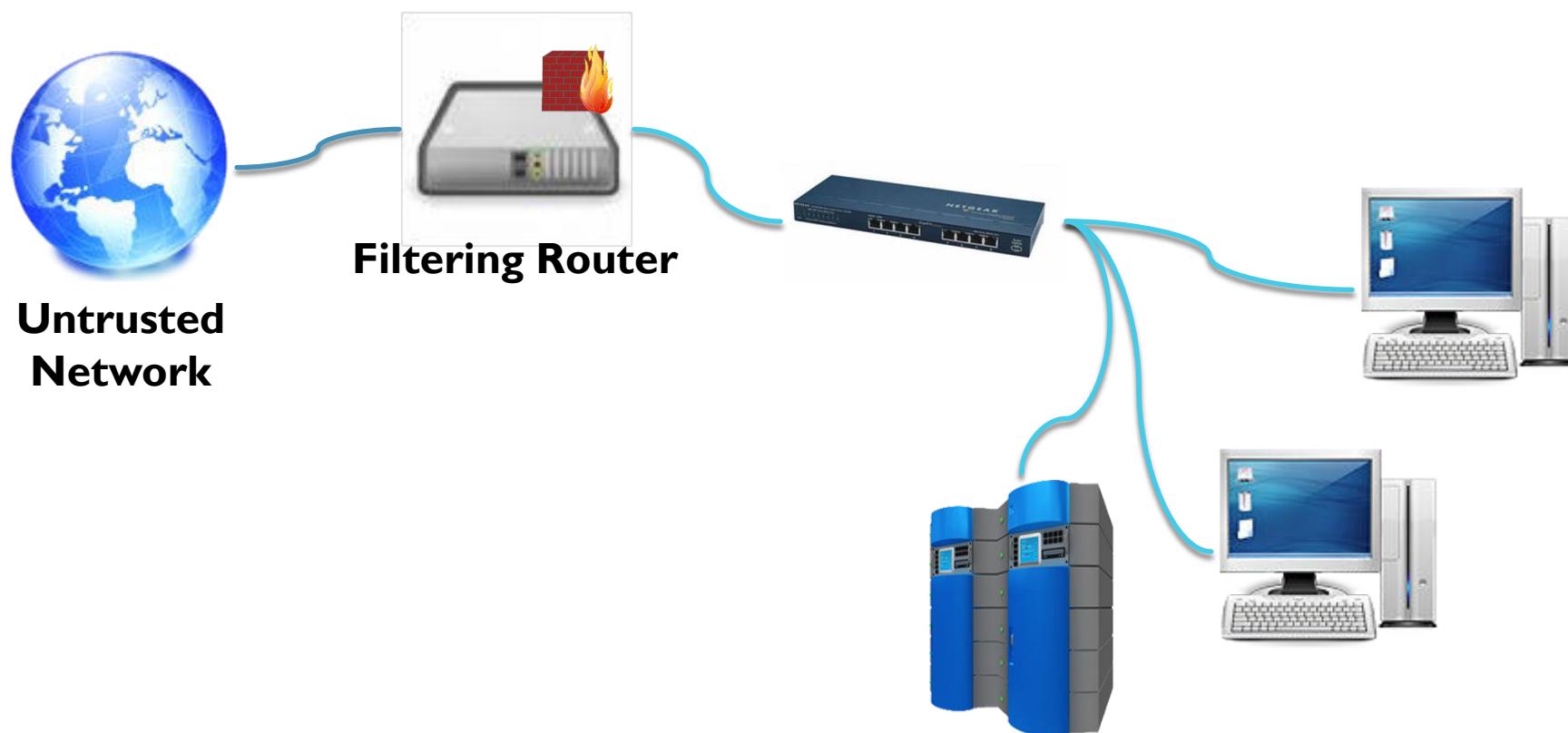
- Cannot protect against attacks that do not go through the firewall
- Cannot guard against traitors or accidental infringements
 - Though risk can be reduced by internal firewalls between departments etc.
- People are also a weak link...
 - Security of network is only as good as weakest link - one weak host weakens entire network



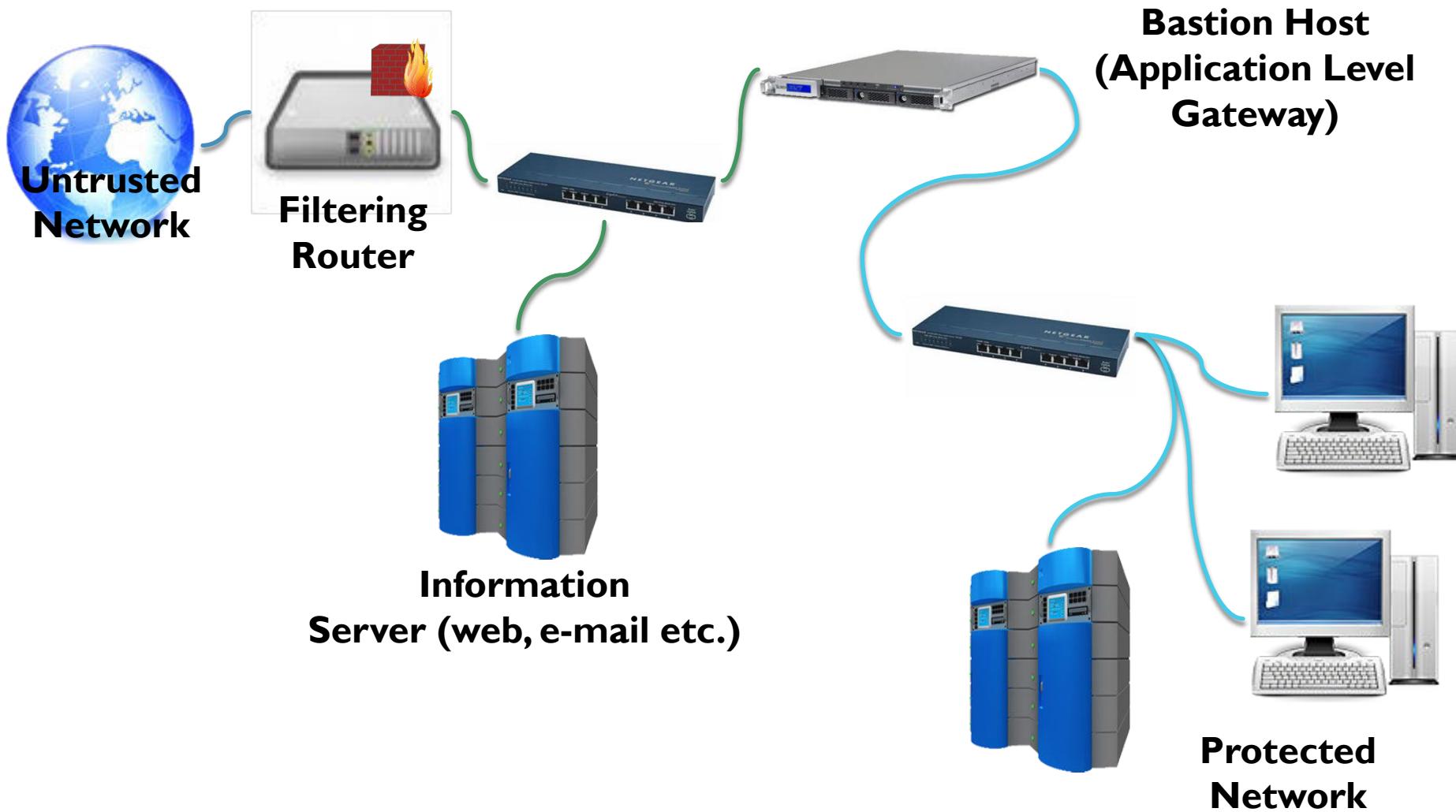
FIREWALL TOPOLOGIES

- Many different topologies
 - Have to find right balance: complexity vs. security
- Divide Organisation into zones
 - Firewall security specific to each one
- Number of decisions to be made:
 - Stance of Firewall
 - Philosophy behind the ACL/rulebase design
 - Example: “Everything not explicitly allowed is denied”
 - Overall Security Policy of Organisation
 - Financial cost of Firewall
 - Components or building blocks of the Firewall system

SIMPLEST TOPOLOGY



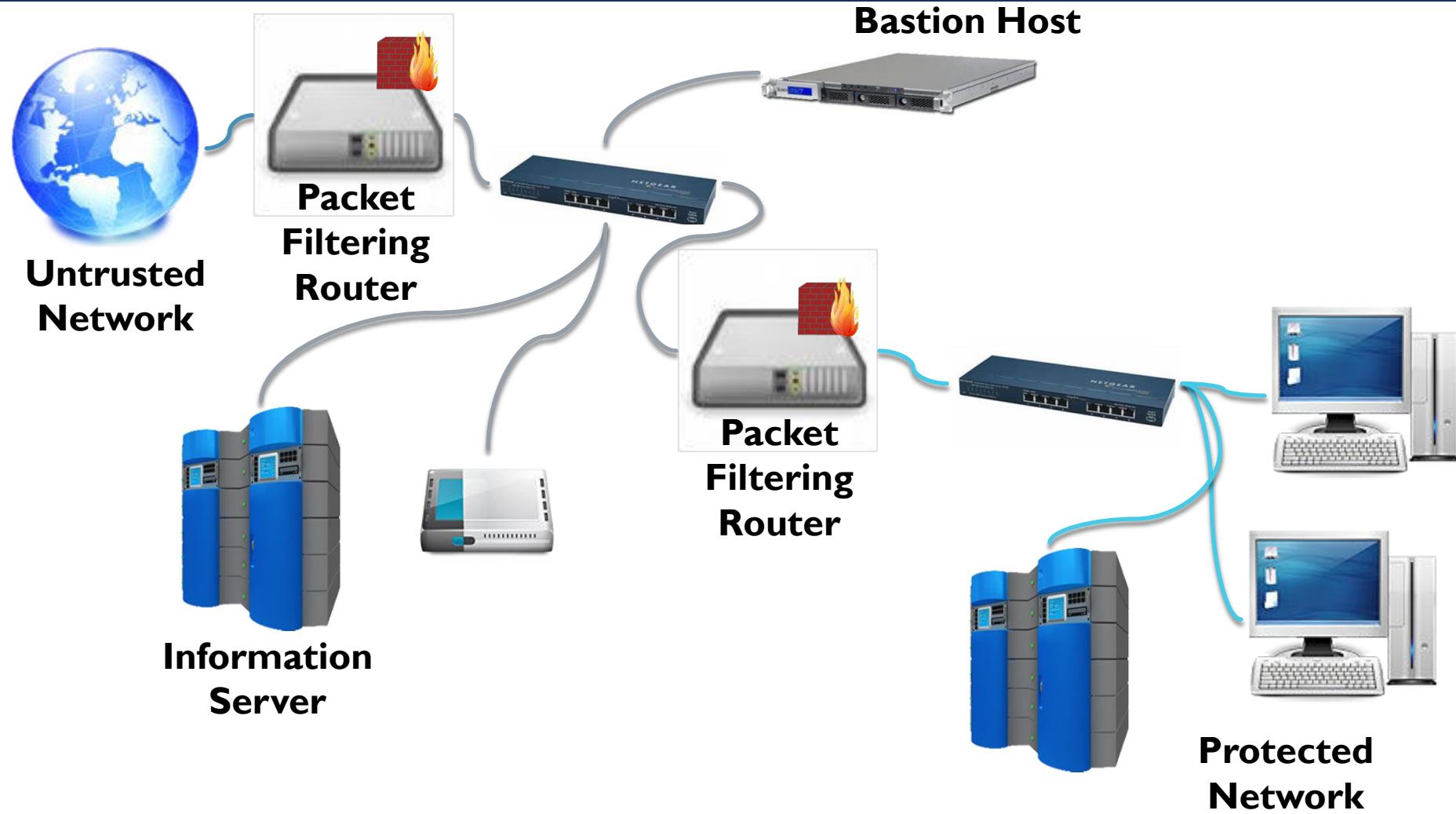
FIREWALLS - SCREENED HOST



DEMILITARIZED ZONE (DMZ)

- DMZ is a Screened-Subnet Firewall
 - Employs Two Filtering Routers
- Screened subnet typically contains...
 - The Bastion Host
 - Information Server (IS)
 - Remote Access Server (RAS)
 - Other public servers
 - Protected at both ends by the secure routers

FIREWALLS - DEMILITARISED ZONE



DMZ FIREWALLS

- Inner router will typically...
 - Allow connections to hosts in the DMZ only if started by hosts in the protected network
- Outer router will typically...
 - Allow connections to hosts in the DMZ started by hosts in the outside network
 - Allow connections to hosts in the outside network started by the Bastion host
- Anything not specifically allowed is disallowed

UNIFIED THREAT MANAGEMENT (UTM)

- A single network firewall that also contains:
 - **Spam** protection
 - **Anti-virus** capability
 - Intrusion detection system (**IDS**)
 - **Web content filtering**
- Helps Guard against “blended threats”
- Simplifies management for non-specialists
- Advanced Solution -> **SIEM**

SIEM - SECURITY INFORMATION EVENT MANAGEMENT

- Logging and Event Aggregation
 - Network (Router, Switch, Firewall etc.)
 - System (Server, Workstation etc.)
 - Application (Web, DB)
- Analyze all the above and detect relationships
- E.g.
 - Log Rhythm (<http://logrhythm.com>)
 - IBM QRadar (<http://www.q1labs.com>)

INTRUSION DETECTION SYSTEMS & INTRUSION PREVENTION SYSTEMS

- **IDS** aim - to automatically detect and identify possible security incidents
- **IPS** may have the capacity to stop incidents
 - Block access
 - Terminate connection
 - Reconfigure the security settings
 - Deleting Email attachments

IDS

- What does and IDS/IPS do when an incident is detected?

Typical functions:

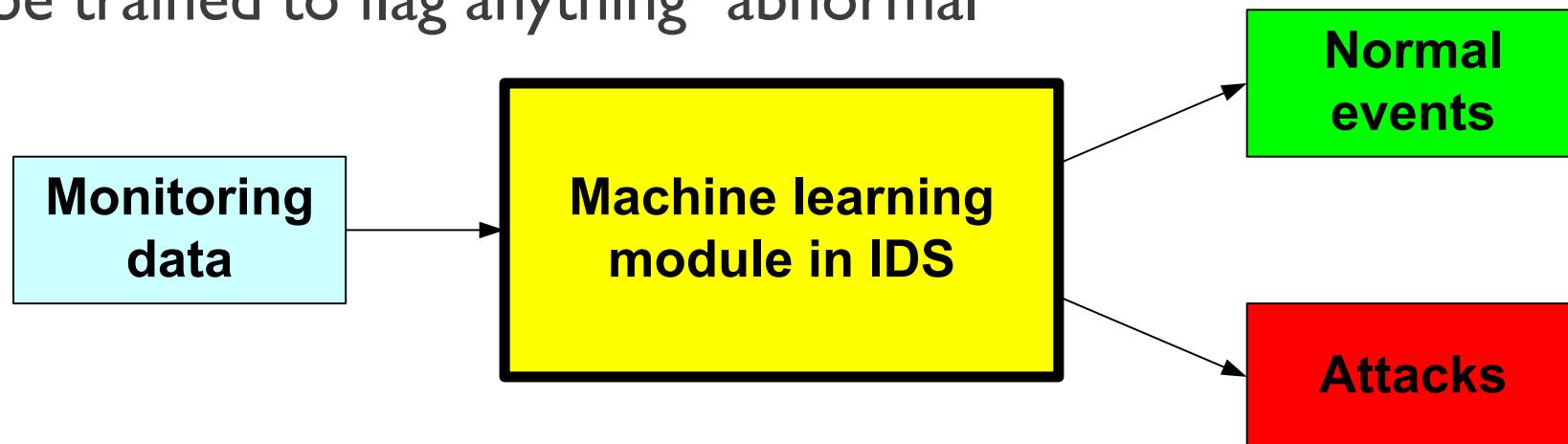
- IDS/IPS **collect/log** data about the incident
- Trigger **alerts** to the key personnel involved in the system security
- Compile **reports** that summarize the events of interest

IDS ANALYSIS

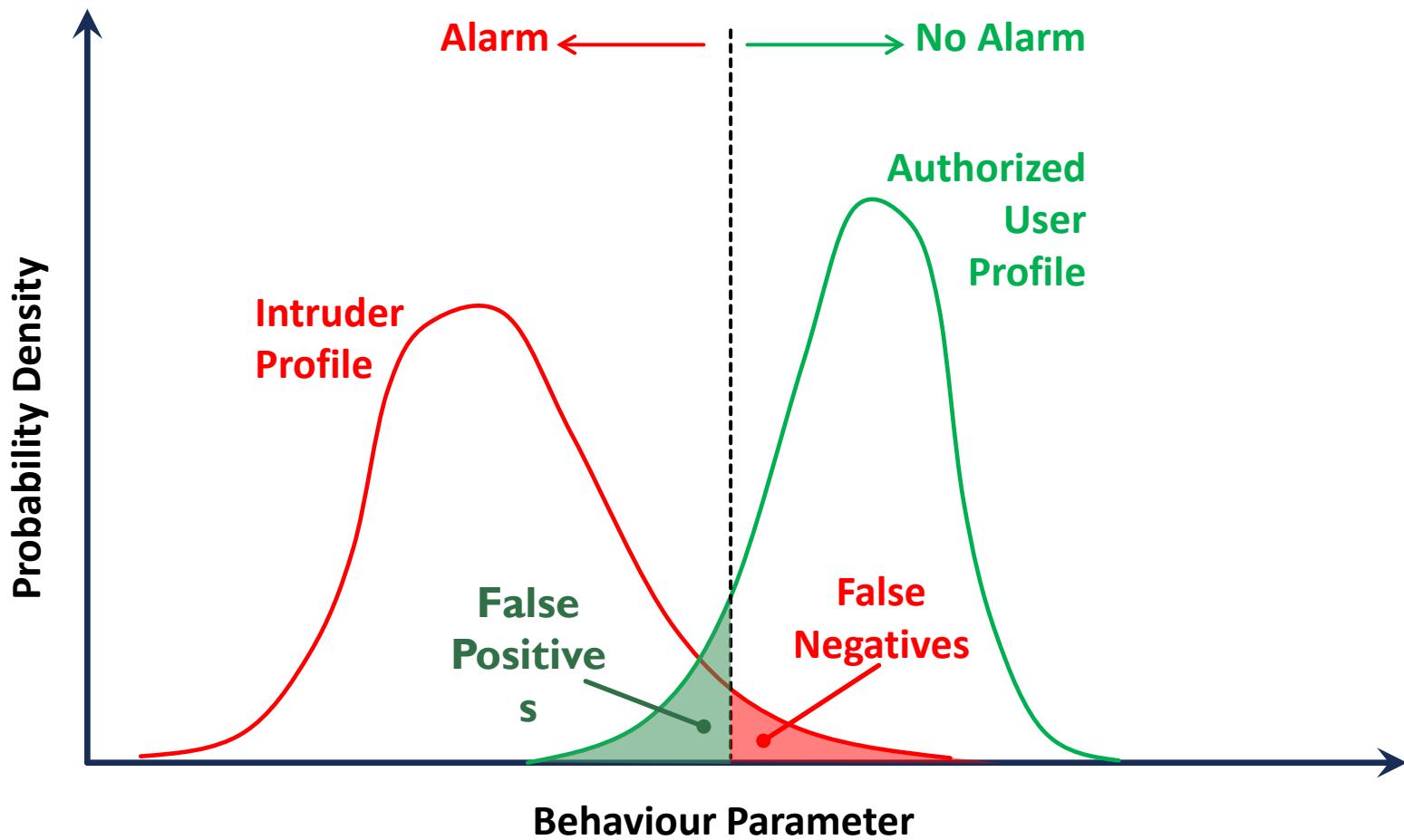
- Using **signatures of known attacks (Signature Based)**

or

- Using **Machine Learning (Anomaly Based)**
 - Eg: Neural Networks or K-Means Algorithm
- Could simply be trained to flag anything “abnormal”



INTRUSION DETECTION



VIRTUAL PRIVATE NETWORKS (VPN)

- Another secondary function often packaged with firewalls/routers
- **Goal:** Transmit private data across public network whilst maintaining confidentiality and authenticity
 - Encrypt TCP/IP Packets
 - Works at lower level: layer 3 (link encryption)
 - Packet encrypted before IP header added

VPN – TUNNELLING

- **Goal:** Hide source/destination IP addresses
- A feature of most routers/firewalls
- Encrypted/decrypted at tunnel ends
- **Advantages:**
 - Hides source address
 - Bypass restrictions*
- **Disadvantages:**
 - Increases packet size, therefore chance of fragmentation
 - Loss of end to end confidentiality
 - Slow

LESSONS LEARNED



FIREWALL



ACLs & PACKET FILTERING



FIREWALL TOPOLOGIES



UTM, SIEM, IDS, IPS & VPN



QUESTIONS ?



Thank
You

