School of Software

National Engineering Laboratory
for Big Data System
Program on "Innovation & Entrepreneurship "

Internet Security: State of the Art & Innovation

By

Abdelmonim Naway
AMISI FATAKI Clement
Jiwen Zhang

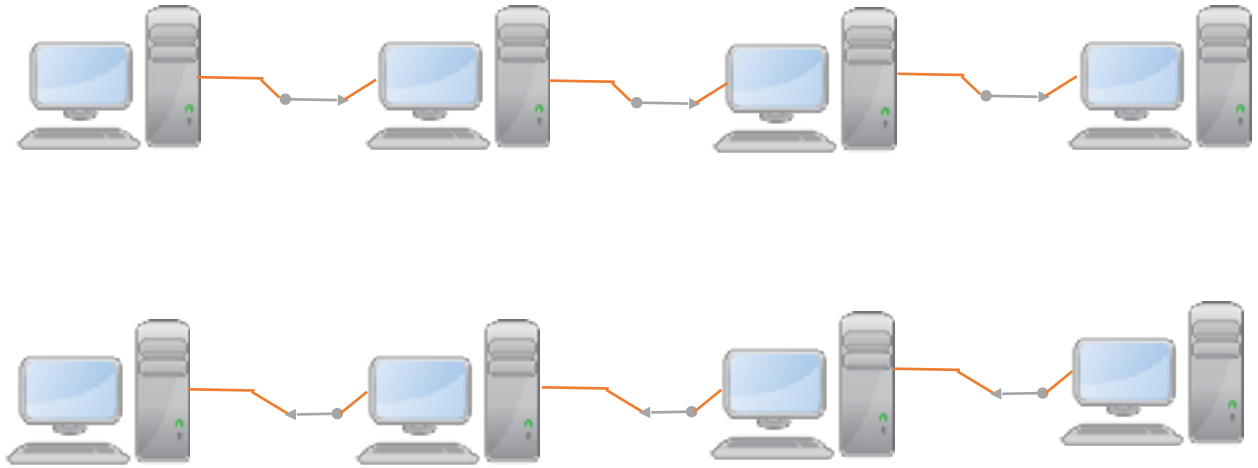
Sept. 28. 2018

Outline

- Introduction to Internet
- Review of Concepts
- Terminologies
- Common Threats and Attacks
- Best Practices on Internet
- AI & Machine Learning in the Cybersecurity Industry
- The role of Blockchain in CyberSecurity
- Conclusion

Introduction to Internet

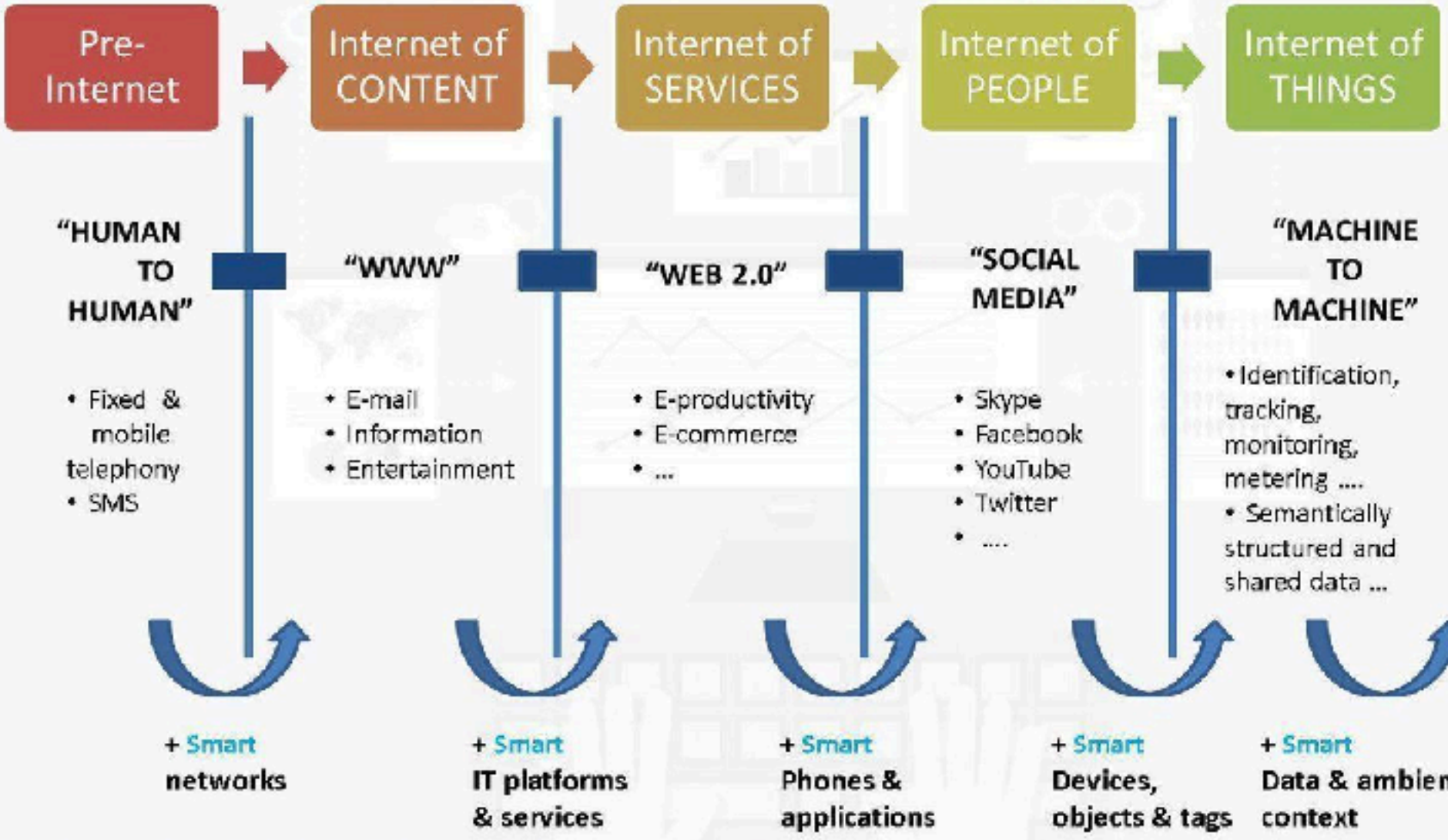
- A network of networks in which users at any one computer can, if they have permission, get information from any other computer.



- Today, people are not only use the Internet to talk to each other, but also for...

- Recently, other devices has been Connected to the Internet.

Evolution of Internet of Things



Security Threats

- Unfortunately, the straightforward connectivity of these devices comes at a price
- A **computer virus** is a malicious software program loaded onto a user's **computer** without the user's knowledge and performs malicious actions.
- One person could steal another's identity by guessing, cracking or extracting a password.
- Vulnerabilities such as these will never completely go away because they are built into the Internet's architecture.
- Criminals use them to steal Billions of dollars, Governments use them for surveillance, Hacktivists use them to further their political goals.
- In 2016 alone, over 3.1 billion records were stolen or leaked through data breaches of major organizations.

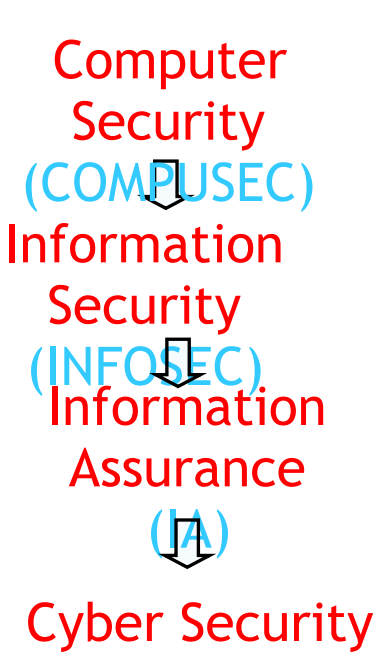
Review of Concepts

- **What is Information security ?**
  - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- What is Computer Security?
  - Computer security deals with the prevention and detection of unauthorized actions by users of a computer system.
- **What is Network Security?**
  - Network security is a subset of information/cyber security which deals with planning and implementing network security measures to protect the integrity of networks and programs against hacking and unauthorized access

- **What is Information Assurance?**
  - Emphasis on Information Sharing
  - Establishing and controlling trust
  - Authorization and Authentication (A&A)
- **What is Data Security?**
  - is the prevention of unauthorized access, use, disruption, modification or destruction of data in storage.
- **What is Cybersecurity?**
  - Protection of information and systems within networks that are connected to the Internet.
- **What is Internet Security?**
  - internet security is a branch of computer security that deals specifically with Internet-based threats. These include hacking, where unauthorized users gain access to computer systems, email accounts or websites; viruses and other malicious software (malware).

Review of Concepts

- Progression of Terminology



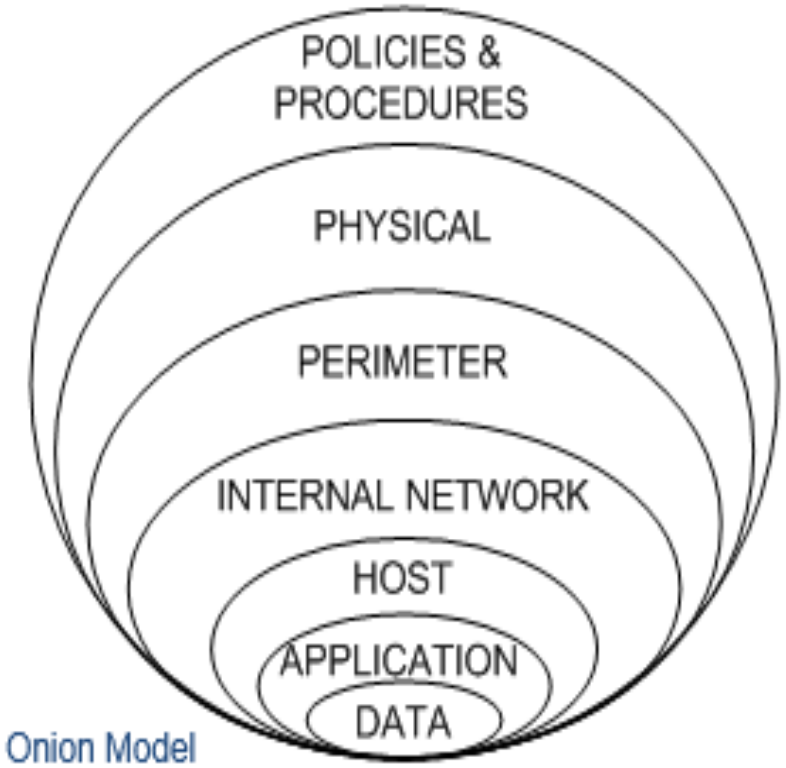
Legacy Term (no longer used).

Legacy Term (still used).

Term widely accepted today with focus on Information Sharing.

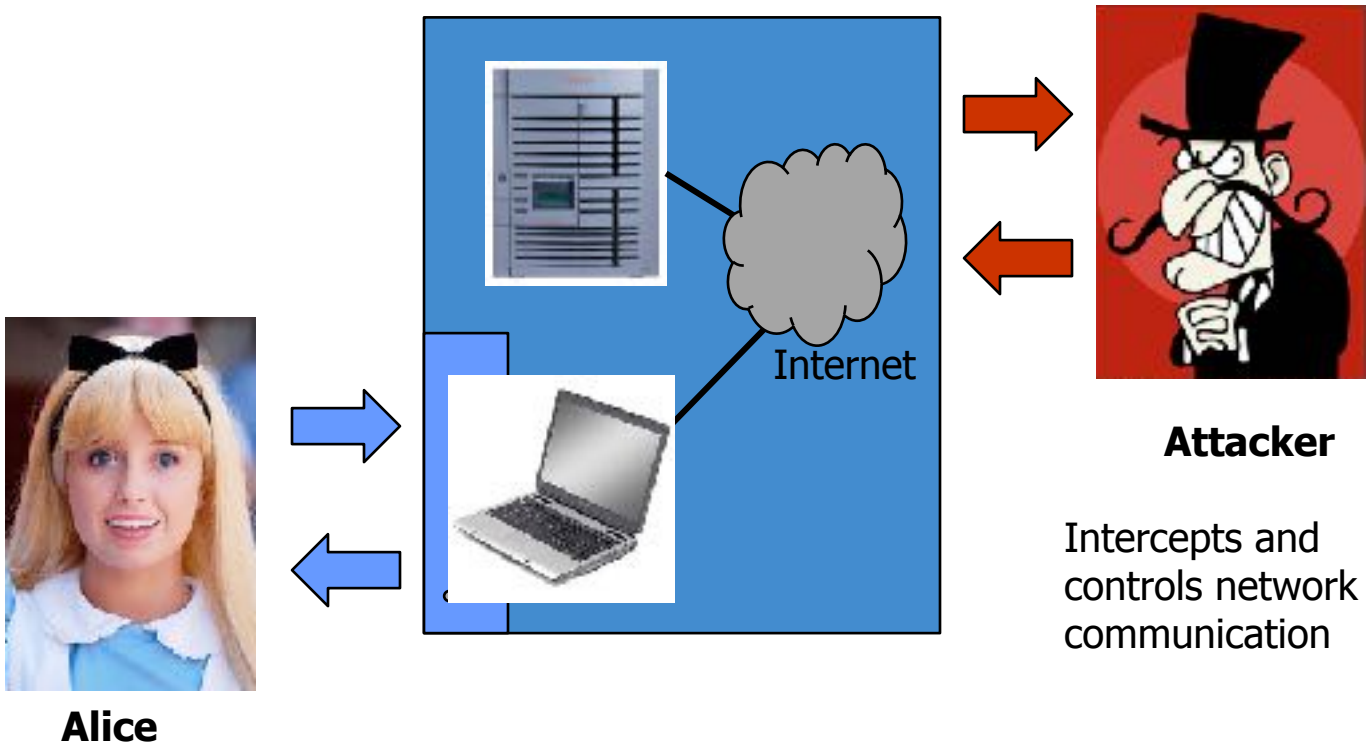
Broad Term quickly being adopted.

- What is the Defense in Depth Strategy?
  - Using layers of defense as protection.
  - People, Technology, and Operations.



Onion Model

Security Breach



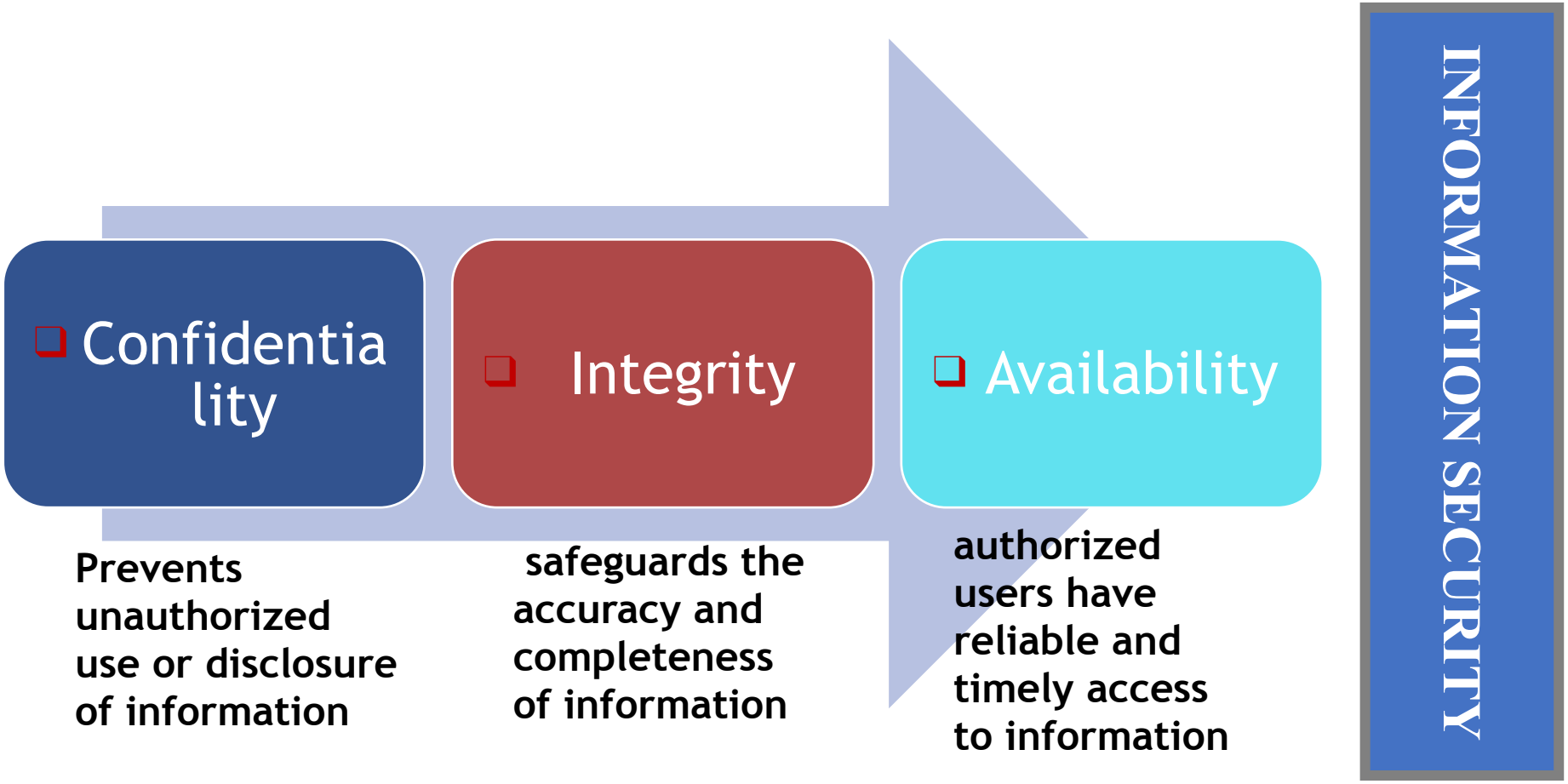
- Security is about
  - Honest user (e.g., Alice, Bob, …)
  - Dishonest Attacker
    - Disrupts honest user's use of the system (Integrity, availability)
    - Learns information intended for Alice only (Confidentiality)

Source:Wei Wang, INFOSEC 2016, BJTU

Terminologies

- CIA
  - Confidentiality
  - Integrity
  - Availability
- Access Control
  - Authentication
  - Authorisation
  - Accountability
- Risk
- Threat
- Vulnerability
- Impact

Goals of Information Security



Access Control

- The ability to permit or deny the use of an object by a subject.

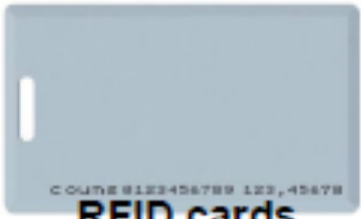
It provides 3 essential services:

- Authentication (identification of a user)
- Authorisation (who is allowed to use a service)
- Accountability (what did a user do)

Authentication

- a means to verify or prove a user's identity
- The term "user" may refer to:
  - Person
  - Application or process
  - Machine or device
- Identification comes before authentification
  - Provide username to establish user's identity
- To prove identity, a user must present either of the following:
  - What you know (passwords, passphrase, PIN)
  - What you have (token, smart cards, passcodes, RFID)
  - Who you are (biometrics such as fingerprints and iris scan, signature or voice)

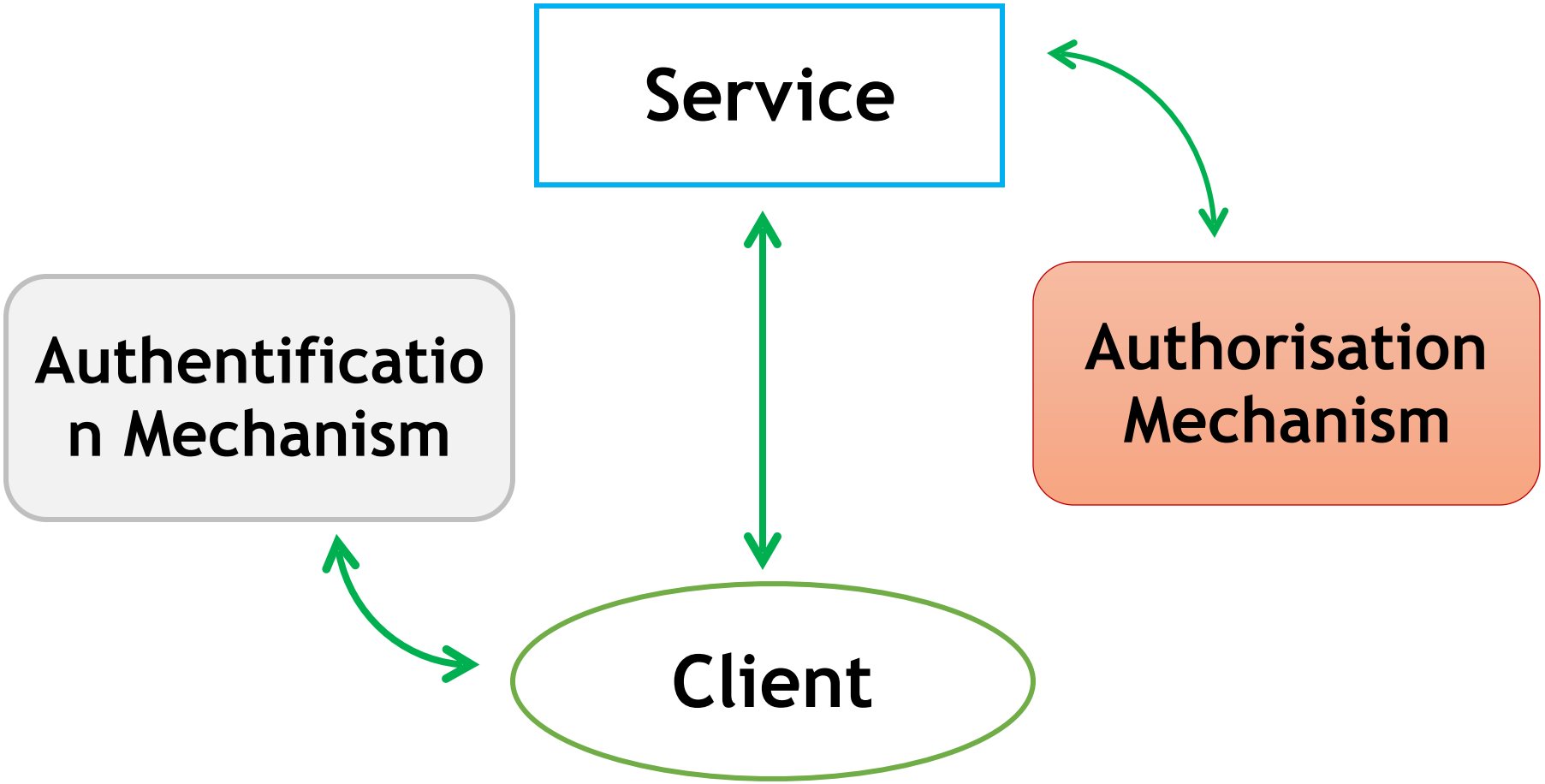
Authentication – Examples of Tokens



Authorisation

- Defines the user's rights and permissions on a system
- Typically done after user has been authenticated
- Grants a user access to a particular resource and what actions he is permitted to perform on that resource
- Access criteria based on the level of trust:
  - Roles
  - Groups
  - Location
  - Time
  - Transaction type

Authentication vs. Authorisation



“Authentication simply identifies a party, Authorisation defines whether they can perform certain action” - RFC 3552

Accountability

- The security goal is to generate the requirement for actions of an entity to be traced uniquely to that entity
  - Senders cannot deny sending information
  - Receivers cannot deny receiving it
  - Users cannot deny performing a certain action
- Supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention and after-action recovery and legal action

Source: NIST Risk Management Guide for Information Technology Systems

Reliability

- Relating to (accidental) failures, and safety, relating to impact of system failures on their environment, which also deal with situations where a system has to perform properly in adverse conditions.

Privacy

- Is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively.

Risk, Threats, and Vulnerability

- Threat
  - Any circumstance or event with the potential to cause harm to a networked system
- Vulnerability
  - A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy
- Risk
  - The possibility that a particular vulnerability will be exploited

Common Security Threats

Network Attacks

- Denial-of-Service (DOS)
- Phishing emails
- Advertising

Web Attacks

- Cross-site Scripting(XSS)
- SQL Injection

OS, applications and software attacks

- Virus
- Trojan
- Worms
- Rootkits

Social Engineering

- The art of manipulating people so they give up confidential information

Security Mechanisms

Cryptographic Techniques	Use mathematical algorithms to transform data into a form that is not readily intelligible
Firewalls	Software and hardware for access limitations
Network Monitoring Intrusion Detection and Prevention Systems	Intrusion Detection and Prevention Systems
Hardware for authentication	Smartcards, security tokens
Security Policies	Define who has access to which resources
Physical Security	Keep data in a safe place which limited and authorized physical access

Best practices on Internet(Users)

- Keep your OS and programs updated
- Crate strong passwords
- Physical Protection
- Use Anti-virus software
- Scan External data (USB-drives, E-mail attachments)
- Only use trusted and Open Source Software

AI & Machine Learning in the Cyber Security Industry

- The complexity of cyber threats is increasing, making it harder to detect attacks, and harder still to protect against them
- Machine learning can learn how *to automatically detect unusual patterns in encrypted* web traffic and Internet of things (IoT) environments.
- Ultimately, this would help improve network security defenses.
- Another big cyber security issue has been the skills gaps:
  - organisations have not been able to find staff with the necessary skills.
  - AI and machine learning tools would help overcome these gaps.

The Role of Blockchain in Cybersecurity

Blockchain can offer the following for security:

- Blockchain resolves the '**lack of trust**' problem between counterparties at a very basic level.
  - This could potentially help enhance cyber-defense as the platform can prevent fraudulent activities via consensus mechanisms
- Eliminating Human Factor from Authentication
  - Businesses are able to authenticate devices and users without the need for a password with the help of blockchain technology.
  - This eliminates human intervention from the process of authentication, thereby avoiding it from becoming a potential attack vector.
- Decentralized Storage
  - Blockchain users can maintain their data on their computer in their network. Because of this, they can make sure that the chain won't collapse
- Traceability
  - Every transaction added to a private or public blockchain is timestamped and signed digitally.

Thanks !

monim88@msn.com
clement.fataki@gmail.com
blairzhang2015@gmail.com