NETWORK SECURITY

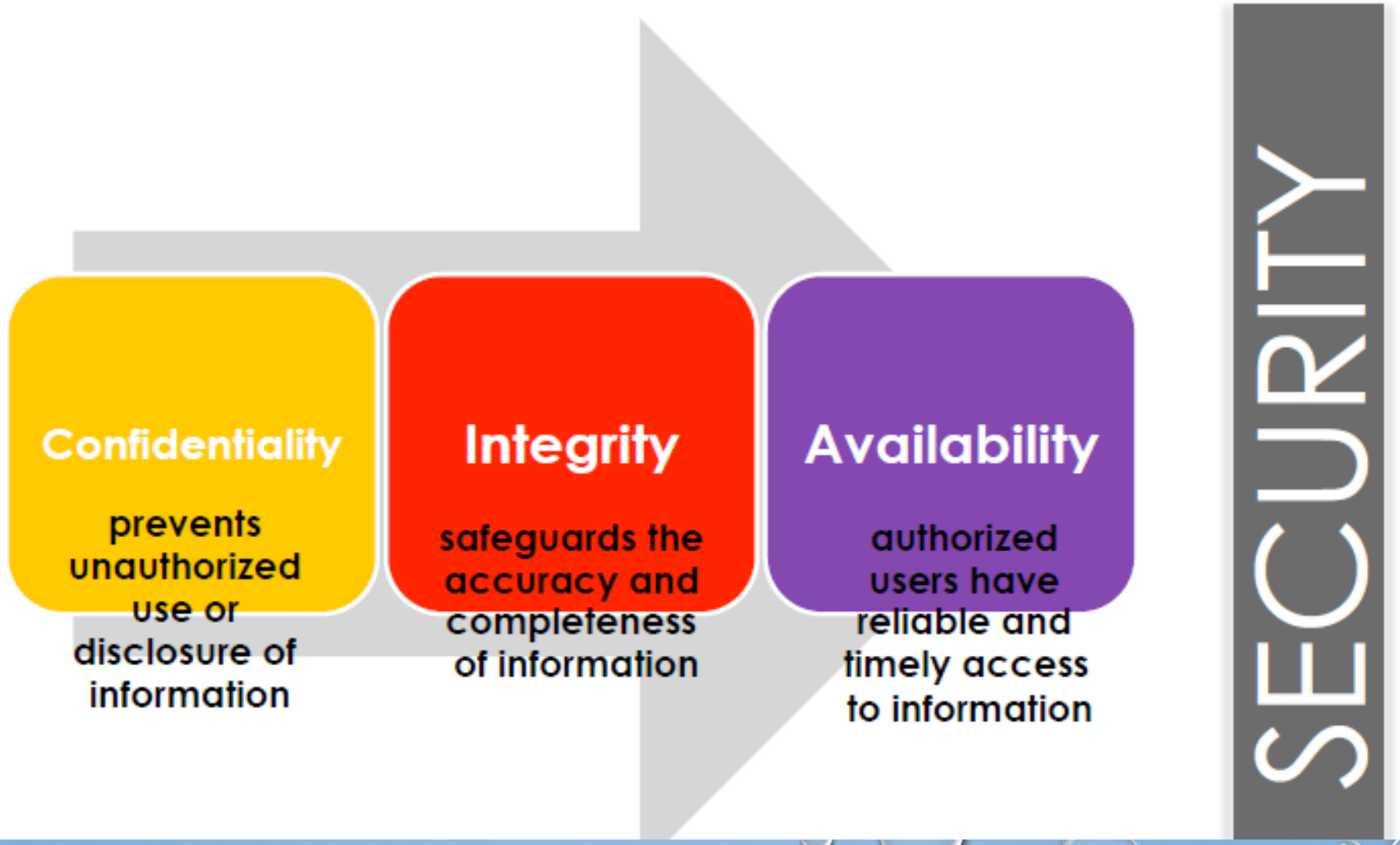
Network security is the security provided to a network from unauthorized access and risks.

It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Types of Security

- Computer Security
  - generic name for the collection of tools designed to protect data and to thwart hackers
- Network Security
  - measures to protect data during their transmission
- Internet Security
  - measures to protect data during their transmission over a collection of interconnected networks

Goals of Security



Terminology

- Access control - ability to permit or deny the use of an object by a subject.
- It provides 3 essential services:
  - Identification and authentication (who can login)
  - Authorization (what authorized users can do)
  - Accountability (identifies what a user did)

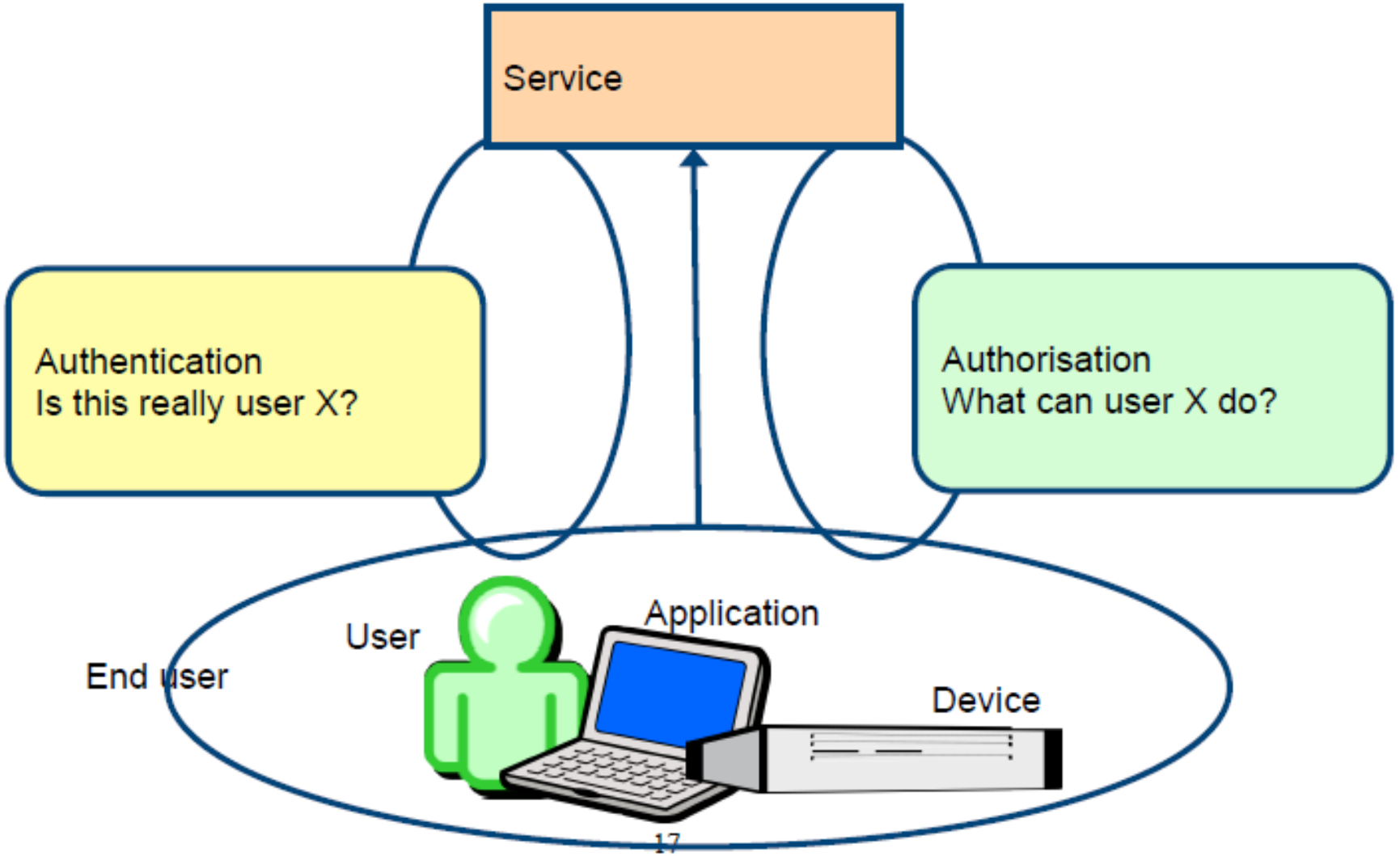
Authentication

- Validating a claimed identity of an end user or a device such as host, server, switch, router, etc.
- *Must be careful to understand whether a technology is using user, device or application authentication.*

Authorization

- The act of granting access rights to a user, groups of users, system, or program.
  - Typically this is done in conjunction with authentication.

Authentication and authorisation



Non-Repudiation

- A property of a cryptographic system that prevents a sender from denying later that he or she sent a message or performed a certain action.

Audit

A chronological record of system activities that is sufficient to enable the reconstruction and examination of a given sequence of events

Vulnerability

- A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy
  - Software bugs
  - Configuration mistakes
  - Network design flaw
- Exploit
  - Taking advantage of a vulnerability

Risk

- The possibility that a particular vulnerability will be exploited
  - Risk analysis: the process of identifying:
    - Security risks
    - Determining their impact
    - And identifying areas require protection

Threat

- Any circumstance or event with the potential to cause harm to a networked system
  - Denial of service

    Attacks make computer resources (e.g., bandwidth, disk space, or CPU time) unavailable to its intended users
  - Unauthorised access

    Access without permission issues by a rightful owner of devices or networks
  - Impersonation
  - Worms
  - Viruses

Security Terminology

- **Attack** In the context of computer/network security, an attack is an attempt to access resources on a computer or a network without authorization, or to bypass security measures that are in place.
- **Audit** To track security-related events, such as logging onto the system or network, accessing objects, or exercising user/group rights or privileges.
- **Availability of data** Reliable and timely access to data.
- **Breach** Successfully defeating security measures to gain access to data or resources without authorization, or to make data or resources available to unauthorized persons, or to delete or alter computer files.
- **Brute force attack** Attempt to "crack" passwords by sequentially trying all possible combinations of characters until the right combination works to allow access.

- **Buffer** A holding area for data.
- **Buffer overflow** A way to crash a system by putting more data into a buffer than the buffer is able to hold.
- **CIA triad** Confidentiality, Integrity, and Availability of data. Ensuring the confidentiality, integrity, and availability of data and services are primary security objectives that are often related to each other. See also *availability of data*, *confidentiality of data*, and *integrity of data*.
- **Confidentiality of data** Ensuring that the contents of messages will be kept secret. See also *integrity of data*.
- **Countermeasures** Steps taken to prevent or respond to an attack or malicious code.
- **Cracker** A hacker who specializes in "cracking" or discovering system passwords to gain access to computer systems without authorization. See also *hacker*.
- **Crash** Sudden failure of a computer system, rendering it unusable.

- **Defense-in-depth** The practice of implementing multiple layers of security. Effective defense-in-depth strategies do not limit themselves to focusing on technology, but also focus on operations and people. For example, a firewall can protect against unauthorized intrusion, but training and the implementation of well-considered security policies help to ensure that the firewall is properly configured.
- **Denial of Service attack** A deliberate action that keeps a computer or network from functioning as intended (for example, preventing users from being able to log onto the network).
- **Exposure** A measure of the extent to which a network or individual computer is open to attack, based on its particular vulnerabilities, how well known it is to hackers, and the time duration during which intruders have the opportunity to attack. For example, a computer using a dialup analog connection has less exposure to attack coming over the Internet, because it is connected for a shorter period of time than those using "always-on" connections such as cable, DSL or T-carrier.

- **Hacker** A person who spends time learning the details of computer programming and operating systems, how to test the limits of their capabilities, and where their vulnerabilities lie. See also *cracker*.
- **Integrity of data** Ensuring that data has not been modified or altered, that the data received is identical to the data that was sent.
- **Least privilege** The principle of least privilege requires that users and administrators have only the minimum level of access to perform their job-related duties. In military parlance, the principle of least privilege is referred to as *need to know*.
- **Malicious code** A computer program or script that performs an action that intentionally damages a system or data, that performs another unauthorized purpose, or that provides unauthorized access to the system.
- **Penetration testing** Evaluating a system by attempting to circumvent the computer's or network's security measures.

- **Reliability** The probability of a computer system or network continuing to perform in a satisfactory manner for a specific time period under normal operating conditions.
- **Risk** The probability that a specific security threat will be able to exploit a system vulnerability, resulting in damage, loss of data, or other undesired results. That is, a risk is the sum of the threat plus the vulnerability.
- **Risk management** The process of identifying, controlling, and either minimizing or completely eliminating events that pose a threat to system reliability, data integrity, and data confidentiality.
- **Sniffer** A program that captures data as it travels across a network. Also called a *packet sniffer*.
- **Social engineering** Gaining unauthorized access to a system or network by subverting personnel (for example, posing as a member of the IT department to convince users to reveal their passwords).
- **TCSEC** Trusted Computer System Evaluation Criteria. A means of evaluating the level of security of a system.

- **Technical vulnerability** A flaw or bug in the hardware or software components of a system that leaves it vulnerable to security breach.
- **Threat** A potential danger to data or systems. A threat agent can be a virus; a hacker; a natural phenomenon, such as a tornado; a disgruntled employee; a competitor, and other menaces.
- **Trojan horse** A computer program that appears to perform a desirable function but contains hidden code that is intended to allow unauthorized collection, modification or destruction of data.
- **Virus** A program that is introduced onto a system or network for the purpose of performing an unauthorized action (which can vary from popping up a harmless message to destroying all data on the hard disk).
- **Vulnerability** A weakness in the hardware or software or security plan that leaves a system or network open to threat of unauthorized access or damage or destruction of data.
- **Worm** A program that replicates itself, spreading from one machine to another across a network.

More Basic Terminology

Identification

Identification is simply the process of identifying one's self to another entity or determining the identity of the individual or entity with whom you are communicating.

Authentication

Authentication serves as proof that you are who you say you are or what you claim to be.

Authentication is critical if there is to be any trust between parties.

Authentication is required when communicating over a network or logging onto a network

When communicating over a network you should ask yourself two questions:

1) With whom am I communicating? and

2) Why do I believe this person or entity is who he, she, or it claims to be?

Access Control (Authorization)

This refers to the ability to control the level of access that individuals or entities have to a network or system and how much information they can receive.

Availability

This refers to whether the network, system, hardware, and software are reliable and can recover quickly and completely in the event of an interruption in service.

Confidentiality

This can also be called privacy or secrecy and refers to the protection of information from unauthorized disclosure.

Integrity

This can be thought of as accuracy. This refers to the ability to protect information, data, or transmissions from unauthorized, uncontrolled, or accidental alterations. The term integrity can also be used in reference to the functioning of a network, system, or application.

Accountability

This refers to the ability to track or audit what an individual or entity is doing on a network or system.

Nonrepudiation

The ability to prevent individuals or entities from denying (repudiating) that information, data, or files were sent or received or that information or files were accessed or altered, when in fact they were.