Information Security Fundamentals

Dr. Eng. Manel Abdelkader

Why study Information Security

- Being an IT expert requires knowledge about IT security
  - Analogy: Building architects must have knowledge about fire safety
- Developing IT systems without considering security will lead to vulnerable IT systems
- IT experts without security skills are part of the problem
- Learn about IT security to become part of the solution !

Objectives

- Understand the prominent security challenges in a dynamic environment
- Understand the range of vulnerabilities and threats that thwart the information system
- Learn proactive countermeasures that can be used to guarantee the required security level
- Learn ways to improve response and recovery capabilities in the case of occurrence of security incidents

Outline

1. Security Fundamentals
2. Security and Risk Management.
3. Cryptography
4. Key Management and PKI
5. Authentication and identity management
6. Access control

Assessment mode

- 15% quizes
- 15% Labs
- 30% midterm
- 40% Final exam

Absenteeism

- More than 3 absences => not allowed to enter the exam.
- Absence in a quiz => could not retake the quiz.

Security Fundamentals

Chapter 1

Objectives

- ❑ Information Security
- ❑ Security Properties
- ❑ Threats, Attacks, and Assets
- ❑ Security mechanisms

What is information security

- Information Security focuses on protecting from damage or harm
- What are the assets to be protected?
  - Example: data files, software, IT equipment and infrastructure
- Covers both intentional and accidental events
  - Threat agents can be people or acts of nature
  - People can cause harm by accident or by intent

Information States

- Information security involves protecting information assets from harm or damage.
- Information is considered in one of three possible states:
  - During storage
    - Information storage containers
    - Electronic, physical, human

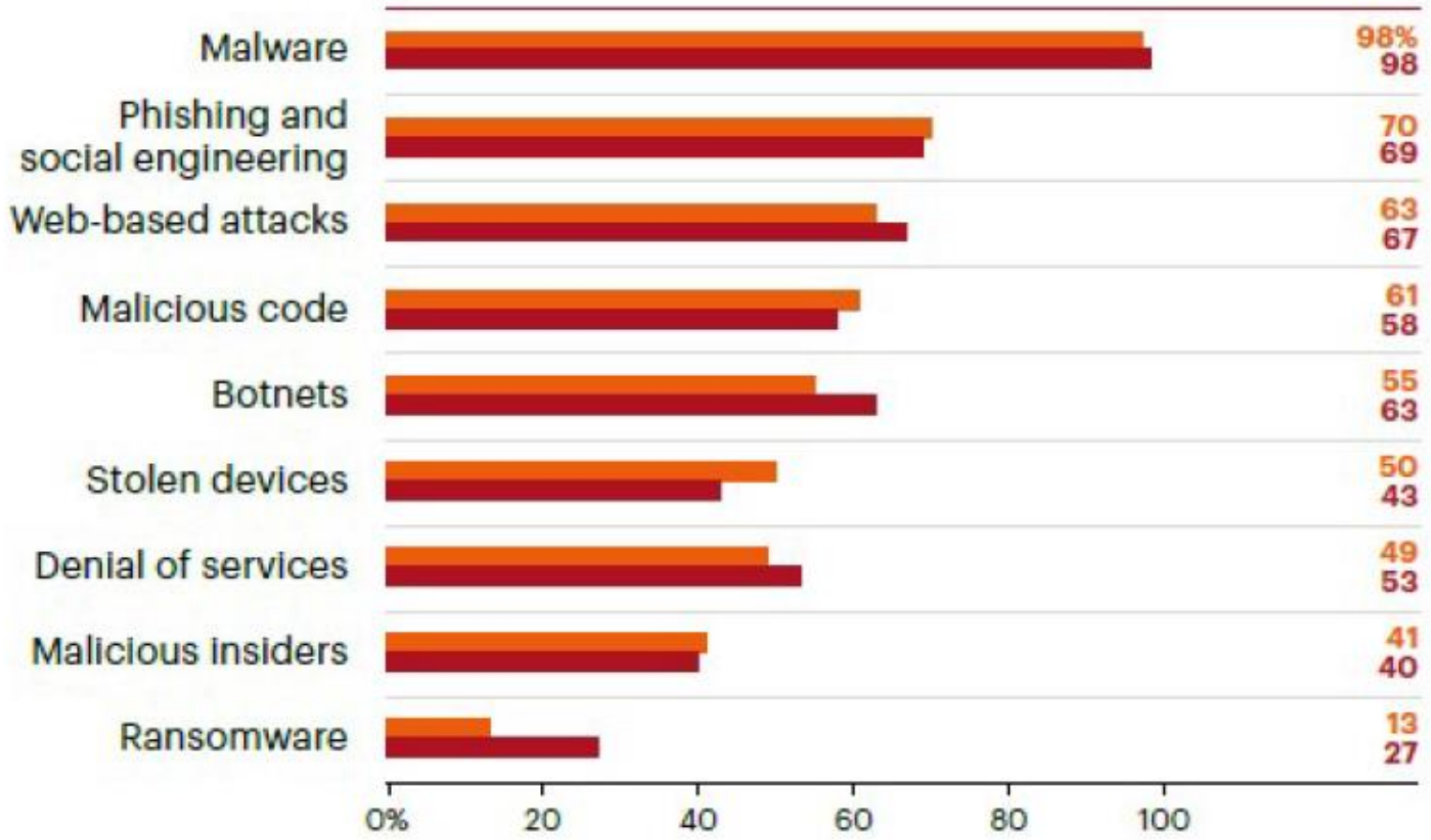
  - During transmission
    - Physical or electronic

  - During processing (use)
    - Physical or electronic

The need for Information Security

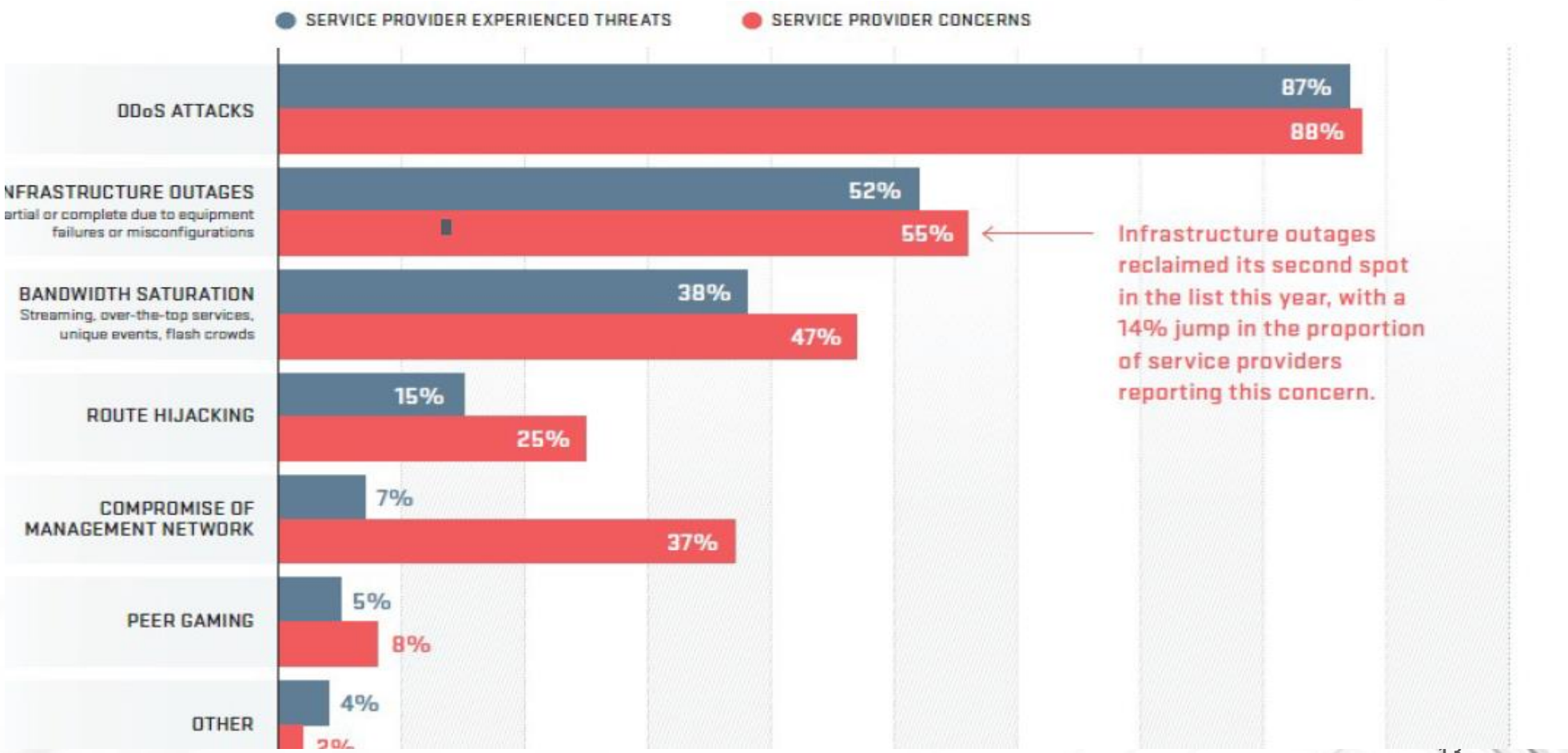
- Why not simply solve all security problems once for all?
- Reasons why that's impossible:
  - Rapid innovation constantly generates new technology with new vulnerabilities
  - More activities go online
  - Crime follows the money
  - Information security is a second thought when developing IT
  - New and changing threats
  - More effective and efficient attack technique and tools are being developed
- Conclusion: Information security doesn't have a final goal, it's a continuing process.

Types of cyber attacks (254 companies) Ponemon Institute

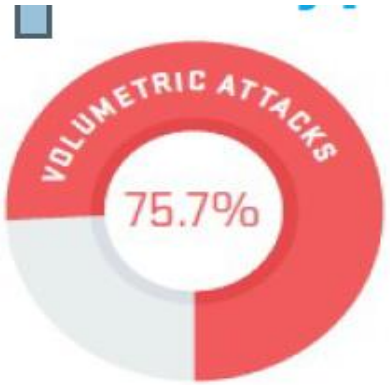


Security trends and analytics

Arbor Networks, the cyber security division of NETSCOUT



DDoS



netric Attacks

ttacks attempt to consume the bandwidth either within get network or service, or between the target network ce and the rest of the internet. These attacks are simply ausing congestion.

2

TCP State-Exhaustion Attacks

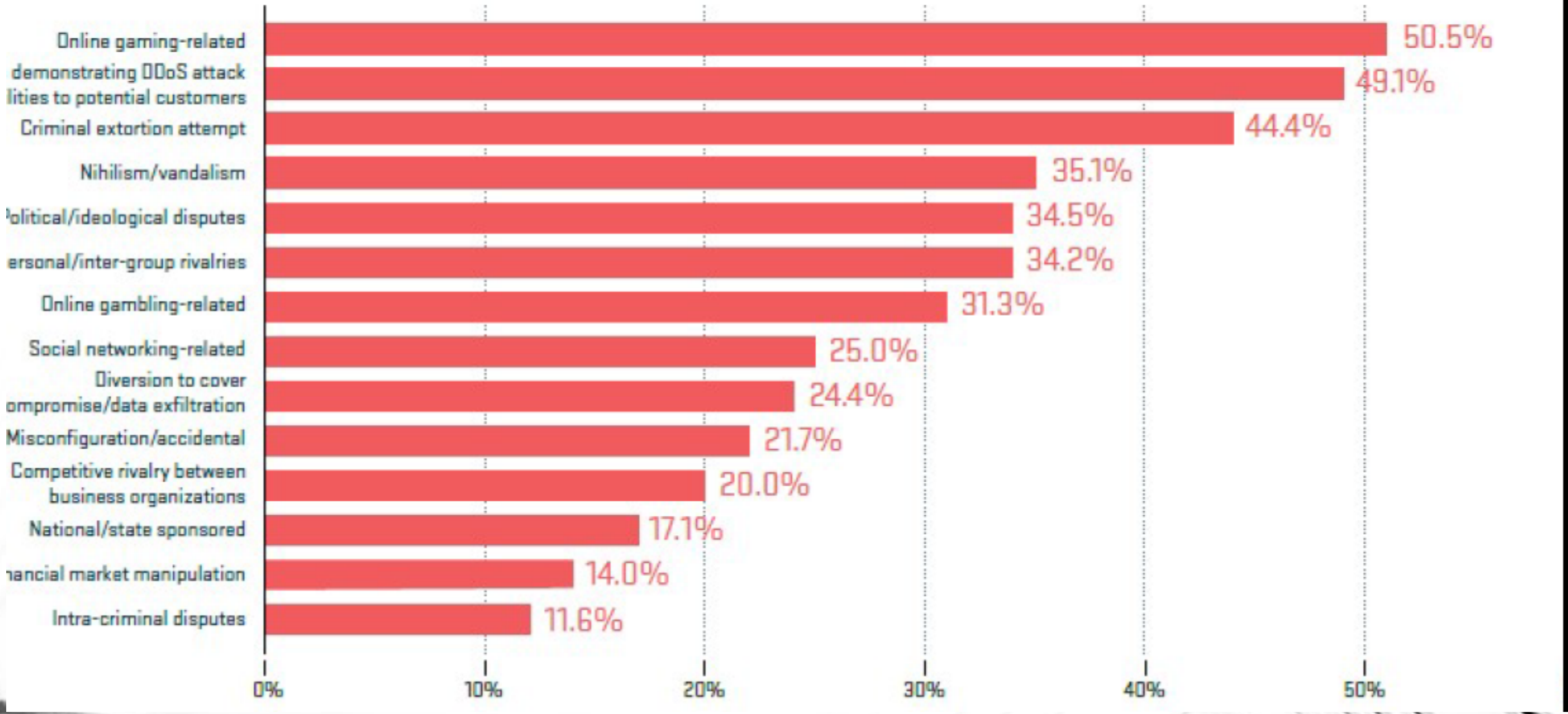
These attacks attempt to consume the connection state tables that are present in many infrastructure components, such as load balancers, firewalls, IPS and the application servers themselves. They can take down even high-capacity devices capable of maintaining state on millions of connections.

3

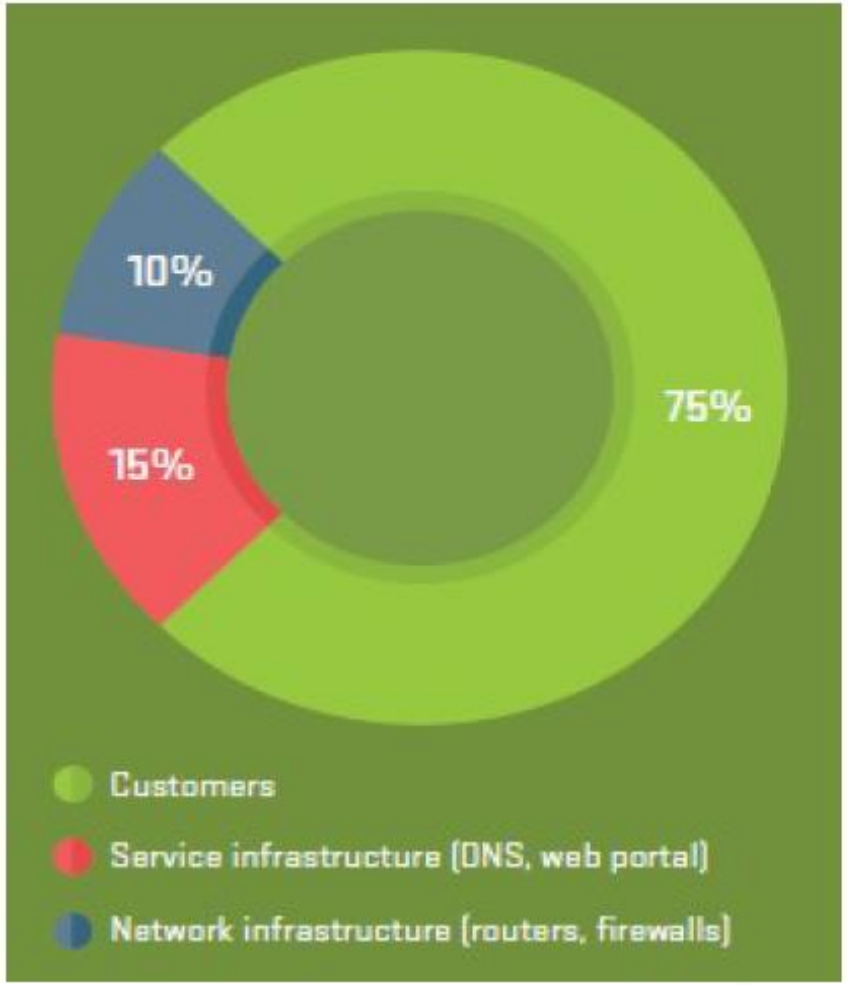
Application-Layer Attacks

These target some aspect of an application c Layer 7. They are the most sophisticated and because they can be very effective with as fe machine generating traffic at a low rate.

Motivations behind DDoS attacks



Attack Target Mix



Attack frequency per month

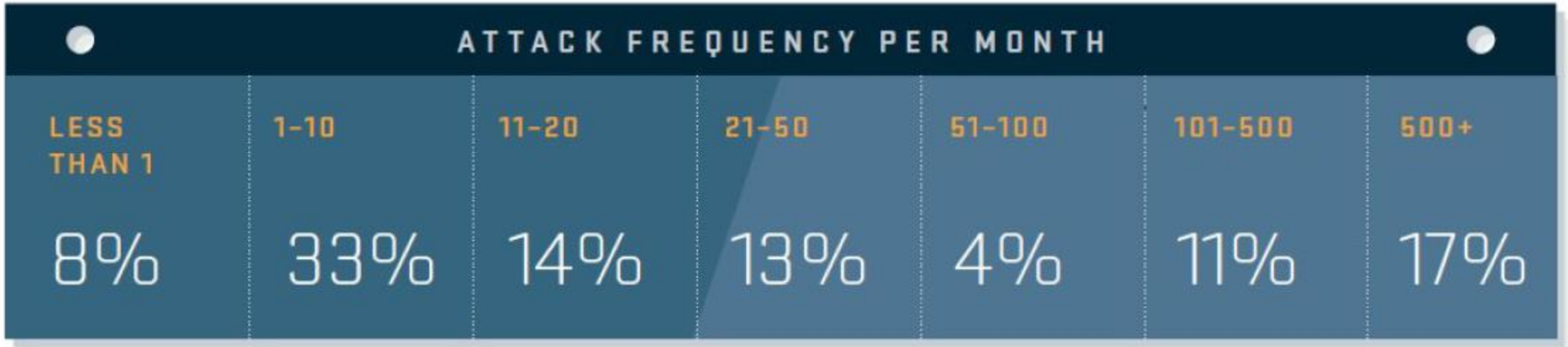
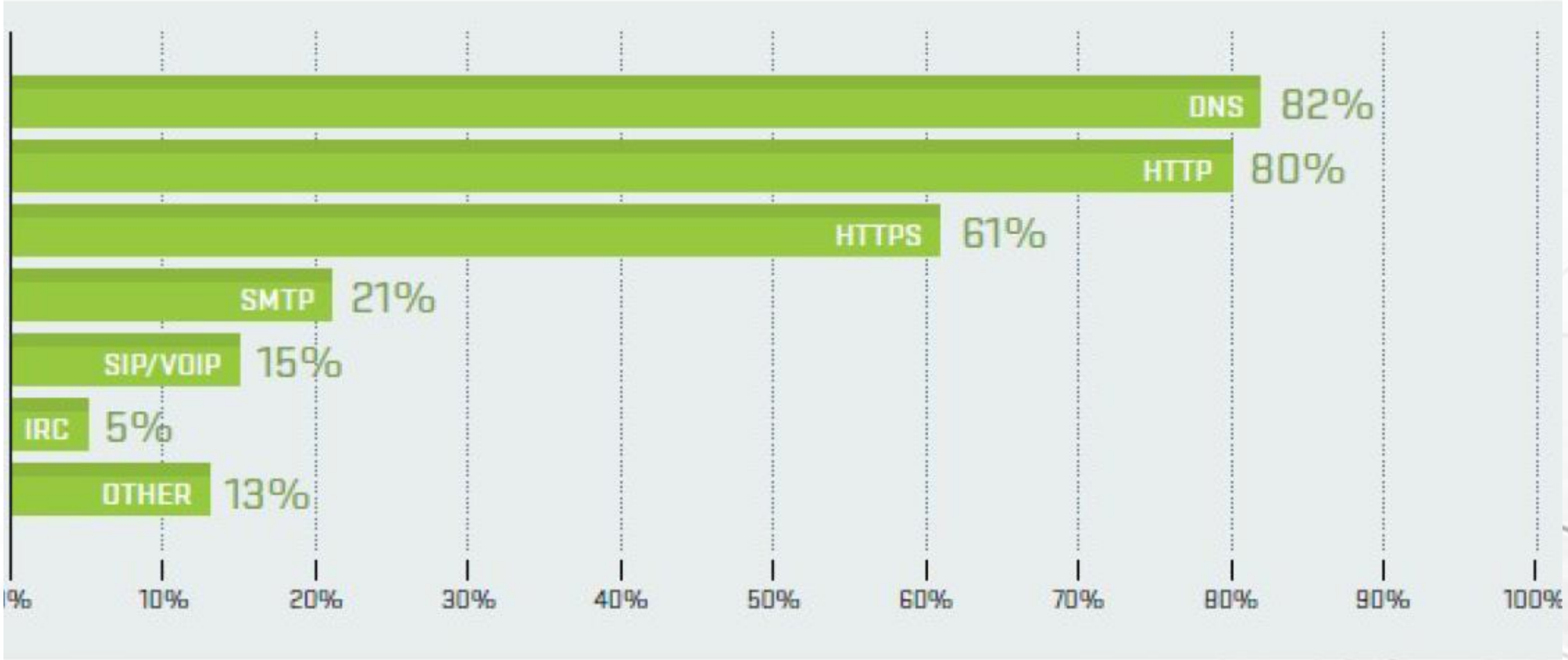


Figure 15 Attack Frequency Per Month

Attack duration

Application layer attack vectors



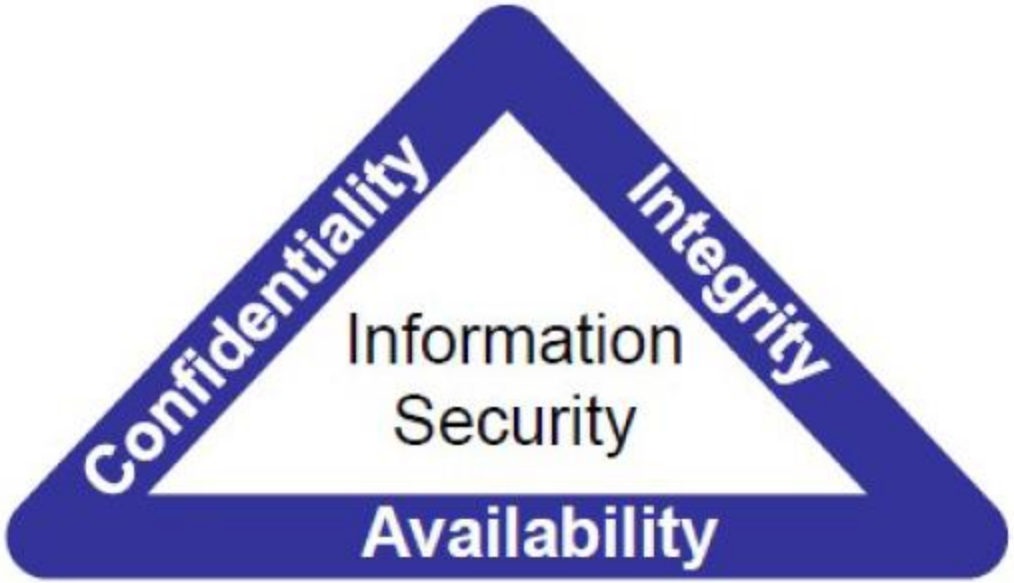
Security Services

Computer security: 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)

NIST 1995

The CIA triad

- A security service provides a high level security property
- The traditional definition of information security is to preserve the three CIA properties for data and services:
  - **Confidentiality**:
  - **Integrity**
  - **Availability**:



- CIA are the three main security properties/services

Confidentiality

- The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (ISO 27000)
- Can be divided into:
  - Secrecy: Protecting business data
  - Privacy: Protecting personal data
  - Anonymity: Hide who is engaging in what actions
- Main threat: Information theft, unintentional disclosure
- Controls: *Encryption, Access Control, Perimeter defence*

  As general controls, also include:

  Secure Systems Development, Incident Response

Integrity

Data Integrity: The property that data has not been altered or destroyed in an unauthorized manner.

(X.800: Security Architecture for OSI)

System Integrity: The property of accuracy and completeness (ISO 27000).

Can include the accountability of actions.

Threats: Data and system corruption, loss of accountability

Controls:

- *Hashing, cryptographic integrity check and encryption*
- *Authentication, access control and logging*
- *Software digital signing*
- *Configuration management and change control (system integrity)*

As general controls, also include:

Secure System Development, Incident Response

Availability

The property of being accessible and usable upon demand by an authorized entity. (ISO 27000)

Main threat: Denial of Service (DoS)

- The prevention of authorized access to resources or the delaying of time critical operations

Controls:

- *Redundancy of resources,*
- *Load balancing,*
- *Software and data backups*

As general controls, also include:

Secure System Development and Incident Response

Data Privacy

To protect specific aspects of information that may be related to natural persons (personal information).

- Prevent unauthorized collection and storage of personal information
- Prevent unauthorized use of collected personal information
- Make sure your personal information is correct
- Ensure transparency and access for data subjects
- Provide adequate information security (CIA) around personal information
- Define clear responsibilities around personal information
- GDPR becomes EU law on 25 May 2018
  (General Data Protection Regulation)

Authenticity (security service)

The CIA properties are quite general security services.
Other security services are often mentioned.
Authentication is very important, with various types:

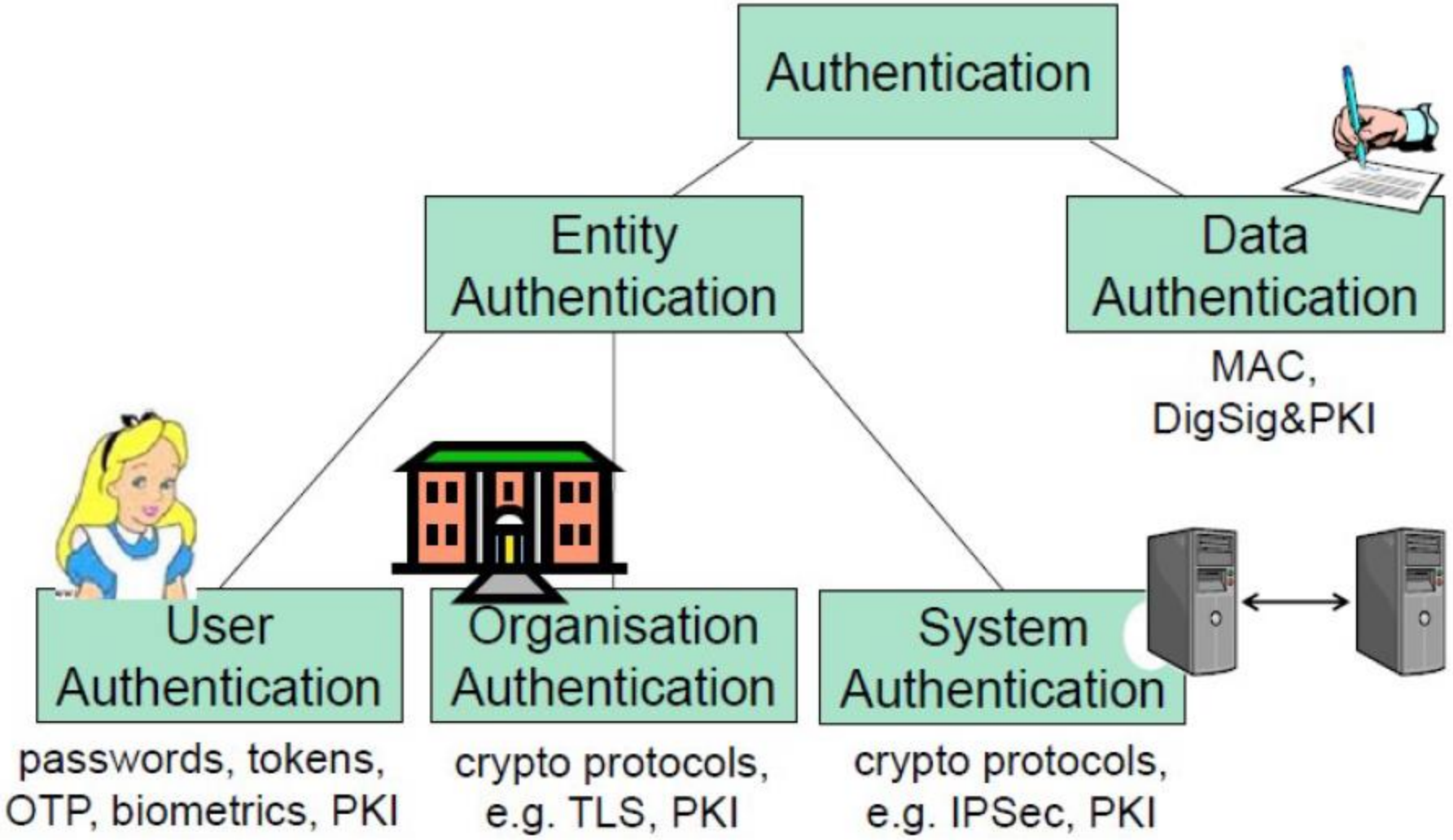
- User authentication:
  - The process of verifying a claimed identity of a (legal) user when accessing a system or an application.

- Organisation authentication:
  - The process of verifying a claimed identity of a (legal) organisation in an online interaction/session

- System authentication (peer entity authentication):
  - The corroboration (verification) that a peer entity (system) in an association (connection, session) is the one claimed (X.800).

- Data origin authentication (message authentication):
  - The corroboration (verification) that the source of data received is as claimed (X.800).

Authentication



Non-Repudiation

Goal: Making sending and receiving messages undeniable through unforgible evidence.

- Non-repudiation of origin: proof that data was sent.
- Non-repudiation of delivery: proof that data was received.
- NB: imprecise interpretation: Has a message been received and read just because it has been delivered to your mailbox?

Main threats:

- Sender falsely denying having sent message
- Recipient falsely denying having received message

Control: *digital signature*

- Cryptographic evidence that can be confirmed by a third party

Data origin authentication and non-repudiation are similar

- Data origin authentication only provides proof to recipient party
- Non-repudiation also provides proof to third parties

Accountability

Goal: Trace action to a specific user and hold them responsible

- *Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party*

(TCSEC/Orange Book)

Main threats:

- Inability to identify source of incident
- Inability to make attacker responsible

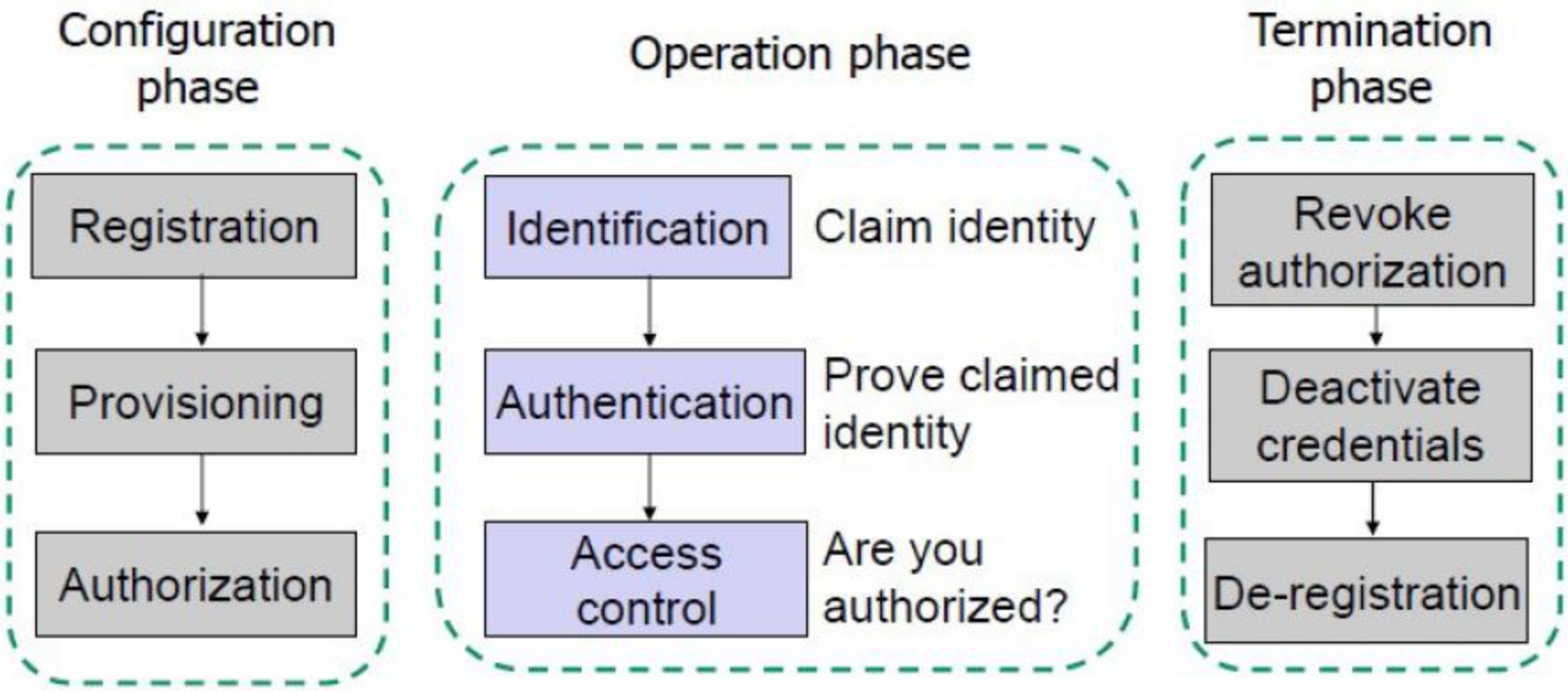
Controls:

- *Identify and authenticate users*
- *Log all system events (audit)*
- *Electronic signature*
- *Non-repudiation based on digital signature*
- *Forensics*

Authorization

- Authorization is to specify access and usage permissions for entities, roles or processes
  - Authorization policy normally defined by humans
  - Issued by an authority within the domain/organisation
- Authorities authorize, systems don't
- Authority can be delegated
  - Management → Sys.Admin
  - Implemented in IT systems as configuration/policy

Identity and Access Management (IAM)



Security against what?

- **Attack :** An abstract concept which is represented by some pieces of information that may vary according to the situation

- Attack results from a threat who exploits a vulnerability

Threats

- Threat: any circumstance or event with the potential to cause harm to a target system
- An attacker or a threat should have:
  1. A method: the necessary skills to pull off the attack.
  2. An opportunity: the time and the vulnerabilities to perform an attack
  3. A motivation: a reason to perform the attack
- Reasons could be very diverse!
  - Revenge
  - Entertainment
  - Economic gain
  - Political/religious

Threats actions

- **Interception:** Gaining unauthorised access to an asset.
  - *Illicit copying, wiretapping,...*
- **Interruption:** Making an asset unavailable/unusable.
  - *Malicious or accidental destruction of hardware, programs or data, DoS.*
- **Modification:** Changing the content or value of an asset.
  - *Alter content of database, modify data in transit,...*
- **Fabrication:** Creation of counterfeit assets.
  - *Add records to database, insert false messages in network,...*

Vulnerability

- A feature or a combination of features of a system that allows an adversary to place the system in a state that is contrary to its normal behavior
- "A vulnerability is a feature or bug in a system or program which enables an attacker to bypass security measures."

  Schultz Jr. et al. 1990

- A vulnerability is "an aspect of a system or network that leaves it open to attack"

  CERT 1993

Classifying vulnerabilities

Application-level vulnerabilities

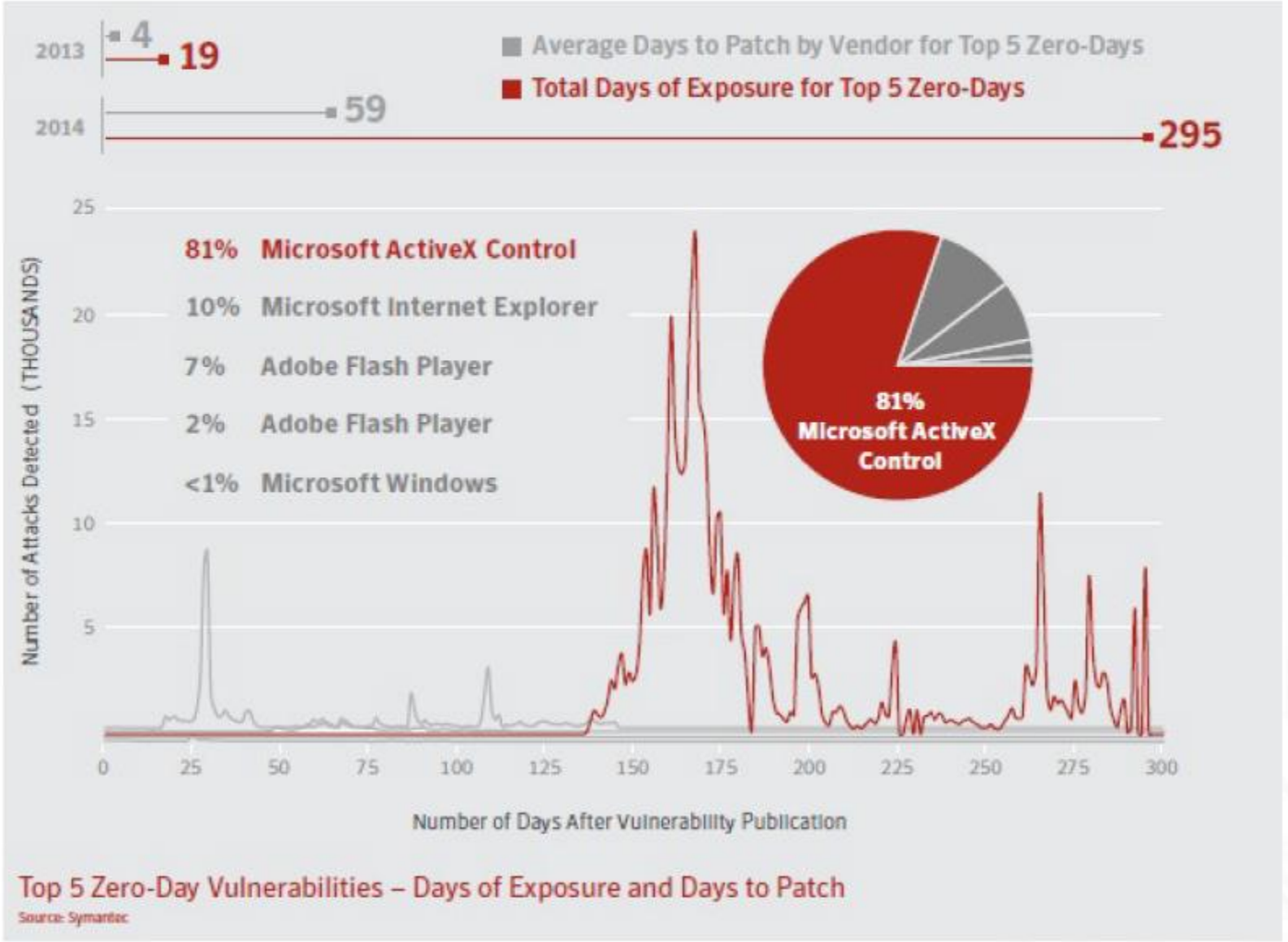
- Operating systems
- Web applications (e.g., servers, servlets)
- Database applications
- Network protocol implementations

Protocol vulnerabilities

Human-related vulnerabilities

- Equipment misconfiguration (i.e firewall, router, switch ...)
- Weak password protection
- Confidentiality violations

Zero-day vulnerabilities



Top 5 Zero-Day Vulnerabilities – Days of Exposure and Days to Patch

Source: Symantec

Threat

- Any event that can result in a loss for the target system
- Q1: What are the vulnerabilities exploited by this event?
- Q2: What is the probability that it would effectively occur ?
- Q3: What would be the resulting damage ?

Intrusion

- An activity that does not respect the system's security policy
- Q1: Which pre-conditions are necessary ?
- Q2: Which actions have been made possible by the intrusion?

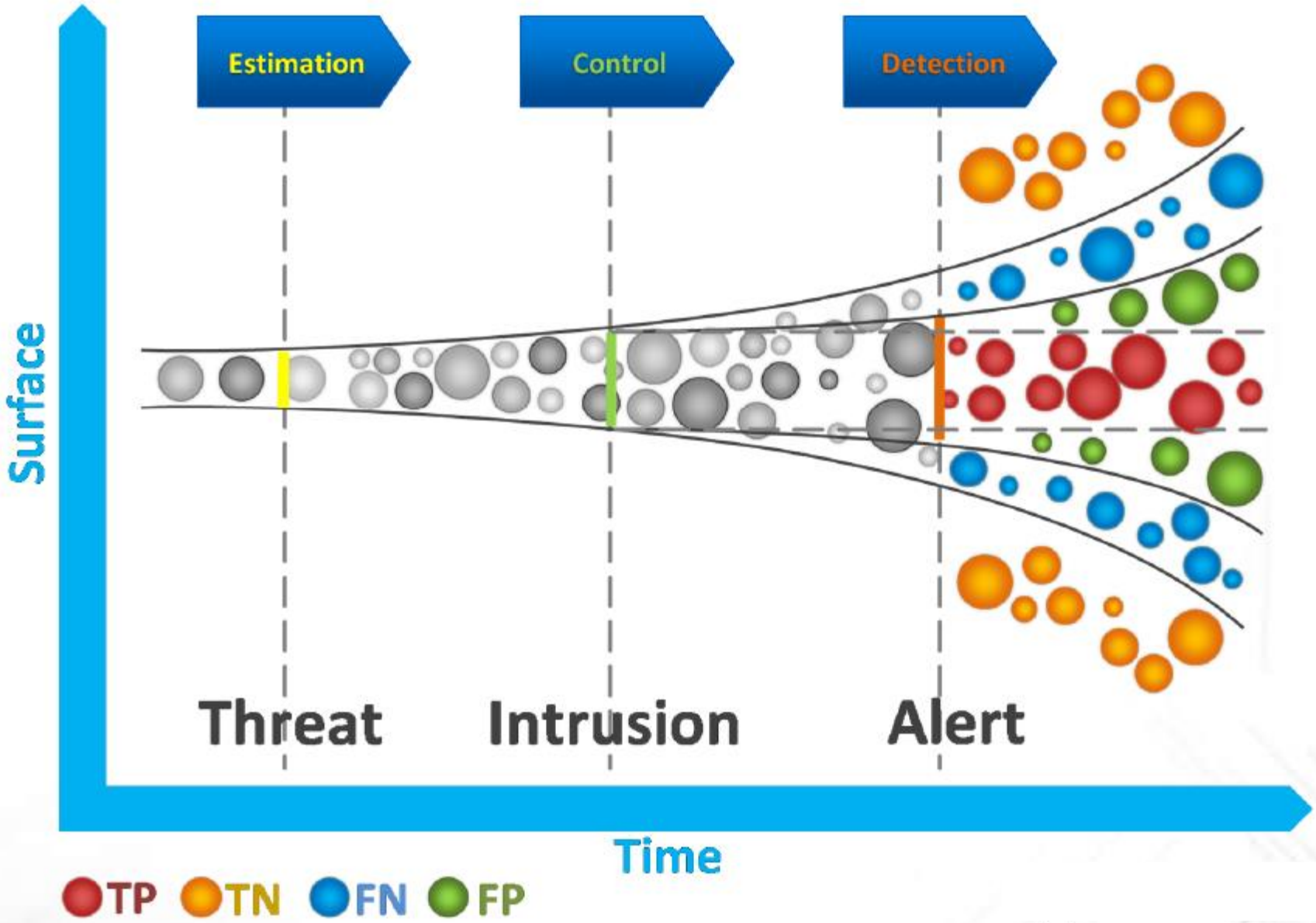
Alert

- A description of an attack which is conveyed by monitoring a set of system parameters
- Q1: What is the accuracy level corresponding to the alert?
- Q2: How to address resiliency and survivability?
- Q3: How to recover once the issue is fixed?

Different visions of cyber-attacks

- Cyber-attack: An abstract concept which is represented by some pieces of information that may vary according to the situation
- Threat: outcome, probability
- Intrusion: elementary actions, composition rules
- Alert: FP probability, FN probability, alert/attack weight

The TIA triad



Security Services and controls

Security services (aka. goals or properties)

- implementation independent
- supported by specific controls

Security controls (aka. mechanisms)

- Practical mechanisms, actions, tools or procedures that are used to provide security services

Security services:

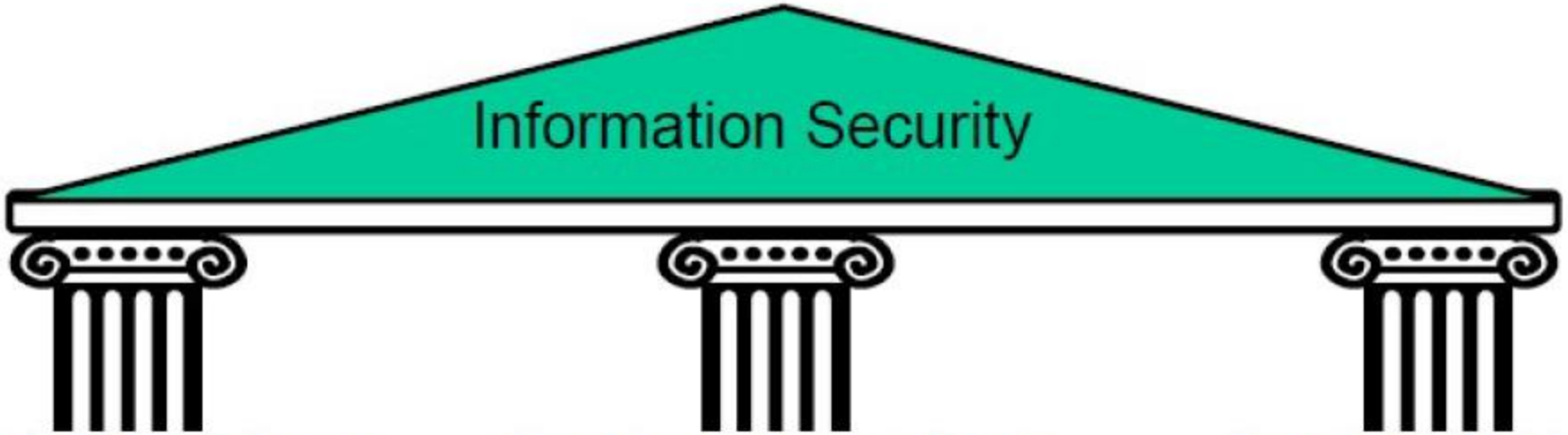
e.g. Confidentiality – Integrity – Availability

support

Security controls:

e.g. Encryption – Firewalls – Awareness

Security Control Categories



Physical controls
- Facility protection
- Security guards
- Locks
- Monitoring
- Environmental controls
- Intrusion detection

Technical controls
- Logical access control
- Cryptographic controls
- Security devices
- User authentication
- Intrusion detection
- Forensics

Administrative controls
- Policies & standards
- Procedures & practice
- Personnel screening
- Awareness training
- Secure System Dev.
- Incident Response

Security Controls functional type

- Preventive controls:
  - prevent attempts to exploit vulnerabilities
    - Example: encryption of files

- Detective controls:
  - warn of attempts to exploit vulnerabilities
    - Example: Intrusion detection systems (IDS)

- Corrective controls:
  - correct errors or irregularities that have been detected.
    - Example: Restoring all applications from the last known good image to bring a corrupted system back online

- Use a combination of controls to help ensure that the organisational processes, people, and technology operate within prescribed bounds.

Security countermeasures

Proactive	Detective	Reactive	Compensatory
Security Awareness Training	System Monitoring	OS Upgrade	Backup Generator
Firewall	IDS	Backup Data Restoral	Hot Site
Anti-virus	Anti-Virus	Anti-Virus	Server Isolation
Security Guard	Motion Detector	Vulnerability Mitigation	
IPS	IPS		