IC 3205 : Introduction to Information Systems Security

Module Outline

- ✓ Introduction to Information Security and trends
- ✓ Encryption mechanisms
- ✓ Network security / application security / Internet of Things (IoT) / ethical hacking

Required tools : Kali Linux, DVWA - Damn Vulnerable Web Application, Burp suite

Assessment Criteria

- Final exam – 60%
- Continuous assessment – 40%
  - ✓ Mid exam – 10%
  - ✓ 02 Quizzes – 10%
  - ✓ Group project -20%

Meaning of Information System Security

- The meaning of the term IS security has evolved in recent years.
- Before the problem of data security became widely publicized in the media, most people's idea of computer security focused on the physical machine.
- Traditionally, computer facilities have been physically protected for three reasons:

- To prevent theft of or damage to the hardware
- To prevent theft of or damage to the information
- To prevent disruption of service

Intro ; Information System Security

- Information System / Computer Security: 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).

Why We Need Information Security?

- Because there are threats
- A threat is an object, person, or other entity that represents a constant danger to an asset

Rising Cost of Cybercrime and Business Impact

IBM states that the global average cost of a data breach crossed $4.88 million in 2024. According to Anne Neuberger, US Deputy National Security Advisor for cyber and emerging technologies, the annual average cost of cybercrime will cross $23 trillion in 2027. However, beyond financial losses, businesses also lose customer trust because of breaches, impacting their reputation and long-term revenue growth.

The rise of generative AI and advanced tools used by attackers is making it necessary for organizations to invest in stronger defenses. IDC states that the global cybersecurity spending will grow 12.2% in 2025 and cross $377 billion by 2028. The US and Western Europe will lead, accounting for over 70% of global security spending, and Latin America, Central & Eastern Europe, and the Middle East & Africa will experience strong growth.

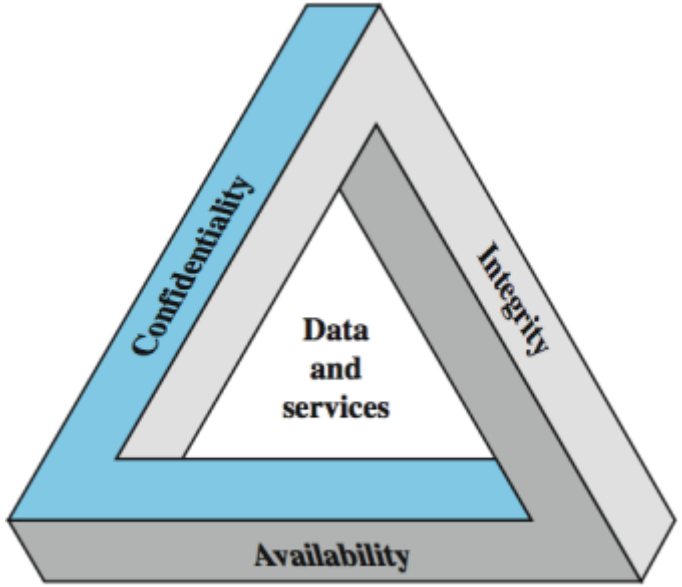
Moreover, Gartner forecasts a 15% rise in global cybersecurity spending, mainly covering security services and software, and network security. Another report by Statista reveals that nearly half of global business leaders will focus on data protection or trust in 2025. Besides, 43% will invest in technology modernization and 34% in ongoing security training.

Ref : https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

Threat Categories

- Acts of human error or failure
- Compromises to intellectual property
- Deliberate acts of espionage or trespass
- Deliberate acts of information extortion
- Deliberate acts of sabotage or vandalism
- Deliberate acts of theft
- Deliberate software attack
- Forces of nature
- Deviations in quality of service
- Technical hardware failures or errors
- Technical software failures or errors
- Technological obsolescence

Key Security Concepts (01)



Key Security Concepts (02)

- Confidentiality : It is used to prevent the disclosure of information to unauthorized individuals or systems. It has been defined as “ensuring that information is accessible only to those authorized to have access”. The other aspect of confidentiality is the protection of traffic flow from analysis.
  - Ex: A credit card number has to be secured during online transaction
- Integrity : means that data cannot be modified without authorization. Like confidentiality, it can be applied to a stream of messages, a single message or selected fields within a message.
- Availability : is defined to be the property of a system or a system resource being accessible and usable upon demand by an authorized system entity. The availability can significantly be affected by a variety of attacks, some amenable to automated counter measures such as authentication and encryption and others need some sort of physical action to prevent or recover from loss of availability of elements of a system

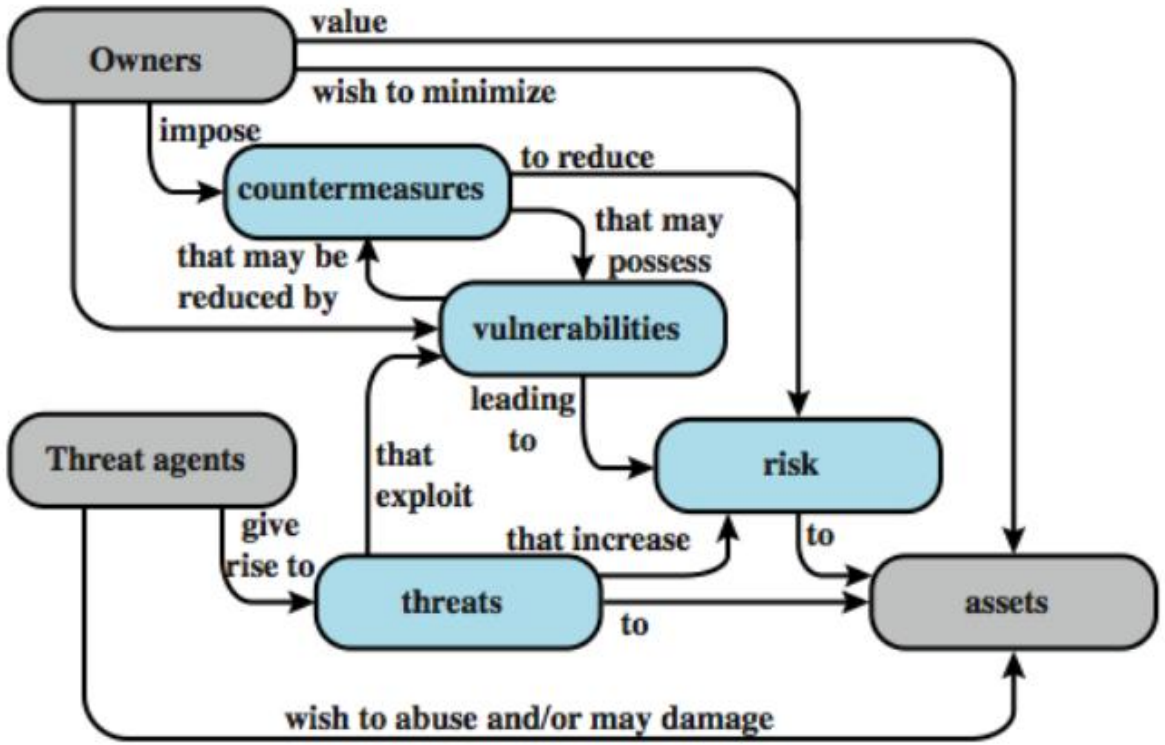
Key Security Concepts (02)

- Authentication : assures that a communication is authentic. For a single message transmission, its function is to assure the recipient that the message is from intended source. For an ongoing interaction two aspects are involved. First, during connection initiation the service assures the authenticity of both parties. Second, the connection between the two hosts is not interfered allowing a third party to masquerade as one of the two parties .
- Non-repudiation : Non-repudiation prevents either sender or receiver from denying a transmitted message.
- Access Control : 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. It is the ability to limit and control the access to host systems and applications via communication links. For this, each entity trying to gain access must first be identified or authenticated, so that access rights can be tailored to the individuals

IS Security Challenges

- Not simple
- Must consider potential attacks
- Involve algorithms and secret info
- Must decide where to deploy mechanisms
- Battle of understanding between attacker / admin
- Not perceived on benefit until fails
- Requires regular monitoring
- Too often an after-thought
- Regarded as impediment to using system

Security Terminology



Vulnerabilities and Attacks

- System resource vulnerabilities may
  - ✓ be corrupted (loss of integrity)

    Data or systems are modified without authorization. Example: An attacker changes bank transaction records.
  - ✓ become leaky (loss of confidentiality)

    Information is exposed to unauthorized parties. Example: A hacker steals passwords from a database.
  - ✓ become unavailable (loss of availability)

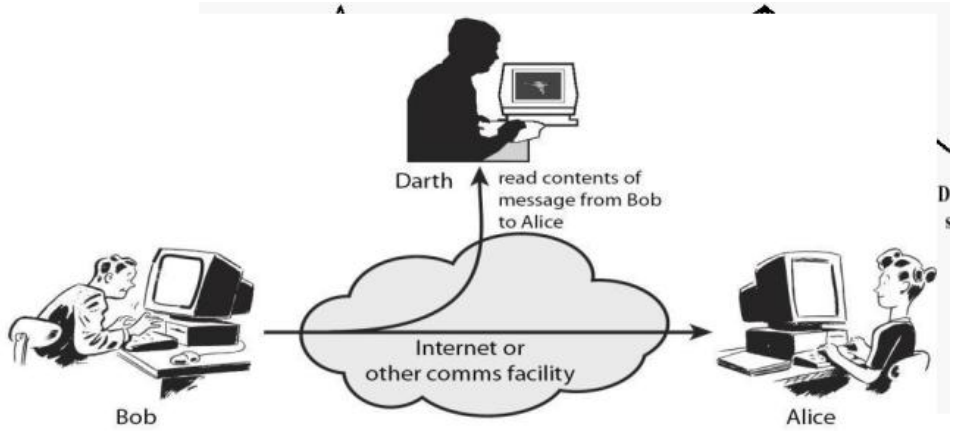
    Systems or services are disrupted or shut down. Example: A denial-of-service (DoS) attack takes a website offline.
- Attacks are threats carried out and may be
  - ✓ passive
  - ✓ active
  - ✓ insider
  - ✓ outsider

Security Attacks (01)

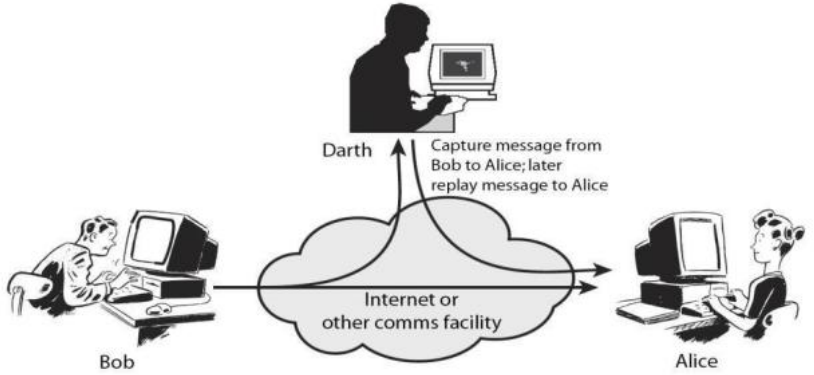
- We want our security system to make sure that no data are disclosed to unauthorized parties
- Data should not be modified in illegitimate ways
- Legitimate user can access the data
- Types of attacks
- Attacks are grouped into two types:
  - Passive attacks: does not involve any modification to the contents of an original message
  - Active attacks: the contents of the original message are modified in some ways

Security Attacks (02)

Passive Attack



Active Attack



Passive Attacks

- Passive Attacks
- A Passive attack attempts to learn or make use of information from the system, but does not affect system resources.
- Two types:
- Release of message content

  It may be desirable to prevent the opponent from learning the contents (i.e. sensitive or confidential info) of the transmission
- Traffic analysis

  A more subtle technique where the opponent could determine the location and identity of communicating hosts and could observe the frequency & length of encrypted messages being exchanged there by guessing the nature of communication taking place

- Passive attacks are very difficult to detect because they do not involve any alternation of the data. As the communications take place in a very normal fashion, neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. So, the emphasis in dealing with passive attacks is on prevention rather than detection.

Active Attacks

- Active Attacks
- Active attacks involve some modification of the data stream or creation of a false stream. An active attack attempts to alter system resources or affect their operation
- Four types:
- Masquerade: an entity pretends to be some other entity. It usually includes one of the other forms of active attack
- Replay: It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
- Modification of messages: It means that some portion of a legitimate message is altered, or that messages are delayed to produce an unauthorized effect
  - Ex: “John’s acc no is 2346” is modified as “John’s acc no is 7892”
- Denial of service: This attack prevents or inhibits the normal use or management of communication facilities
  - Ex: a: Disruption of entire network by disabling it / b: Suppression of all messages to a particular destination by a third party

Attacks / Threats Can be apportioned in to .. (04)

- Interruption
  An asset of the system is destroyed or becomes unavailable or unusable. It is an attack on availability
  Examples: destruction of some hardware / jamming wireless signals / disabling file management systems
- Interception
  An unauthorized party gains access to an asset. Attack on confidentiality.
  Examples: wire tapping to capture data in a network / Illicitly copying data or programs / eavesdropping
- Modification
  When an unauthorized party gains access and tampers an asset. Attack is on Integrity.
  Examples: changing data file / altering a program and the contents of a message
- Fabrication
  An unauthorized party inserts a counterfeit object into the system. Attack on authenticity. Also called impersonation
  Examples: Hackers gaining access to a personal email and sending message / Insertion of records in data

Countermeasures

- Means used to deal with security attacks
  - ✓ prevent
  - ✓ detect
  - ✓ recover
- May result in new vulnerabilities
- Will have residual vulnerability
- Goal is to minimize risk given constraints

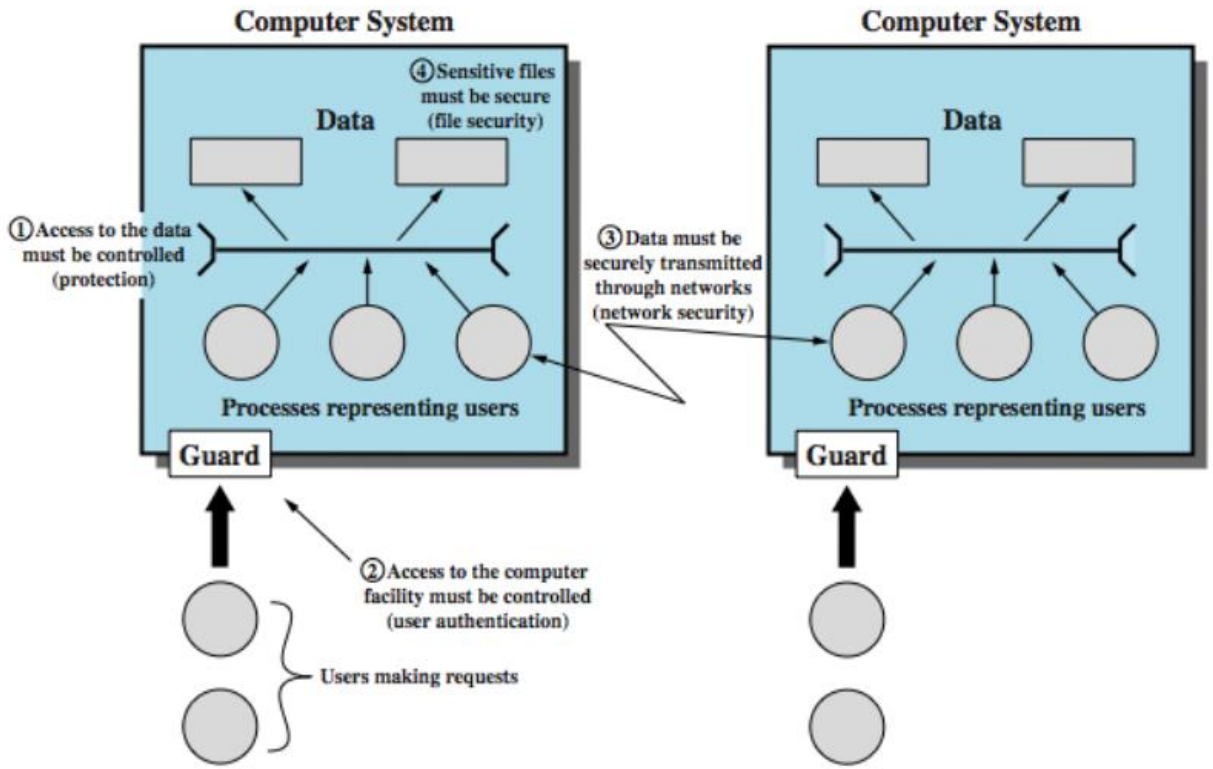
The residual risk is the amount of risk or danger associated with an action or event remaining after natural or inherent risks have been reduced by risk controls

$$\text{residual risk} = (\text{inherent risk}) - (\text{impact of risk controls})$$

Threat Consequences

- Unauthorized disclosure
  - ✓ exposure, interception, inference, intrusion
- Deception
  - ✓ masquerade, falsification, repudiation
- Disruption
  - ✓ incapacitation, corruption, obstruction
- Usurpation
  - ✓ misuse

Scope of Computer Security



Network Security Attacks

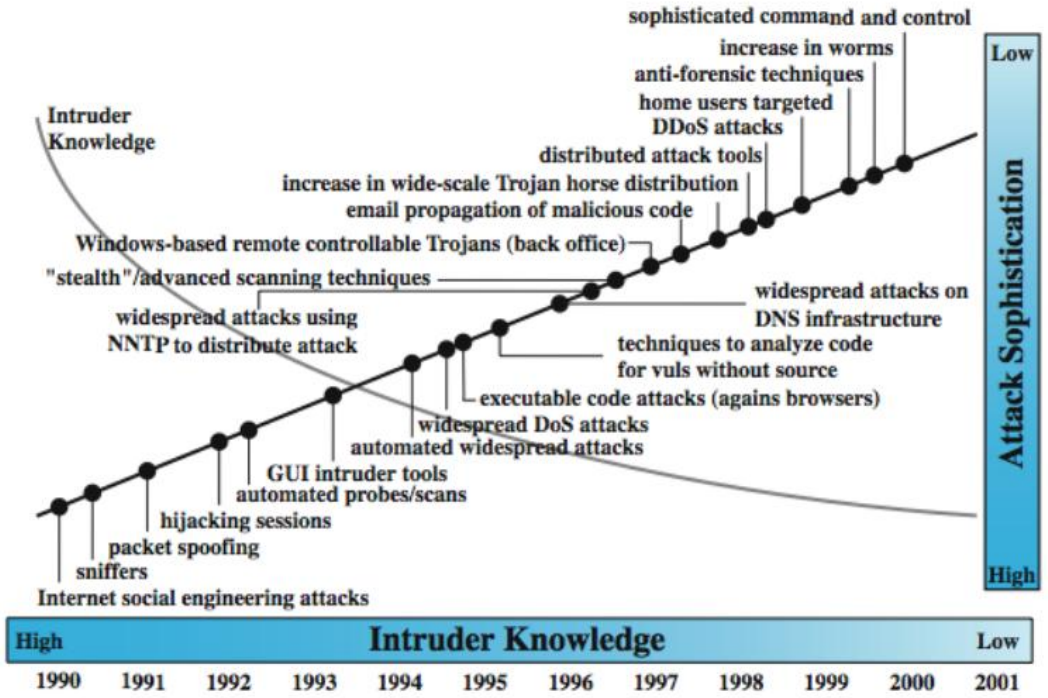
- Classify as passive or active
- Passive attacks
  - ✓release of message contents
  - ✓ eavesdropping
  - ✓ traffic analysis
  - ✓ are hard to detect so aim to prevent
- Active attacks modify/fake data
  - ✓ masquerade
  - ✓ replay
  - ✓ modification
  - ✓ denial of service
  - ✓ hard to prevent so aim to detect

A replay attack is a form of network attack in which valid data transmission is maliciously or fraudulently repeated or delayed

Security Functional Requirements

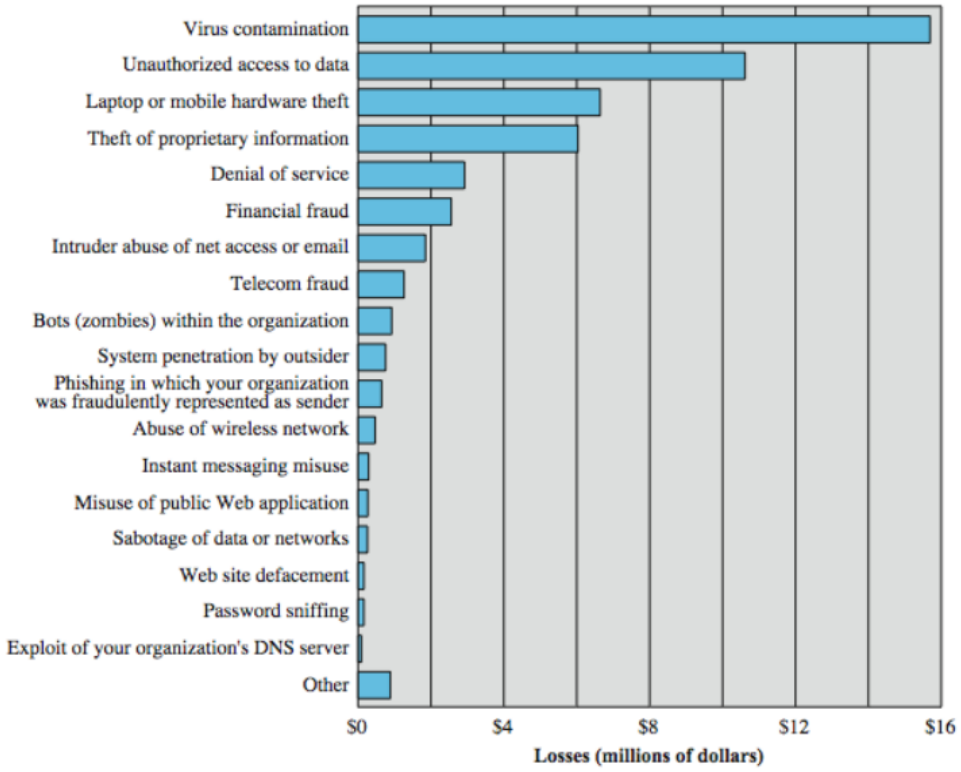
- Technical measures:
  - ✓ access control; identification & authentication; system & communication protection; system & information integrity
- Management controls and procedures
  - ✓ awareness & training; audit & accountability; certification, accreditation & security assessments; contingency planning; maintenance; physical & environmental protection; planning; personnel security; risk assessment; systems & services acquisition
- Overlapping technical and management:
  - ✓ configuration management; incident response; media protection

Security Trends



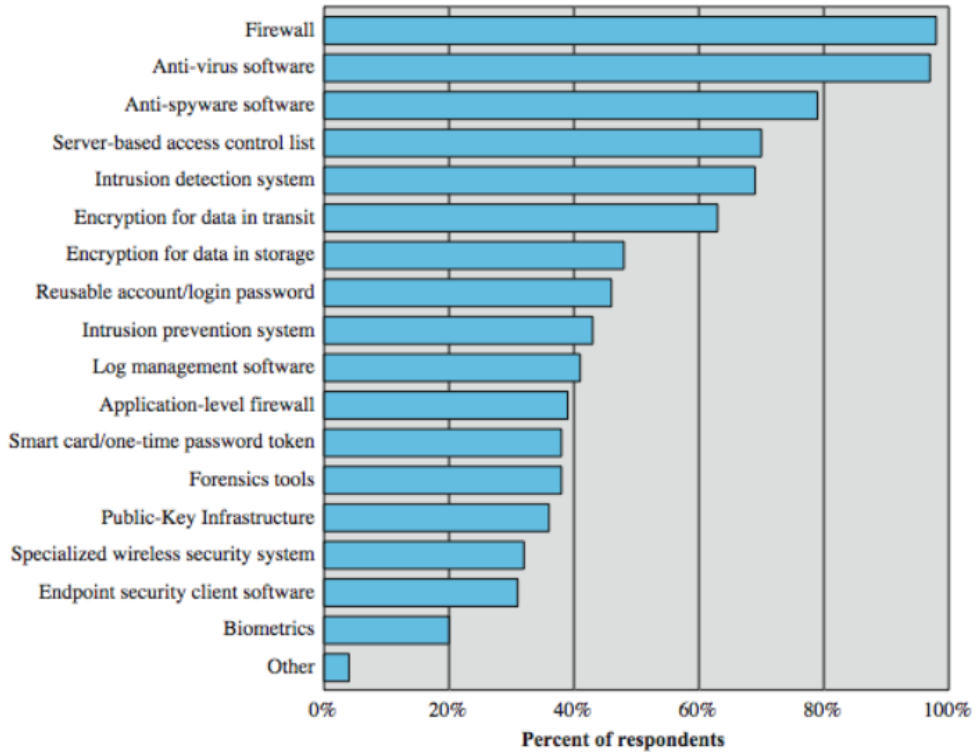
Source : https://images.app.goo.gl/z7HuHJNpy6oh8gsa6

Computer Security Losses

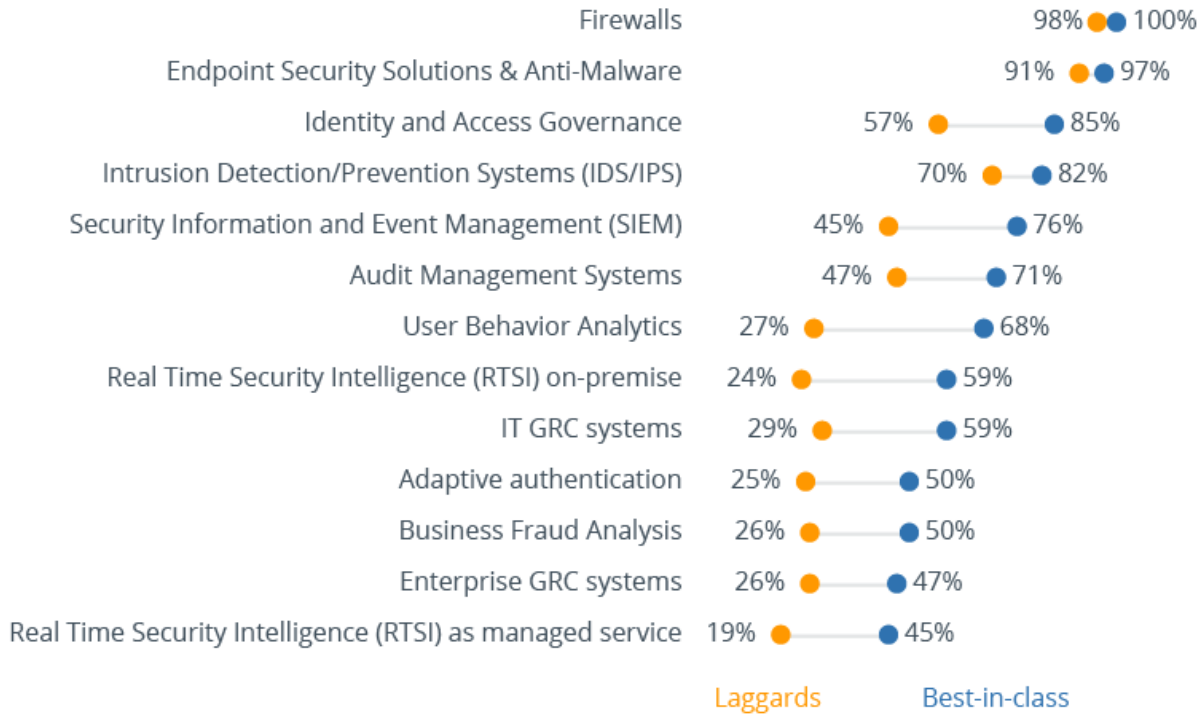


Source: Computer Security Institute/FBI 2006 Computer Crime and Security Survey

Security Technologies Used



Source: Computer Security Institute/FBI 2006 Computer Crime and Security Survey



Source : https://images.app.goo.gl/zYZ7c8zruMMNVGXq5