System Access Threats

Intruders

Masquerader

an individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account

Misfeasor

a legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges

Clandestine user

an individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection

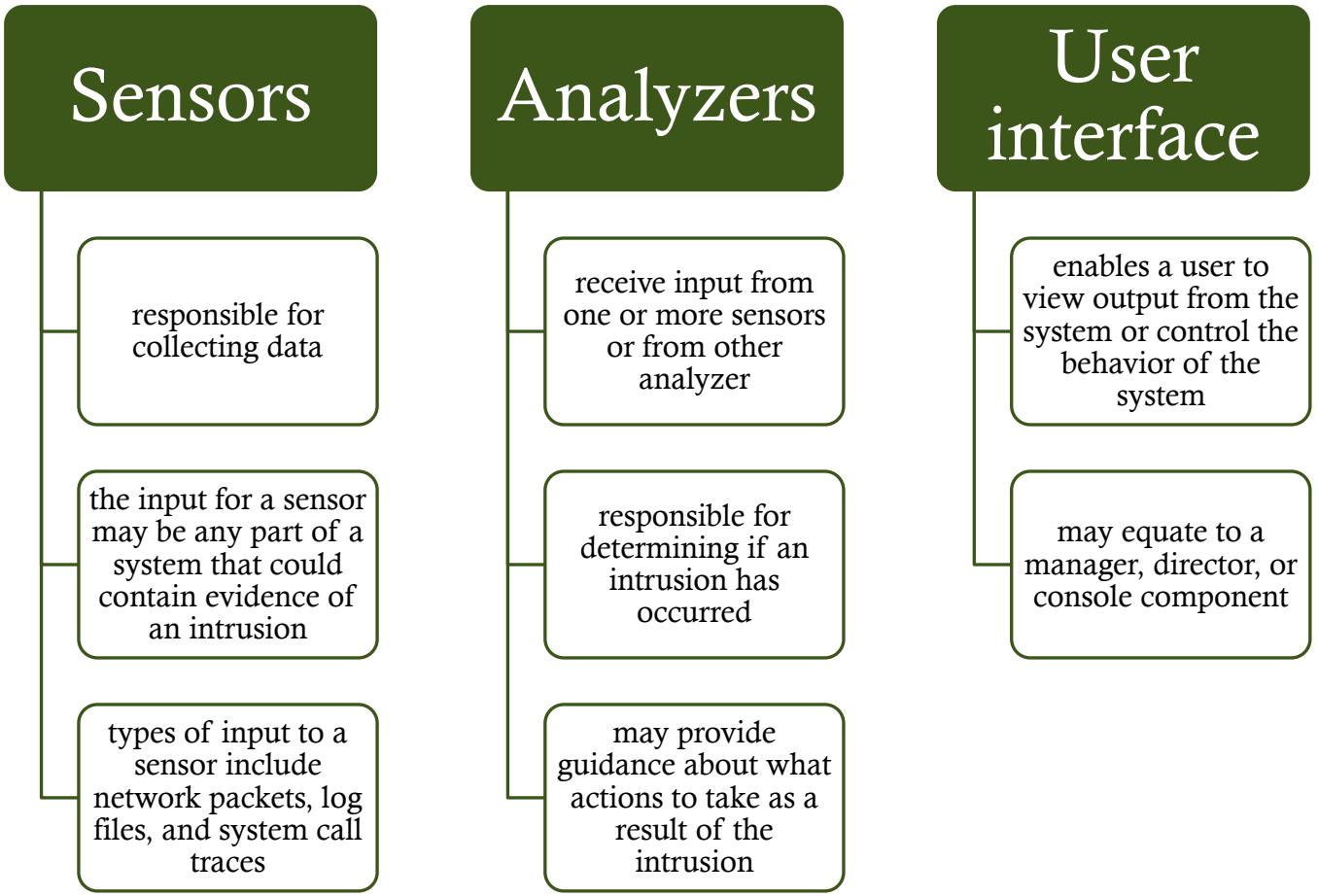
Malicious Software

- Programs that exploit vulnerabilities in computing systems
- Also referred to as malware
- Can be divided into two categories:
  - parasitic
    - fragments of programs that cannot exist independently of some actual application program, utility, or system program
    - viruses, logic bombs, and backdoors are examples
  - independent
    - self-contained programs that can be scheduled and run by the operating system
    - worms and bot programs are examples

Countermeasures

- RFC 4949 (*Internet Security Glossary)* defines intrusion detection as a security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner
- Intrusion detection systems (IDSs) can be classified as:
  - host-based IDS
    - monitors the characteristics of a single host and the events occurring within that host for suspicious activity
  - network-based IDS
    - monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity

IDS Components



Authentication

- In most computer security contexts, user authentication is the fundamental building block and the primary line of defense
- RFC 4949 defines user authentication as 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
  - verification step
    - presenting or generating authentication information that corroborates the binding between the entity and the identifier

Means of Authentication

- Something the individual knows
  - examples include a password, a personal identification number (PIN), or answers to a prearranged set of questions
- Something the individual possesses
  - examples include electronic keycards, smart cards, and physical keys
  - 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

Access Control

- Implements a security policy that specifies who or what may have access to each specific system resource and the type of access that is permitted in each instance
- Mediates between a user and system resources, such as applications, operating systems, firewalls, routers, files, and databases
- A security administrator maintains an authorization database that specifies what type of access to which resources is allowed for this user
  - the access control function consults this database to determine whether to grant access
- An auditing function monitors and keeps a record of user accesses to system resources

Firewalls

Design goals:

1) The firewall acts as a choke point, so that all incoming traffic and all outgoing traffic must pass through the firewall

2) The firewall enforces the local security policy, which defines the traffic that is authorized to pass

3) The firewall is secure against attacks

- Can be an effective means of protecting a local system or network of systems from network-based security threats while affording access to the outside world via wide area networks and the Internet

- Traditionally, a firewall is a dedicated computer that interfaces with computers outside a network and has special security precautions built into it in order to protect sensitive files on computers within the network

Buffer Overflow Attacks

- Also known as a ***buffer overrun***
- Defined in the NIST (National Institute of Standards and Technology) *Glossary of Key Information Security Terms* as:

> "A condition at an interface under which more input can be placed into a buffer or data-holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system"

- One of the most prevalent and dangerous types of security attacks