University of BRISTOL

Systems & Software Security

COMSM0050

2020/2021

bristol.ac.uk

University of BRISTOL

Host-based intrusion detection

bristol.ac.uk

RFC 2828 definition

- **Security Intrusion:** A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.
- **Intrusion Detection:** 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.

Examples of intrusion

- Remote root compromise
- Web server defacement
- Guessing passwords
- Copying databases containing credit cards
- Viewing sensitive data without authorization
- etc.

Type of intrusion detection

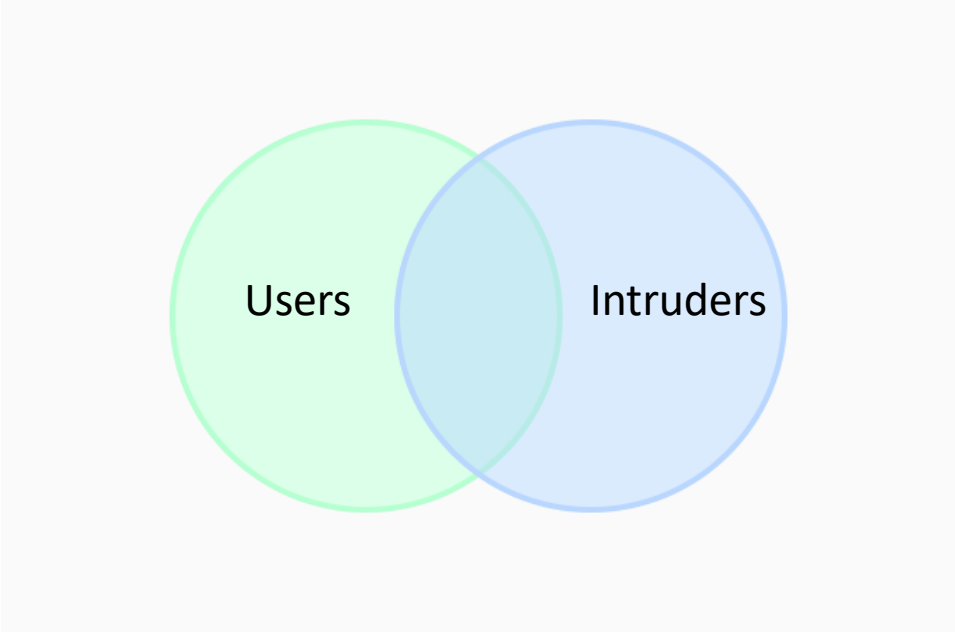
- Host-based
  - Use information recorded from the OS perspective
  - e.g. information logged by one reference monitor
- Network-based
  - Use information recorded at the network interface
  - e.g. record of network packets

Type of intrusion detection

- Host-based
  - Use information recorded from the OS perspective
  - e.g. information logged by one reference monitor
- Network-based
  - Use information recorded at the network interface
  - e.g. record of network packets
- Signature-based
  - Identify known attack pattern aka “signature”
- Anomaly-based
  - Identify pattern that deviate from some “normal”

Basic principle

- Assume intruder behavior differs from legitimate users
- Overlap in behavior is source of problem
  - False negative
  - False positive



IDS requirements

- Run continually
- Be fault tolerant
- Resist subversion
- Impose a minimum overhead on the system
- Adapt to changes in users and systems
- Scale to monitor complex systems
- Provide graceful degradation of service
- Allow dynamic reconfiguration

Types of audit record

- Native audit record
  - OS generally already collect information (see previous lecture)
  - Pros: no extra collection mechanism needed
  - Cons: may lack information relevant to detection
- Detection-specific audit record
  - Additional infrastructure to collect information relevant to the IDS
  - Pros: can be customised to IDS need
  - Cons: extra-overhead and complexity

Signature or Anomaly-based?

- Anomaly-based systems build a model of how the system normally behave
  - Pros: can identify unknown attack
  - Cons: require system behavior to be reasonably fixed (e.g. server)
- Signature-based systems identify rules to match attack patterns
  - Pros: can accommodate changing system behavior
  - Cons: can only detect known pattern
- No silver-bullet there