UNIT IV

TECHNICAL SECURITY

Intrusion Detection-Digital Rights Management

INTRUSION DETECTION

An **intrusion detection system** (**IDS**) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violationis typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sourcesand uses alarm filtering techniques to distinguish malicious activity from false alarms

IDS types range in scope from single computers to large networks. The most common classifications are **network intrusion detection systems** (**NIDS**) and **host-based intrusion detection systems** (**HIDS**).
A system that monitors important operating system files is an example of an HIDS, while a system that analyzes incoming network traffic is an example of an NIDS. It is also possible to classify IDS by detection approach. The most well-known variants are signature-based detection

Some IDS products have the ability to respond to detected intrusions. Systems with responsecapabilities are typically referred to as an **intrusion prevention system.**

Host intrusion detection systems

Host intrusion detection systems (HIDS) run on individual hosts or devices on the network. AHIDS monitors the inbound and outbound packets from the device only and will alert the useror administrator if suspicious activity is detected.

Detection method

Signature-based IDS refers to the detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware.This terminology originates from anti-virus software, which refers to these detected patterns as signatures. Although signature-based IDS can easily detect known attacks, it is difficult to detect new attacks, for which no pattern is available.

Classification

Intrusion prevention systems can be classified into four different types:

1. **Network-based intrusion prevention system (NIPS)**: monitors the entire network forsuspicious traffic by analyzing protocol activity.
2. **Wireless intrusion prevention system (WIPS)**: monitor a wireless

network forsuspicious traffic by analyzing wireless networking protocols.

3. **Network behavior analysis (NBA)**: examines network traffic to identify threats thatgenerate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations.
4. **Host-based intrusion prevention system (HIPS)**: an installed software package whichmonitors a single host for suspicious activity by analyzing events occurring within that host.

Detection methods

The majority of intrusion prevention systems utilize one of three detection methods: signature-based, statistical anomaly-based, and stateful protocol analysis.

1. **Signature-based detection**: Signature-based IDS monitors packets in the Network andcompares with pre-configured and pre-determined attack patterns known as signatures.
2. **Statistical anomaly-based detection**: An IDS which is anomaly-based will monitornetwork traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network

Stateful protocol analysis detection: This method identifies deviations of protocol statesby comparing observed events with "pre-determined profiles of generally accepted definitions of benign activity"

DIGITAL RIGHTS MANAGEMENT

Digital rights management encompasses a set of hardware and software technologies designed to control how we use, edit, and share content or information assets via online or offline channels. DRM also includes technological protection measures, as it intends to protect the copyright for technology-enabled content.

1. **Copy prevention** – This is among the oldest types of DRM. The user can view or consume the content from the primary channel (streaming platform, DVD, website, etc.)but cannot make a copy.

2. **Copy restrictions** – This is similar to copy prevention, but the user is allowed to make acertain number of copies in certain conditions.

3. **Password protection** – This is a simple but highly effective DRM technique, where the user must know a unique password to access a document. This type of DRM is frequentlyused by financial services providers to keep consumer transactions safe.

4. **Watermarks** –Watermarks are regularly used for stock photographs, GIFs, and videos, enabling users to pursue content libraries without using them for commercialpurposes.

5. **Device control** – This advanced technology prevents users from opening a file unless they are on an approved device. Enterprise DRM relies heavily on device-based control,as does certain OTT media.For example, device manufacturers must obtain DRM certification from Netflix.

DRM techniques:

- **Restrictive licensing** – The content provider creates a license that legally prevents usersfrom using it for commercial or public distribution purposes. Technically, the user mightstill be able to reuse the content, but they would be legally liable.
- **Digital trust infrastructure** –This technique gives users the autonomy to play around with content asthey wish while keeping the reigns of control squarely in the hands of thecontent provider. Digital trust infrastructure is extremely relevant for enterprises, particularly with the advent of block chain technology.
- **One way hashing** - It takes digital content as the input and generates a final output message for user consumption. If the content is altered in any way, the output message will change, thereby revealing that the content is inauthentic. One way hashing is used toverify digital content and assure users/consumers of its untampered nature.
- **Secure communication protocols** – Communication protocols like SSL and TSLmaintain the sanctity of information flowing through the internet. Secure communication protocols are a DRM staple and must be part of your content technology stack, either using a private or a public CMS landscape.
- **Timebound decryption keys** – Encrypting data is an excellent way to keep it out of unethical hands. The time-bound decryption keys that protect digital rights. The key would allow users to decrypt the content for a specific period of time, as specified by thelicensing/purchase terms.