FIT5037: Network Security
Intrusion detection

Faculty of Information Technology
Monash University

May 21, 2019

Copyright Notice

Lecture 11: Intrusion detection

Lecture Topics:

- Symmetric key cryptography
- Asymmetric key cryptography
- Pseudorandom Number Generators and hash functions
- Authentication Methods and AAA protocols
- Security at Network layer (IPsec)
- Security at Network layer (firewalls and wireless security)
- Security at Transport layer
- Security at Application layer
- Computer system security and malicious code
- Computer system vulnerabilities and penetration testing
- **Intrusion detection**
- Denial of Service Attacks and Countermeasures / Revision

Outline

- Principles of IDS/IPS
- Detection Methods
- Network-based IDS/IPS
- Wireless IDS/IPS
- Host-based IDS/IPS

Intrusion Detection and Prevention Principles[1]

- *intrusion detection*: process of monitoring and then analysis of system or network events for signs of possible *incidents*
- *incidents*: violations or threats of violation of
  - computer system security policies
  - acceptable use policies
  - standard security practices
- incident causes:
  - malware
  - attackers gaining unauthorised access from external network (Internet)
  - authorised users misuse their privileges
  - authorised users attempt to gain additional access
  - etc.
- *Intrusion Detection System*: software that automates the intrusion detection process
- *Intrusion Prevention System*: an IDS with additional capability to *attempt* to stop possible incidents
- NIST SP 800-94 uses IDPS term to refer to both

[1] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Uses of IDS/IPS[2]

- focused on identifying possible incidents
  - detect when an attacker has compromised a system by exploiting a vulnerability
    - IDS/IPS generates a report for system administrators
  - log information that can be used in handling the incident
  - could be configured to detect violation of security policy
    - e.g. using a rule-based access control rule similar to firewalls to detect network traffic that violates acceptable use policy
  - could potentially detect reconnaissance activity
    - this may be part of a malware propagation engine
    - may also indicate attackers targeting the organisation
  - could potentially respond to an attack (in IPS role) by attempting to stop it
- may also be used to identify security policy problems
  - e.g. producing alert reports for traffic that should be dropped by firewall
- help identify threat level to an organisation
  - based on frequency and characteristics of attack against organisation
    - caution not to create a false sense of security (lack of detection does not necessarily mean lack of threat)
- play as deterrent for individuals from violating security policy
  - if individuals are aware that their actions are monitored

[2] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

IPS General Response Strategies[3]

IPS differs from IDS in having the capability to respond to attacks, possible strategies are:

- terminating network connection or user session that is used for an attack
- block access to target system from offending user account or IP address
- block all access to target host, service, application
  - this could lead to DoS
- change the security environment by changing the configuration of other security controls
  - e.g. changing firewall rules or gateway router
- change attack content by removing or replacing malicious part of packets
  - e.g. removing an infected file attachment from an email

[3] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

IDS/IPS Shortcomings[4]

- the detection may not be 100% accurate
- detection of benign traffic as malicious is referred to as *false positive*
  - sends false alarms that wastes administrators time to investigate
  - denies access to legitimate users (IPS) may also need to be resolved by administrators
- failure in detection of malicious activity
  - allows an attacker/malware to gain access
- generally reduction in rate of one leads to increase in rate of the other
  - choosing to reduce false negatives (more security) may increase false positives (more time to analyse the alerts)
  - altering the configuration to improve detection accuracy is referred to as *tuning*
- *evasion* techniques may be used by an attacker to bypass an IDS/IPS
  - e.g. slowing down port/network scanning to evade rate-based rules
  - changing the encoding of messages that target will understand but not IDS/IPS
  - IDS/IPS may have rules to detect some of evasion techniques (but not all may be detected)

[4] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

IDS/IPS Common Functions

- Audit Record (Logging)
  - recording of security related events
  - audit records/logs can be stored locally or sent to Security Information Event Management (SIEM) solutions
- Notification or Alert
  - a method to send notification or alert messages to security administrators
    - e.g. emails, web interface, messages in IDS/IPS user interface, Simple Network Management Protocol (SNMP) traps, syslog messages
- Report production
  - produce a summary of events or provide details on particular events

IDS/IPS Detection Methods: Signature-based[5]

- *signature* is a pattern that corresponds to a known threat
- signature-based detection compares observed events with known and identified threat patterns
  - e.g. using `telnet` with user name `root` to access a resource (violation of security policy)
  - e.g. an email with a particular subject with file attachment that are characteristics of a malware
- is effective in detecting known threats
  - when pattern does not change
    - for instance during the beginning of propagation of a malware that does not mutate
- less effective when evasion techniques are used or threat is unknown
  - zero-day attacks and malware
  - poly or metamorphic malware
- is the simplest form of detection methods
  - does not understand the state of complex communications
  - has little understanding of applications and protocols
    - for example matching a web request with 403 response of forbidden or 404 of page not found
  - lack the ability to remember previous events when processing current ones

[5] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

IDS/IPS Detection Methods: Anomaly-based[6]

- process of comparing observed events against activity that is considered normal to identify significant deviation
- a *profile* represents normal behaviour of users, systems, networks etc.
  - profiles are developed by monitoring the characteristics of typical activities over a period of time
    - statistical analysis can be used in developing profiles
  - examples of behavioural attributes:
    - number of emails sent by a user
    - number of failed login attempts
    - level of processor usage for a host in a given period of time
- effective at detecting previously unknown threats
  - e.g. a new malware infection that
    - consumes processing power
    - sends large number of emails
    - initiate large number of network connections
    - etc.
- profiles can be *static* or *dynamic*
  - static profiles do not change after creation
  - dynamic profiles constantly adjust with observation of additional events

[6] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

IDS/IPS Detection Methods: Rule-based anomaly detection vs. Penetration Identification[7]

Chapter 9 of Stallings book discusses two method of Rule-based detection

- **Rule-based anomaly detection**: rules are *automatically* generated from normal behaviour profiles
  - historical audit records are analysed to generate these rules
  - current behaviour is checked against these rules (not statistical results)
  - any considerable deviation signals intrusion
  - does not require knowledge of security vulnerabilities within the system
- **Penetration Identification**: rules are created by *experts* based on knowledge of known penetrations that would exploit known weaknesses as well as common malicious behaviour
  - rules are specific to host, OS, network
  - rules are generated by experts rather than by analysing audit records or user/host/network profiling
  - involves input from system administrator and security analyst to collect a suite of known scenarios and key events that threaten security
  - may detect unknown threats (zero-day) attacks if the rules are violated
  - for instance rules written for common malicious behaviour

[7] Chapter 9 of the *Network Security Essentials-Application Standards*, 5th Edition by *William Stallings*

IDS/IPS Anomaly-based Detection: Shortcomings[8]

- the normal behaviour may inadvertently include malicious behaviour
  - for instance if there are infected systems during learning/training phase
- it is challenging to make the profiles accurate
  - for instance large file transmission once every month may trigger the IDS/IPS
- may generate large number of false positives in dynamic environment
  - benign activities deviate significantly from profile
- may be challenging to analyse why a particular alert is generated
  - whether it is false positive due to complexity of events

[8] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

IDS/IPS Detection Methods: Stateful Protocol Analysis[9]

- process of comparing profile of benign protocol activity against observed events for that protocol to identify deviation
- in contrast with anomaly-based detection it relies on vendor-developed profiles of particular protocols
- overlaps partly with firewall however performs more advanced analysis (up to application layer)
- can understand and track the state of network, transport, and application layer protocols (stateful)
  - for example understand the commands allowed in unauthenticated FTP sessions vs. authenticated ones
  - can pair requests with responses (change of state)
- can identify unexpected sequences of commands
  - e.g. issuing the same command repeatedly or issuing commands out of the defined order by protocol
- rely on protocol models developed by standard bodies e.g. IETF RFCs
  - protocol definitions may leave certain aspects to implementation leading to deviation
  - protocol models take these deviations into account
  - vendor-specific violations of protocol makes creation of model challenging
  - requires update if protocol model changes

[9] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

IDS/IPS General Deployment Types[10]

- **Network-based**: monitors network traffic to identify suspicious activity
  - can be limited to a network segment
    - for instance DMZ to detect suspicious traffic reaching exposed servers to the Internet
  - commonly deployed at a boundary between networks
- **Wireless**: monitors wireless network traffic to identify suspicious activity of wireless protocols
  - cannot (does not) identify suspicious activity of higher-layer network protocols
  - deployed within wireless range of the organisation
- **Host-based**: monitors characteristics of a single host to identify suspicious activity
  - network activity, system logs, running processes, application activity, file access and modification etc.
  - generally deployed on critical hosts such as servers

[10] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

IDS/IPS Solutions: Common Components[11]

IDS/IPS solutions may have multiple components

- **Sensor or Agent**: monitor and analyse activities
  - sensor is generally used for network-based IDS/IPS
  - agent is generally used for a host-based IDS/IPS
- **Management Server**: a centralised device that receives information from managed sensors and agents
  - may be able to *correlate* events observed by multiple agents
  - can be deployed as a software or an appliance
- **Database Server**: a repository to store received information from agents and sensors
- **Console**: a program that provides an interface for administrators to configure, monitor, and or generate report

Components can be deployed as part of a distributed solution or all in a single device/host

[11] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

IDS/IPS Solutions: Network Communication[12]

Communication between components

- over the organisation's standard network
  - IDS/IPS traffic may be detected/observed by an adversary
- a separate network strictly for security software referred to as *management network*
  - each component has an additional network interface connected to management network
  - no traffic is passed between the two networks by components
  - management network is isolated
  - advantages of separate network for management
    - conceal the existence of IDS/IPS solution from attacker
    - reserve adequate bandwidth to function in case of incidents e.g. under a DDoS attack
  - disadvantages of separate management network
    - additional cost of the management network
    - inconvenience for administrator having to use the separate network
  - VLANs can be used as an alternative in separating management network

[12] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

IDS/IPS Solutions: Security Capabilities[13]

- **Information Gathering**: gather information on hosts or networks from observed activities
  - e.g. identifying OS, application running on hosts, general characteristics of networks
- **Logging**: log data related to detected events
  - can be used in investigating incidents and correlate events between IDS/IPS and logs of other systems
  - common data fields include: date and time, type of event, action performed
  - specific data fields in network-based IDS/IPS: performing packet capture, in host-based IDS/IPS: record user IDs
- **Detection**: types and accuracy of detection depends on the detection method
  - some common criteria used by various technologies or methods
    - *Threshold*: a value that sets the limit between normal and abnormal behaviour
    - *Blacklists* and *Whitelists*: a list of entities such as hosts, TCP or UDP port numbers, applications, usernames etc. associated with malicious activities or known to be benign respectively
    - *Alert Settings*: allow administrators to customise alert types for instance set an alert to on or off, set a priority or security level, specify what information to be recorded etc.
    - *Code/Rule Viewing or Editing*: allow administrators to view or edit (or add) detection code/rules
- **Prevention**: allow administrator to specify preventive actions
  - e.g. enable or disable prevention, reset a connection, drop packets, block source etc.

[13] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Network-based IDS/IPS[14]

- has typical components of any IDS/IPS
- sensors monitor and analyse network activity in one or more segments
  - network interface is put in *promiscuous mode* accepting all traffic it receives regardless of the intended destination
- a N-IDS/IPS appliance generally is comprised of specialised hardware and sensor software
  - optimised for sensor activity
    - specialised NIC for efficient packet capture
    - specialised processors or other hardware components for fast analysis
    - part of software may reside in firmware for better performance
  - custom hardened OS not intended to be accessed directly
- a software-only IDS/IPS can be installed onto hosts that meet certain criteria
  - may include a customised OS or may be installed onto a standard OS

[14] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Network-based IDS/IPS: Sensor Placement[15]

- **Inline**: network traffic passes through the IDS/IPS
  - in case of IPS enables the device to prevent and stop attacks for instance by dropping packets
  - generally placed behind firewalls to reduce the traffic inspected by IDS/IPS
    - firewall will drop some packets that need not be inspected by IDS/IPS
- **Passive**: monitors a copy of actual network traffic using various methods
  - *Spanning Port*: a capability in network switches that allow all traffic that passes through switch to be observed from a switch port
    - could be resource intensive
    - misconfiguration could lead to traffic not being monitored
  - *Network Tap*: a direct connection between sensor and physical network media such as a fibre optic cable
    - problems with the tap could result in network downtime or traffic not received/monitored
  - *IDS Load Balancer*: aggregates and directs network traffic to monitoring systems such as IDS sensors
    - could receive traffic from multiple spanning ports or taps
    - could send a copy to multiple sensors for high availability
    - could balance based on volume, IP addresses, protocols, or other characteristics
    - division of traffic between multiple IDS/IPS could potentially miss related events

[15] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Network-based IDS/IPS Detection Capability: Types of Events[16]

- Application layer reconnaissance and attacks
  - e.g. banner grabbing, buffer overflows, format string attacks, password guessing, malware transmission
- Transport layer reconnaissance and attacks
  - e.g. port scanning, unusual packet fragmentation, SYN floods
  - generally TCP and UDP protocols
- Network layer reconnaissance and attacks
  - e.g. spoofed IP addresses, illegal IP header values
  - generally IPv4, ICMP, and IGMP
- Unexpected application services
  - e.g. tunneled protocols, backdoors, hosts running unauthorised services
  - can be detected through
    - stateful protocol analysis: identify if the activity in a connection is consistent with expected application protocol
- Policy violations
  - e.g. use of inappropriate web sites, use of forbidden application protocols
    - anomaly detection methods: identify changes in network flows

[16] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Network-based IDS/IPS: Limitations[17]

- inability to inspect encrypted traffic
  - VPN connections, protocols secured by TLS and DTLS, and encrypted application layer protocols such as SSH
  - place IDS/IPS where decrypted communication can be observed e.g. behind VPN gateways
  - use host-based agents/sensors to observe the traffic on the end hosts
- may not be able to perform full analysis under high loads
  - passive IDS/IPS sensors may drop some packets leading to some incidents to go undetected
  - inline IDS/IPS sensors dropping packets could lead to network disruption
    - sensors may drop lower priority traffic to handle high loads
    - vendors may use specialised hardware to increase performance
- IDS/IPS sensors are susceptible to attacks
  - DDoS attacks can generate large volumes of traffic
  - anomalous activity such as fragmented packets could increase the work load
  - *blinding* technique can be used to generate a large number of lower priority alerts
    - the high volume of alerts will either cause IDS/IPS to crash
    - or the actual attack is not noticed within the large number of alerts (hide the actual attack)

[17] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Network-based IPS: Prevention Capabilities[18]

- Passive only
  - ending current TCP session: IPS sends a TCP reset packet to both ends of a communication
    - is not effective against UDP traffic
    - reset message may not arrive in time to prevent an exploitation (delay due to processing time in IPS)
- Inline only
  - performing inline firewalling
    - drop packets detected as suspicious or as an attack
  - throttling bandwidth usage
    - for instance a traffic identified as inappropriate usage, DoS attack, malware propagation then limit the network bandwidth
  - alter malicious content
    - sanitise a packet payload (malicious content removed or replaced)
- Both Passive and Inline
  - reconfigure other network security devices
    - sending commands to firewalls, routers, and switches to change the configuration
    - e.g. block traffic from a particular source, placing infected hosts in quarantine VLAN etc.
  - run a third party program or script
    - an administrator can write a script that will be run when certain alerts are triggered (highly customisable)

[18] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Wireless IDS/IPS[19]

- generally has the common components of IDS/IPS
  - console, database (optional), management server, sensor
  - components are typically connected to each other through wired network
- differs with Network-based IDS/IPS in sensor monitoring
  - sensors perform the same basic role as Network-based IDS/IPS sensors however only monitor wireless traffic
  - sensors may be dedicated or bundled with Access Points
  - sensors may be deployed in fixed locations or may be mobile
    - mobile sensors may be standalone devices
- two frequency bands are monitored: 2.4 Ghz and 5 Ghz
  - a sensor may not be able to monitor all traffic on a frequency band simultaneously
  - sensors frequently changing channels to monitor other channel activities
    - this referred to as *channel scanning*
  - sensors may be customised with multiple antennas and higher radio power to monitor multiple channels

[19] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Wireless IDS/IPS: Sensor Locations[20]

- fundamentally different from choosing other types of IDS/IPS sensor locations
- sensors are deployed to
  - monitor the RF range of organisation WLAN for both APs and STAs
  - monitor physical regions of the facilities to detect wireless activity
    - for instance in locations where there should not be any wireless activity
    - to identify rogue APs and ad hoc WLAN
    - to monitor channel use
- other considerations for sensor locations
  - physical security of the sensor to prevent for instance tampering
    - closed location (wiring closet) or use of anti-tamper features
    - visible by security cameras
  - sensor range
    - can be affected by surrounding walls, doors etc.
    - can have overlap to cover the region
  - cost
    - a cost/threat analysis can identify how many sensors and where to deploy

[20] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Wireless IDS/IPS: Security Capabilities[21]

- information gathering
  - identify WLAN devices
    - create and maintain an inventory of observed WLAN devices e.g. APs, STAs
    - usually includes the SSID, MAC address which also identifies the vendor of Wireless NIC
    - may have capability to fingerprint the vendor (verify the vendor)
  - identify WLANs
    - keep track of observed WLANs: tag authorised WLANs, benign neighbouring WLAN, rogue WLAN etc.
- Logging
  - log information such as date and time, source MAC address, channel number, event type, sensor ID that observed the event etc.
- Detection
  - unauthorised WLANs and WLAN devices such as rogue APs, unauthorised STAs, unauthorised WLANs
  - attacks against wireless network
    - wireless network scanners, logical DoS attacks such as flooding, physical DoS attacks such as jamming the RF signal
  - misconfiguration of WLAN components
    - APs and STAs not using proper security controls e.g. WEP is enabled or used
  - policy violation at WLAN protocol level
  - unusual usage patterns
    - may use anomaly-based method
    - failed attempts to join the WLAN (e.g. in a short period of time)

Wireless IDS/IPS: Limitations[22]

- inability to detect certain wireless protocol attacks
  - attacker can passively monitor wireless traffic (not detectable)
  - attacker can perform offline processing on captured traffic to recover keys for weak algorithms (if used e.g. WEP)
    - recovered key can be used to capture and recover more traffic (still not detectable)
    - join the network and authenticate with recovered key
- susceptible to evasion techniques
  - attacker may identify the wireless IDS/IPS in use and use techniques to evade the product's channel scanning
    - for instance perform an attack in a short period of time in a channel not monitored by wireless IDS/IPS
- susceptible to attacks
  - logical and physical DoS attack on the sensor itself

[22] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Wireless IPS: Prevention Capabilities[23]

- **Wireless**
  - may be able to terminate a connection
    - between an authorised AP and a rogue or misconfigured STA
    - between an authorised STA and a rogue or misconfigured AP
    - generally is done by sending disassociate messages to endpoints
- **Wired**
  - may be able to instruct a switch to block the activity of an AP or a STA
  - this only applies to wired activity of an AP or STA
- typically allow administrators to configure prevention capabilities and actions
- may have a simulation or learning mode that suppresses prevention however indicates when a preventive action will be taken
  - allows administrators to tune the device

[23] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Host-based IDS/IPS[24]

- detection software (agent) is installed on the hosts of interest
- an agent monitors activity on a single host
  - in IPS mode also prevents identified attacks
- an agent is typically designed to protect
  - server: the OS as well as common applications
  - client host: the OS and common user applications of a desktop or laptop
  - application service: a specific application service for instance web or database server program
- may have the common components of IDS/IPS solution
  - console, database server, management server, agent(s) installed on one or more hosts
- since agents are deployed on hosts network communication is through standard network
  - communication between agent and other components may be encrypted

[24] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Host-based IDS/IPS: Host Architecture[25]

- some agents modify host internal architecture by adding an additional layer of code
  - additional layer is placed between existing layers of code to intercept all communications
    - user applications/processes to OS e.g. system calls
    - process to process
    - network
    - resource access such as file system activity
- other agents may monitor activity without modifying internal architecture
  - analyse the log entries and file modifications
  - reduces interference with host's normal operations
  - less effective at detecting threats or preventing attacks

installed on host vs. appliance:

- agent-based appliances can be used
  - deployed inline in front of a host
  - does not require OS support
- installing agents on hosts is preferable
  - have direct access to the host's characteristics
  - allows more comprehensive and accurate analysis, detection, and prevention
  - ~~OS must be supported by~~ agent

Host-based IDS/IPS: Security Capabilities[26]

- Logging
  - date and time, event type, event rating
  - host IP address and port information, application information, filenames and paths, user IDs
- Detection
  - code analysis to identify malicious activity
    - code behaviour analysis: e.g. first running it in a sandbox and analyse and compare to profiles
    - buffer overflow detection: e.g. attempts to access memory outside allocated, other characteristics of stack or heap overflow
    - system call monitoring: e.g. attempt to intercept keystrokes, loading drivers etc.
    - application and library lists: restrict process attempt in loading unauthorised shared libraries
- Network traffic analysis and filtering
- File system monitoring
  - file integrity checks
    - periodically generate hash of files and compare with a hash generated in a known-good state
  - file attribute checks
    - ownership and permission on important files e.g. private keys, shadow file, configuration files etc.
  - file access attempts
    - monitor attempts to access critical files such as system binaries
    - could prevent malware installation

[26] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Host-based IDS/IPS: Limitations[27]

- Alert generation delays
  - most detection technique generate events in real-time however some techniques only check periodically for events occurred
- Centralised reporting delays
  - most H-IDS/IPS are intended to forward alerts to management servers on a periodic basis
  - the periodic approach introduces delay in generating alerts
- Host resource usage
  - an agent running on a host consumes resources of the host
  - modification of internal architecture introduces additional delay
- Conflicts with existing security controls
  - agents may conflict with security controls if duplicate functionality is provided
    - e.g. personal firewall, VPN client
- Interruptions
  - updating agents may require host to be rebooted
  - problems in agent software could interrupt host normal activities

[27] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Host-based IPS: Prevention Capabilities[28]

- code analysis
  - prevent code from being executed e.g. malware or unauthorised applications
  - prevent network application to invoke shells
- network traffic analysis and filtering
  - stop incoming network traffic from being processed by the host
  - stop outgoing network traffic to exit host
  - identify and stop malicious file download or transfer
  - stop violations of acceptable use policy
- file system monitoring
  - prevent access to files
    - read, modification, replacement, deletion of files
  - prevent creation of files
  - can stop malware installation
- removable media restrictions
- host hardening
- process status monitoring

[28] NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Multiple IDS/IPS Integration and SIEM[29]

- multiple IDS/IPS products from multiple vendors can be deployed
  - some vendors make products for one particular IDS/IPS technology
  - different products may detect different attacks (not detected by the other)
  - generally operate independently (from each other)
- multiple IDS/IPS products from a single vendor may be integrated directly
  - could reduce administration time
    - familiarity with products interface
    - reduced integration time due to compatibility
- Security Information and Event Management (SIEM) software may indirectly integrate multiple IDS/IPS products
  - designed to import information from various security-related logs
  - correlate the events to detect suspicious activity or incidents
  - generally supports informations from IDS/IPS, firewalls, antivirus, OS logs, application server logs etc.
  - some SIEM products could initiate preventive actions
  - complements IDS/IPS: able to correlate events, wider range of sources of information
- limitations of SIEM
  - considerable delay between event time and when SIEM sees the log data
  - SIEM may not receive the complete content and only receive a summary
  - SIEM must support the IDS/IPS

References

The materials in this document are reproduced, at times without modification, from the following sources:

- NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)
- Chapter 9 of the *Network Security Essentials-Application Standards*, 5th Edition by *William Stallings*