
ESTD1845
QUEEN'S
UNIVERSITY
BELFAST

Intrusion Detection and Prevention Systems – Part 2

Dr. Sandra Scott-Hayward

CSC3064 Lecture 14

School of Electronics, Electrical Engineering and Computer Science

Session Overview

- IDS Evasion
- Intrusion Prevention Systems
- Unified Threat Management

References:
Jacobson, Douglas. *Introduction to network security*. CRC Press, 2008.
Schäfer, Günter, and Michael Rossberg. *Security in Fixed and Wireless Networks*. John Wiley & Sons, 2016.
Stallings, William. *Network security essentials: applications and standards*. Pearson Education India, 2007

QUEEN'S UNIVERSITY BELFAST

IDS Evasion

- Anomaly detection:
  - Attacker may act slowly
  - May generate high amount of “legitimate traffic” to cover attack
  - …

- Signature-based IDS:
  - Attackers may try to construct attacks such that they are not detected
  - Works extremely well when the attacker has access to the rule set
  - Encoding – Application layer protocols accept different expressions meaning the same thing e.g. Example: ‘a’, ‘%61’ and ‘%u0061’ all express the same letter. An IDS must be aware of all of the possible encodings that its end hosts accept
  - Encryption – Content cannot be read unless the IDS has a copy of the private key

General problems of IDS

Audit Data:

- Amount of log data:
  Auditing often generates a rather high data volume
  ⇒ Significant storage capacities are required
  ⇒ Processing of audit data should be automated as much as possible
- Location of audit data storage:
  Alternatives: on specific “log server”, or the system to be supervised
  ⇒ If stored on log server, data must be transferred to this server
  ⇒ If stored on the system to be supervised, the log uses significant amounts of resources of the system
- Protection of audit data:
  If a system becomes compromised, audit data stored on it might also be compromised
- Expressiveness of audit data:
  Which information is relevant?
  Audits often contain a rather low percentage of useful information

QUEEN'S UNIVERSITY BELFAST

General problems of IDS

Privacy (→ "Data Protection"):

- User-identifying data elements are logged, e.g.:
  - *Directly identifying elements:* user ids
  - *Indirectly / partly identifying elements:* names of directories and subdirectories (home directory), file names, program names
  - *Minimally identifying elements:* host type + time + action, access rights + time + action
- IDS audits may violate the privacy of users:
  - Violation of the user's right to determine for themselves, which data is collected regarding them
  - Collected information might be abused if not secured properly
  - Recording of events puts a psychological burden on users (→ "big brother is watching you")
- Potential solution:
  - *Pseudonymous audit:* log activities with user pseudonyms and ensure that they can only be mapped to user ids upon incident detection

QUEEN'S UNIVERSITY BELFAST

General problems of IDS

- *Limited efficiency of analysis:*
  - Most IDS follow a centralist approach for analysis: so-called *agents* collect audit data and one central *evaluation unit* analyzes this data
    - $\Rightarrow$ No (partial) evaluation in agents
    - $\Rightarrow$ Performance bottleneck
  - Insufficient efficiency, especially concerning attack variants and attacks with parallel actions
- *High number of false positives:*
  - In practice, many IDS report too many false alarms (some publications report up to 10.000 per month)
  - Potential countermeasure: alarm correlation ($\rightarrow$ hierarchical approach)
- Further problems / open issues:
  - Self protection (including strategies to cope with high load)
  - High maintenance overhead
  - Cooperation between multiple IDS

QUEEN'S UNIVERSITY BELFAST

Intrusion Prevention Systems - Motivation

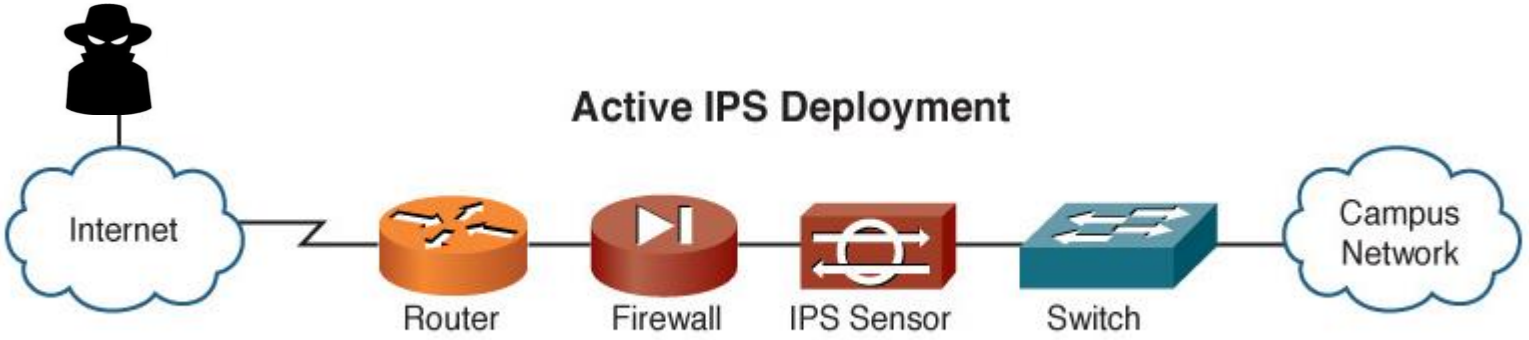
- Automatic event generation insufficient
  - Automatic exploitation is extremely fast → human intervention would be too late
  - Too many attacks on current systems → must be handled automatically for reasons of efficiency

- Led to the development of Intrusion Prevention Systems (IPS)

- Differentiation between IDS and IPS no longer meaningful as nearly all modern IDS are also IPS

Intrusion Prevention Systems - Approaches

- Inline operation and suppression
  - All traffic goes through the IPS
  - Any flow (and possibly similar flows) generating an attack event will be suppressed
  - Pros:
    - Efficient
    - No race conditions (i.e. traffic won't reach target before being processed)
  - Cons:
    - Possible bottleneck and single point of failure
    - May be difficult to set up



QUEEN'S UNIVERSITY BELFAST

Intrusion Prevention Systems - Approaches

- Firewall reconfiguration
  - IPS reconfigures an existing firewall to suppress suspicious flows
  - Pros:
    - Relatively easy to set up
    - No single points of failure
  - Cons:
    - Race conditions (what if the attack already reached the target, especially if the IPS is under load?)

Intrusion Prevention Systems - Approaches

- Sending TCP-RST packets
  - IPS resets TCP flows by resetting the connection
  - Pros:
    - Extremely easy to setup
    - No single point of failure
  - Cons:
    - Race conditions
    - Works only for TCP

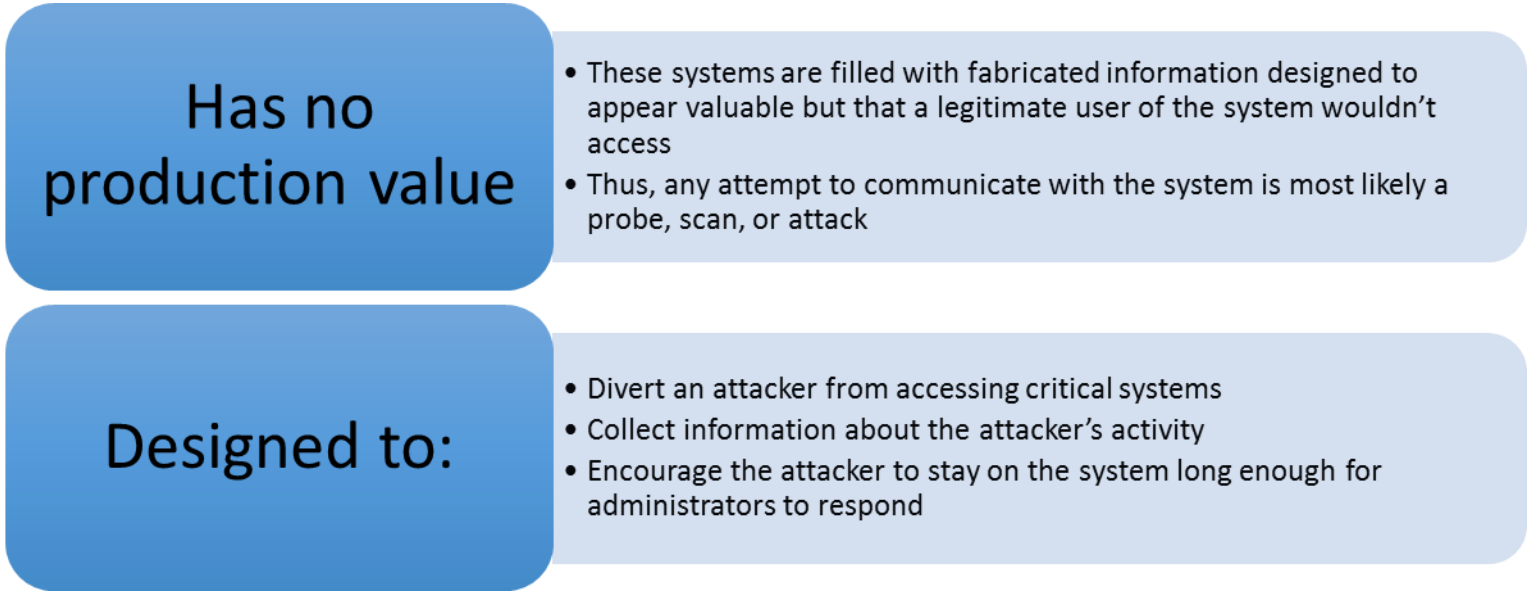
Intrusion Prevention Systems - Approaches

- Deflection
  - Reconfiguration of firewall and/or routers
  - Attacker is transparently redirected to honey pots to slow down their attack
  - Pro:
    - May cause a significant slow down
  - Cons:
    - Difficult to setup (if done well)
    - Race conditions …

QUEEN'S UNIVERSITY BELFAST

Honeypots

- Decoy systems that are designed to lure a potential attacker away from critical systems

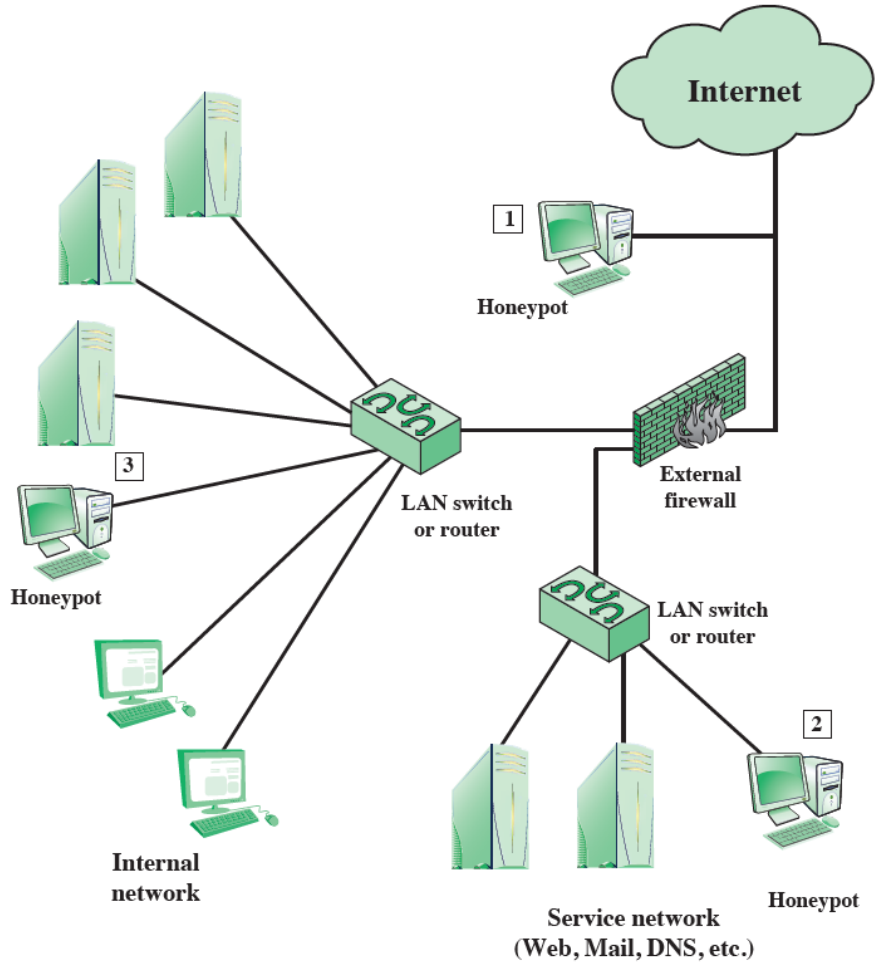


- Because any attack against the honeypot is made to seem successful, administrators have time to mobilize and log and track the attacker without ever exposing production systems
- Also build entire honeypot networks (honeynets) that emulate an enterprise, with actual or simulated traffic and data

QUEEN'S UNIVERSITY BELFAST

Example Honeypot Deployment

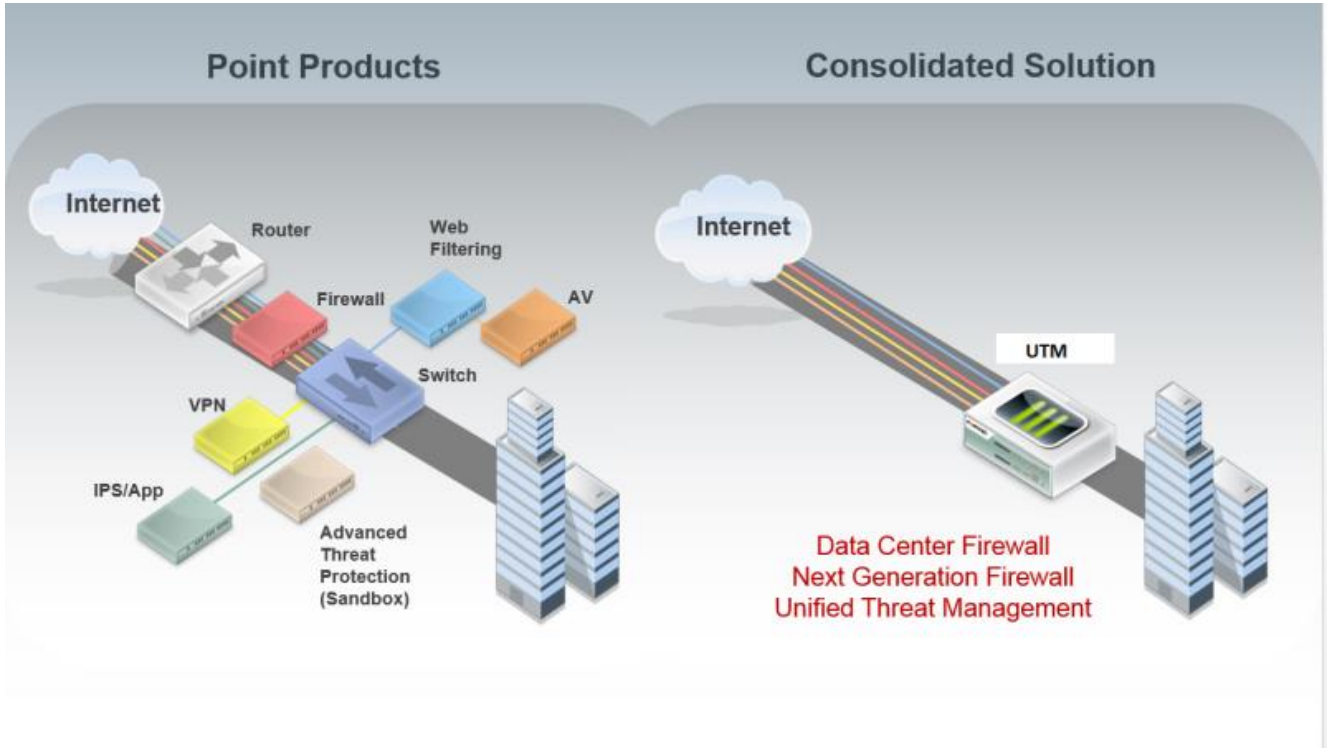
- Location 1: Outside external firewall to track connection attempts to unused IP addresses
- Location 2: Within the DMZ
- Location 3: Fully internal

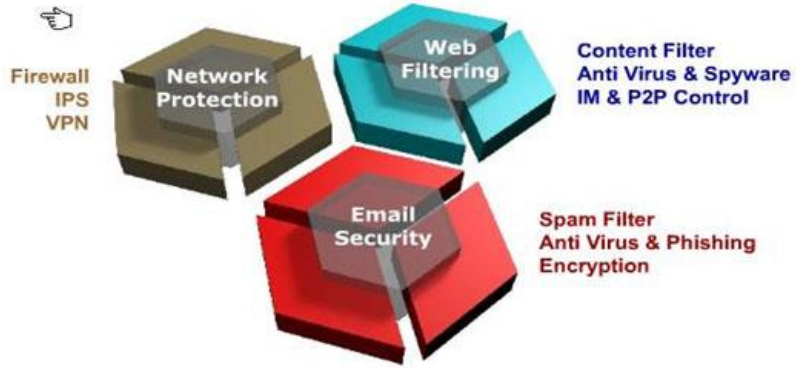


QUEEN'S UNIVERSITY BELFAST

IDPS Today – Unified Threat Management

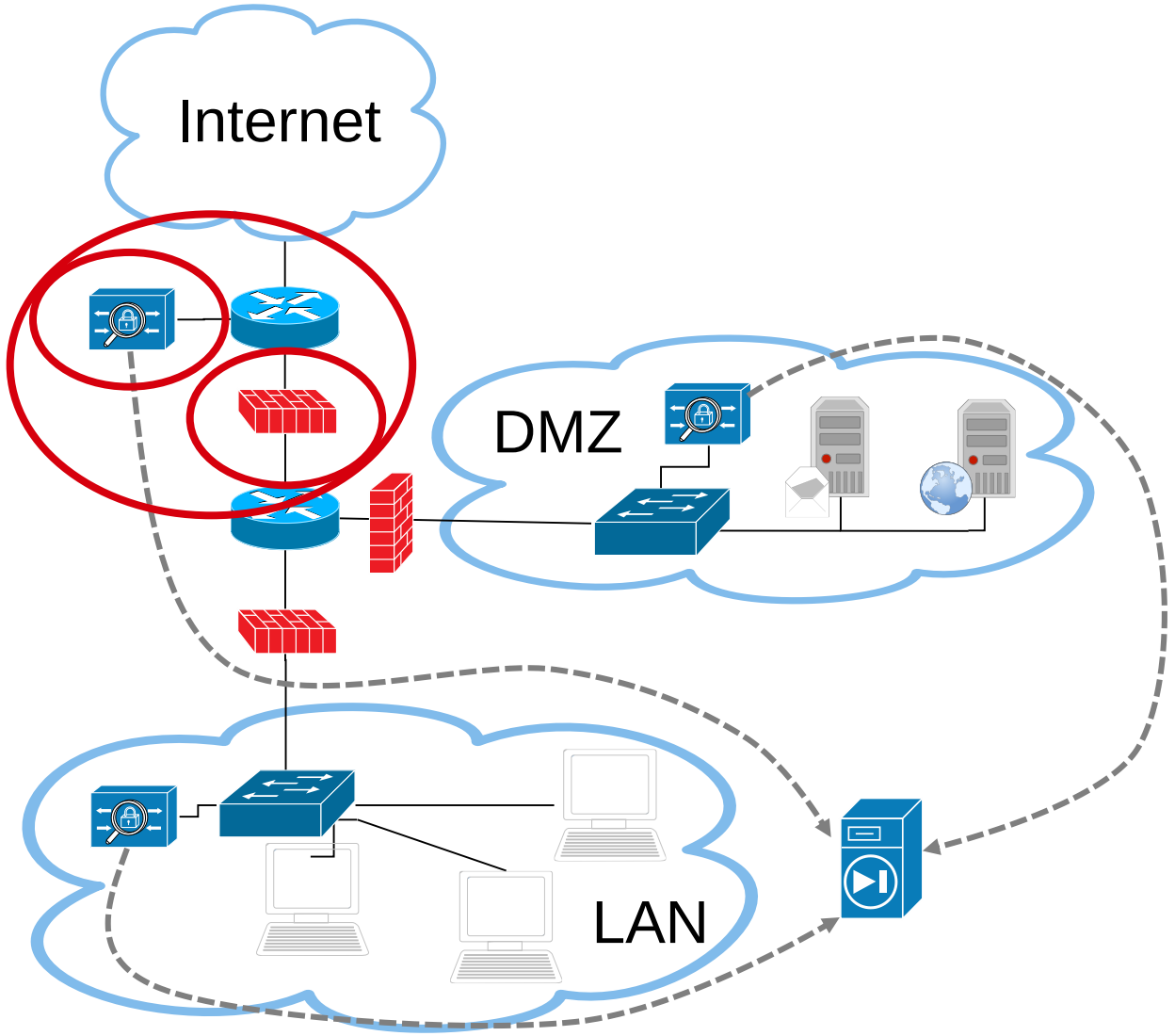
- Unified Threat Management
  - Essentially consolidation of stateful inspection firewalls, antivirus, and IPS into a single appliance, …





QUEEN'S UNIVERSITY BELFAST

UTM



QUEEN'S UNIVERSITY BELFAST

Summary

- IDS Evasion
- Problems of IDS
- Intrusion Prevention System Approaches
- Unified Threat Management

QUEEN'S UNIVERSITY BELFAST

Questions?

Next Session: Network Security Administration

Tuesday, 05 March 2019

QUEEN'S UNIVERSITY BELFAST