Generating adaptive security policies and automated configuration scenarios in intrusion management systems

Dimitrios Patsos, Sarandis Mitropoulos, Christos Douligeris
Department of Informatics, University of Piraeus,
80, Karaoli and Dimitriou Street, 185 40 Piraeus, Greece.
{dpat, sarandis, cdoulig}@ unipi.gr

11th Panhellenic Conference on Informatics (PCI 2007) at Patras, Greece, 18-20th May 2007.
This work has been partially supported by GSRT under a PENED grant and by the IST FET Coordination Action ACCA 6475)

Agenda

- Introduction
- Related Work
- Intrusion Management Systems
  - Construction of attack paths
  - Construction of counter-attack paths
  - Attack and counter attack path correlation and aggregation and construction of a real-time vulnerability, exploit and signature mapping
  - Generation of per attack path policies and enforcement of per attack path policies in Intrusion Detection and Prevention (IDP) Systems
  - Enhancements to Incident Response and Digital Forensics
  - Implementation Details and Workflow of Operation
- Case Study
- Limitations
- Conclusions

Introduction

- **Terminology** (simplified):
- Vulnerability: potential hazard that exist in nearly every piece of software
  - *No formal/standardized language to classify or model vulnerabilities*
- Exploit: the pragmatic information (e.g. piece of code) that utilizes one (or more) vulnerabilities to realize an actual attack
- Attack path: the series of consecutive vulnerability exploits that result in the realization of an attack
  - For simplicity and without loss of generality, we may positively assume that a different order may not result to the same attack path, if it even results to any.

Introduction (2)

- **Terminology** (formally):
- $a_i = \{(e_{j1}|v_{k1}), (e_{j2}|v_{k2}) , \ldots, (e_{jp}|v_{kq})\}$, where:
  - a_i *belongs to* A, the set of attack paths a_i
  - e_{jp} *belongs to* E, the set of exploits e_{jp}
  - v_{kq} *belongs to* V, the set of vulnerabilities v_{kq}
- More formally in [Krasser et. al. (2005)].

Introduction (3)

- A many to many relationship between vulnerabilities and exploits
- One exploit can utilize one or more vulnerabilities and vice versa.
- The significance of a vulnerability can be estimated only when the context is well understood.
- Information regarding exploits or the actual exploits are more difficult to be found
  - A large number of websites & mailing lists are known to host such information.
- The information related to exploits is also linked with specific vulnerabilities.

Introduction (4)

- An attack is usually addressed by one (or more) corresponding signatures , which are usually found in antivirus programs or IDP systems.
- A signature contains the exploit code itself or, more frequently, a synopsis/pattern of the exploit code.
- Most IDP systems are loaded with a large set of such signatures and compare every packet intercepted against every one of these signatures (or according to what the security policy indicates).
- Without properly defined policies, the effectiveness of IDP systems is rather low, especially in networks with heavy traffic.
- As new signatures are loaded- the IDP resources are being exhausted.

Introduction (5)

- A major issue in this context is the mapping of vulnerabilities to exploits and the mapping of exploits to signatures
  - Construction of attack paths and counter-attack paths
  - The attack path: linkage between vulnerabilities and exploits
  - Counter-attack path: the necessary signatures to address these exploits.
- Interesting configuration scenarios for IDP systems
- Security policies that adapt according to every specific attack path.

Introduction (6)

- Intrusion Management Systems (IMS) objectives:
  - reduce IDP mechanisms false positives
  - eliminate Vulnerability Assessment (VA) false negatives,
  - increase the policy effectiveness of IDP systems
  - apply adaptive security policies
  - exchange, correlate and validate security information
  - combine, complement, and leverage the effectiveness of a number of well known techniques.

The problem space

- Intrusion Detection and Prevention systems are configured to identify malicious activity in specific network segments, by using “sensors” that monitor the traffic in a “collision domain”.
- Signatures that match the potential threats of the systems within this “collision domain” are activated so that IDP systems identify malicious traffic originating or destined to machines belonging to this “collision domain”.
- Policies are enforced according to the security needs of the machines in operating system and application software level.

The problem space (2)

- ***Example 1:***
  - A firewall divides a network into n different Security Zones
  - n network sensors are needed to entirely monitor these zones
  - Signatures configured are solely addressing the vulnerabilities of the machines belonging to this domain only
  - low policy effectiveness: the relevancy between the total vulnerabilities addressed in a collision domain is only a fraction of the total signatures used

- ***Example 2:***
  - two different systems -in terms of application and operating system- reside between a Demilitarized Zone (DMZ),
  - the IDP policy for this DMZ must use the entire set of signatures that match the combination of both systems.
  - the overall policy effectiveness weakens considerably as the number of the different systems monitored increases

The problem space (3)

	Operating System 1	**Operating System 2**	**Application 1**	**Application 2**
Signatures for Operating System 1	RELATIVE	NOT RELATIVE	N/A	N/A
Signatures for Operating System 2	NOT RELATIVE	RELATIVE	N/A	N/A
Signatures for Application 1	N/A	N/A	RELATIVE	NOT RELATIVE
Signatures for Application 2	N/A	N/A	NOT RELATIVE	RELATIVE
Policy Effectiveness	**50%**	**50%**	**50%**	**50%**

Related Work

- [Templeton et. al (2000)]: a flexible model for computer attacks along with several proposed applications in VA and IDP.
- [Swiler et. al. (2001)] : an automated tool capable of generating and analyzing attack path information.
- [Sheyner et. al (2002)]: a tool that correlates attack graphs with the most exploitable components of the system configuration.
- [Ammann et. al (2002)]: provide a scalable representation of attack graphs, focusing on revealing end-to-end attack scenarios.
  - *The primary focus of these tools is the modelling of network and computer-based attacks, as well as the production of attack paths and/or graphs, not matching scenarios with IDP policies.*

Related Work (2)

- [Gula (2002)]: various configuration scenarios where vulnerability information could be correlated with IDP audit log information.
  - *does not include "filtering" mechanisms on the information used as input both in vulnerability assessment tools, as well as in Intrusion Detection Systems.*
- [Ning et. al. (2003)]: developed a number of techniques for the automatic learning of attack strategies from intrusion alerts.
  - *Effective correlation of IDP information with static VA information as input, but it does not model network security conditions and/or analyze the attack paths.*
- [Kumar et. al. (2005)] provide Topological Vulnerability Analysis (TVA), a technique heavily used in the framework of IMS.

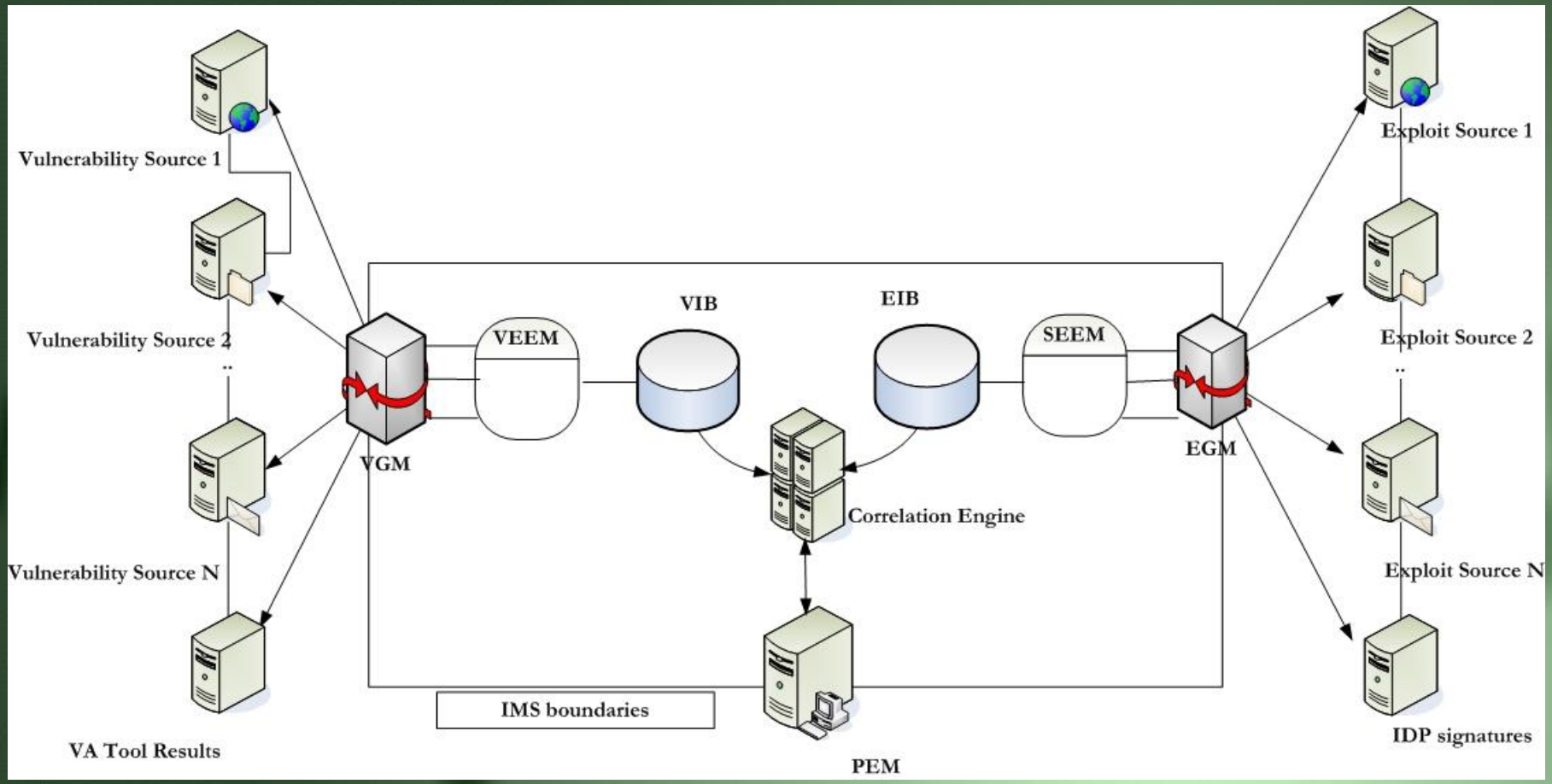
Intrusion Management Systems

- Automated VA tools cannot identify the security policies enforced
- The output of a VA can differ, based upon where –in the network topology- the scan is performed.
- Example:
  - No security mechanism is placed between the VA tool and an un-patched Web Server,
  - Properly configured firewall exists between the VA tool and an un-patched Web Server
  - The results will be entirely different but exactly the same vulnerabilities exist on this Web Server.
- The identification of a large a number of vulnerabilities in a network segment or a system does not indicate a high security exposure of this segment or system, since it is possible that the vulnerabilities unearthed cannot be exploited with a predefined order or a combination that leads to an actual attack.
- IDP systems have significantly advanced in last years so that they are able to be deployed in a variety of topological elements or network devices.
- Apart from dedicated devices, they can be integrated in edge routers, in application firewalls, and in endpoint security solutions. It must be also noted that IDP systems aim at the prevention or detection of attacks (not only vulnerabilities).

Intrusion Management Systems (2)

- An IMS is a security management system, which has the following capabilities:
  - Construction of attack paths, using VA information as input (by producing a real-time vulnerability-exploit mapping).
  - Construction of counter-attack paths, using IDP information as input (by a real-time exploit-signature mapping).
  - Attack path and counter attack path correlation, and aggregation as well as construction of a real-time vulnerability, exploit and signature mapping.
  - Generation of per attack path policies.
  - Enforcement of per attack path policies to IDP by issuing appropriate policy commands.
  - Enhancements to Incident Response and Digital Forensics

Architecture



Construction of Attack-Paths

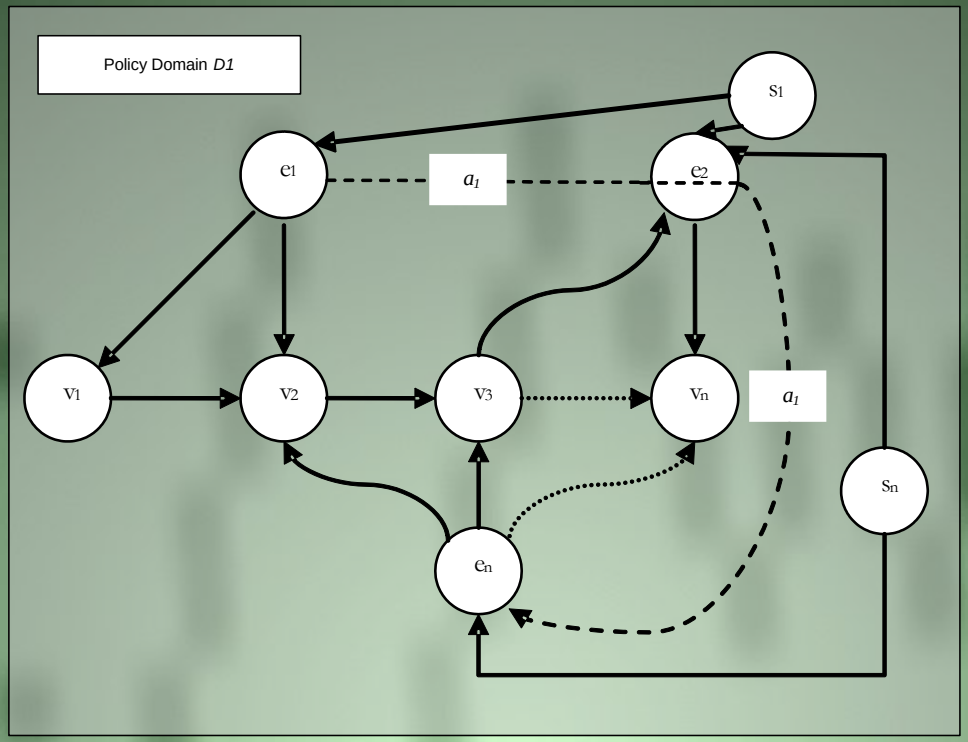
- The Vulnerability Gathering Module (VGM) uses a process to gather vulnerability information from various sources (e.g. the Web, mailing lists, VA tools, etc.).
- The Vulnerability Exploit Extraction Module (VEEM) uses a process to gather exploit information from various sources (e.g. security research sites, hacking sites, etc.).
- An XML program links vulnerabilities with exploits, producing a real-time vulnerability/exploit mapping.
- The Vulnerability Storage Module (VSM) uses a process to store all the above information in the Vulnerability Information Base (VIB).

Construction of counter-attack paths

- In order to construct a counter attack path, the IMS modules perform the following tasks:
- The Exploit Gathering Module (EGM) uses a process to gather attack information from various sources (e.g. the IDP database).
- The Signature Exploit Extraction Module (SEEM) uses a process to extract the exploit information found in these signatures.
- An XML program links signatures with exploits, producing a real-time signature/exploit mapping.
- The Vulnerability Storage Module (VSM) uses a process to store all the above information in the Exploit Information Base (EIB).

Correlation/aggregation and real-time mapping of v, e and s

- Several vulnerability/exploit and exploit/signature mappings are produced.
- These mappings are filtered and aggregated for redundant or not relative entries.
- IMS enforces a security policy p_i in the IDP systems that will use certain signatures (e.g. $s_1,\ldots,s_n$) to address the vulnerabilities and exploits of the attack path a_i.



Generation and enforcement of per attack path policies in IDP

- The Policy Enforcement Module (PEM):
  - analyzes an existing IDP policy,
  - Adapts these policies to the needs of the attack and counter attack paths identified.
  - Identifies and selects only the minimum set of signatures needed to counter a specific attack path.
  - Activates these signatures and reconfigures the IDP system.
- Uses the SISL language [Feiertag, 1999], or another standardized language capable of issuing appropriate policy commands to the IDP.
- The adaptive security policies can facilitate very flexible configuration scenarios in IDP systems
- Policies can be changed according to what the IMS indicates for a specific attack path.
- Extremely useful when an attack –not addressed by any policy- is in progress, since the IMS can provide “self-resisting” attributes to the IDP by continuously modifying a generic baseline policy to counter the attack in progress.

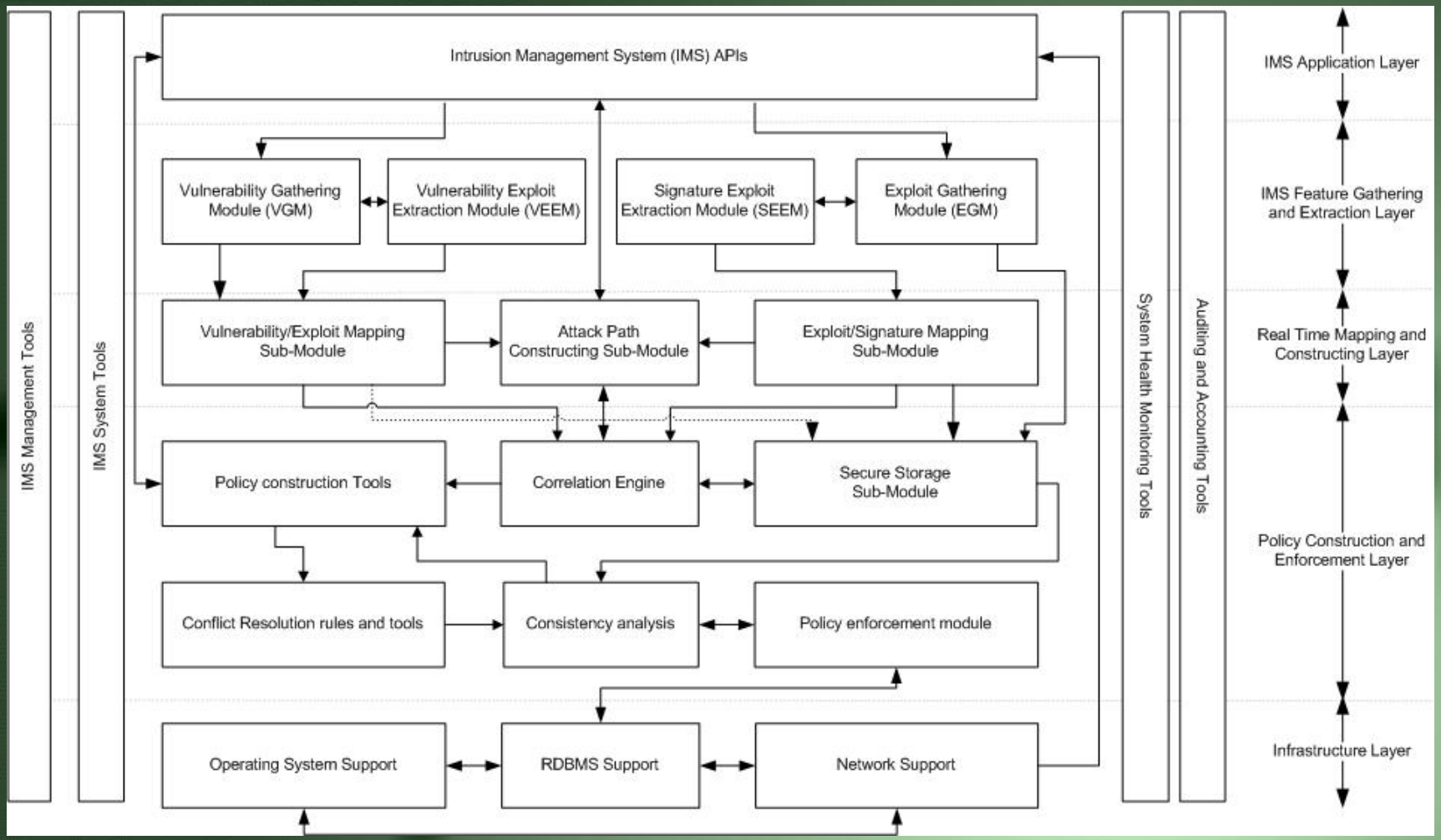
Enhancements to Incident Response and Digital Forensics

- Various formal methodologies on Incident Response
  - Manual or semi-automated procedures on identifying the incident's source, magnitude and severity so that decisions be taken.
- These decisions affect the members of nearly the entire scope of an organization, since a large set of company members have to take specific actions [Mitropoulos et. al. (2006)].
- A critical part of the Incident Response process is the proper and timely identification of a security incident.
- A large part of this procedure is carried out by high-end management systems (Security Information Management Systems (SIMs) that produce results based on correlating security information found in system, network, and application logs.

Enhancements to Incident Response and Digital Forensics (2)

- Intrusion Management Systems aim to eliminate false positive information provided by nearly all modern IDP technologies [Aberdeen (2003)], and provide more accurate information on an incident's occurrence.
- Moreover, they are capable of producing adaptive security policies and issue the corresponding configuration commands to the IDP systems
- The information provided by SIMs can be used from the IMS as well, in terms of policy adjustment.
- Furthermore, in case many cases an organization decides to pursue a Digital Forensics analysis, the IMS can provide the experts with the definition of the overall attack context (since it constructs the attack path)
  - Major importance when a forensics analysis is performed in "live" systems [Adelstein (2006)].

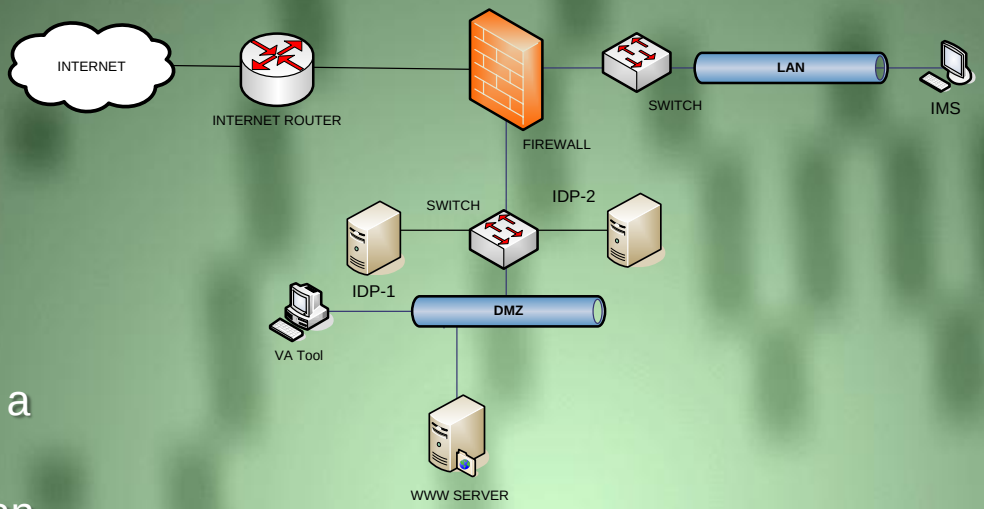
Implementation Details and Workflow of Operation (det.)



Case Study

- The Unchecked Buffer in the Index Server ISAPI Extension vulnerability, also known as “Code Red”
- Allows a remote attacker to gain full system level access to Microsoft Internet Information Services (IIS)
- The ISAPI filter of the .ida (Indexing Service) is originally interacting with the Web Server, mostly due to functionality requirements.
- The ISAPI filter (idq.dll) did not perform the necessary bounds checking on user inputs, and was therefore susceptible to a buffer overflow attack.
- Attackers that exploit this vulnerability can perform nearly any action on the compromised system, varying from copying or deleting files to manipulating the web content according to their desire.

- Lab Setup



Case Study (2)

- The commercial vulnerability scanner indicated the HTTP_Code_Red vulnerability (classified as High).
- This information was passed (semi automatically at this phase) to the Vulnerability Gathering Module (VGM) which was configured to get input from various Web Sites and mailing lists that de-scribe the vulnerability findings.
- The VGM reported the following vulnerability sources that were linked with the aforementioned vulnerability:
  - CVE: 2001-0500, 2001-0506
  - BUGTRAQ: 20010618, 20010817, 20011127
  - CERT: CA-2001-13
  - BID: 2880, 3190
  - Microsoft: MS01-033, MS01-044
  - CIAC: L-098, L-132

Case Study (3)

- This (HTTP_Code_Red vulnerability) is automatically passed to the Vulnerability Exploit Extraction Module (VEEM) where the exploit code was extracted from the vulnerability assessment tool internal database.
- The actual exploit code extracted for the aforementioned vulnerability was:
  - GET/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
    NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
    NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
    NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
    NNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858
    %ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u
- The Vulnerability/Exploit Mapping Sub-module has a very limited field of operation, since the relationship between the present vulnerability and the exploit code is 1-1. The above information was stored in the Vulnerability Information Base (VIB).

Case Study (4)

- After the Exploit Gathering Module (EGM) was provided the exploit code described above, the Signature Exploit Extraction Module (SEEM) returned the HTTP_IIS_Index_Server_Overflow and the HTTP_IIS_ ISAPI_EXTENSION signatures from the systems depicted as IDP-1 and IDP-2, respectively.

- The HTTP_IIS_Index_Server_Overflow alarm of the system IDP-1 required that this signature should be activated in the DMZ, in order to protect the vulnerable Web Server in the network layer. Accordingly, the same action is required to the system IDP-2, since the HTTP_IIS_ ISAPI_EXTENSION signature was the one corresponding to the HTTP_Code_Red vulnerability, as defined by the VA tool.

- At this stage, the development of appropriate interfaces between the commercial IDP products and our IMS prototype is not feasible, due to the limitations set by the vendors.

- Next immediate steps to develop appropriate policy enforcement tools between the IMS prototype and the open-source Snort IDS, developing the appropriate policy management agents (PMA) on the Snort Platform.

Limitations

- Results of IMS are still based on the capabilities of VA tools and IDP systems.
  - An IMS cannot assist in cases when the VA tool misses the detection of a vulnerability or an IDP system identifies normal traffic as an attack.
- Current Main Development barriers
  - No standardized predefined format for both vulnerability and attack description [Gordon (2003)]
  - Critical for understanding vulnerability information found in proprietary or commercial tools.
  - No a predefined standard for IDP signatures.
  - The development of IMS can be only based upon reference systems like the open-source Snort Intrusion Detection System (www.snort.org) and the Nessus vulnerability scanner (www.nessus.org).
- Information exchanged between VA tools and IDP systems in a way that one system provides feedback to the other is not yet effectively addressed.
  - Only commercial products of the same vendor can provide this functionality.

Conclusions and Future Work

- Vulnerability Assessment (VA) tools and Intrusion Detection and Prevention (IDP) systems cannot operate in isolation.
- Intrusion Management Systems (IMS) exchange, correlate and validate valuable security information
- IMS combine, complement and leverage the effectiveness of VA and IDP
- IMS can be used for the automatic generation of adaptive security policies and the enforcement of these policies to IDP systems and VA tools, via well-defined configuration scenarios.
- We proposed an implementation approach for IMS, discussed the benefits of our approach to post-incident procedures, like Incident Response and Digital Forensics, and highlighted open issues and current IMS development limitations.
- Next immediate research steps are to finalize the development of an entire IMS, based upon reference legacy systems (VA and IDP).
- A proposed schema for the vulnerability and intrusion information standardization is also in progress to assist in bypassing this major obstacle and facilitate future growth in IMS development.

Questions !?

Thank you!

Dimitrios G. Patsos,
Ph.D. Candidate,M.Sc.,CME,CCDA,CCSE
Department of Informatics
University of Piraeus
dpat@unipi.gr