Security Architecture based on Defense in Depth for Cloud Computing Environment

Theodoros Mavroeidakos[1] , Angelos Michalas[2] and Dimitrios D. Vergados[3]

[1]University of Piraeus, Greece
Email: mavroeidakos.theodoros@gmail.com

[2]Technological Educational Institute of Western Macedonia, Kastoria, Greece
Email: amichalas@kastoria.teiwm.gr

[3]University of Piraeus, Greece
Email: vergados@unipi.gr

April 9, 2016

Outline

1. Introduction
2. Background
3. Cloud Computing Environment
4. Proposed Security Architecture
5. Configuration of Security Systems
6. Security Architecture Evaluation
7. Conclusions

Introduction

- The security of a cloud computing environment is affected by its deployment and service model.
- The security threats that emerge are highly associated with abstraction level of the end service.
- The presented architecture is created by four principles: the deterrence, the detection, the delay and the denial.
- This architecture consists of cooperative defense zones hosting the systems of CC environment.
- Security legacy systems as well as CC defense mechanisms are incorporated.
- The main objective of this architecture is to secure the operations of CC environment by collaboration between security entities without affecting the environment's capabilities.

Background

- A security model for CC is proposed in [2] which incorporates OTP authentication, hashing algorithms, an encryption algorithm and a data recovery mechanism
- In [3], four CC security models are summarized:
  - The Multiple-Tenancy Model of National Institute of Standards and Technology.
  - The Risk Accumulation Model of Cloud Security Alliance.
  - The Cube Model of Jerico Forum.
  - The Security and Compliance Mapping Model.
- As presented in [4], the IDS SNORT can be deployed within the software defined networks of the OpenStack.
- In [5], the Intrusion Responsive Autonomic System controls the management of logs and analyze them in an isolated big data environment so as to detect intrusions .

Cloud Computing Environment

The proposed CC Security Architecture is mapped in the network topology of the CC environment of OpenStack.This environment consists of five interconnected computing entities:

- Controller Nodes
- Compute Nodes
- Network Nodes
- Block Nodes
- Object Nodes
- The nodes are interconnected through the Management network. VLANs and a Tunneling network are orchestrated for the end service delivery.

Cloud Computing Environment

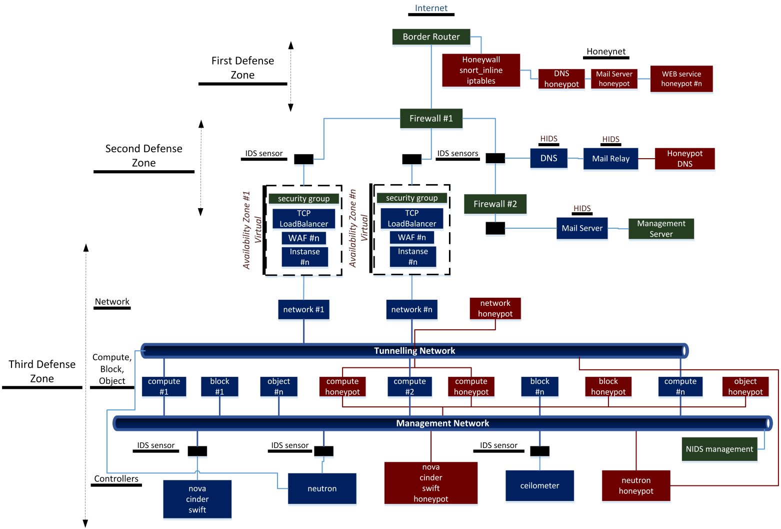


Figure: Security Architecture

Proposed Security Architecture

The proposed CC Security Architecture is defined by a set of distinct functional layers namely:

- the perimeter defense
- the deceptive
- the detection
- the cryptography

Prior to the adaptation of the security mechanisms of each layer, a sequence of policies should be defined. The policies will maintain the balance between:

- productivity
- functionality
- security

Proposed Security Architecture

The following collaboration diagram presents the priority among the layers of the architecture.

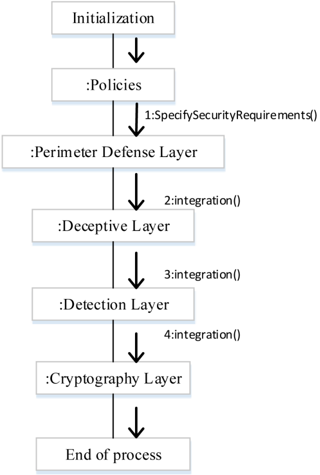


Figure: Collaboration Diagram

Proposed Security Architecture

Perimeter Defense Layer

- This layer divides the CC environment into defense zones so as to protect the classified data with suitable security mechanisms.
- First Defense Zone
  - It extends between the border router and the first stateful inspection firewall.
  - The main security mechanism of the deceptive layer,honeynet, will be emplaced in this zone.
- Second Defense Zone
  - It extends among the first stateful inspection firewall, the security groups of instances and the second stateful inspection firewall.
  - Security groups act as virtual firewalls and control the bidirectional network traffic on the Autoscaling Groups.
- Third Defense Zone
  - It extends behind the second stateful inspection firewall and the security groups.

Proposed Security Architecture

Deceptive Layer

- In this layer reside the deceptive systems which operate in every defense zone.
- A honeynet is emplaced in the first defense zone so as to lure the attackers and detain them enough to detect them.
- Honeynet consists of:
  - the honeywall
  - high interaction honeypots
- A number of high interaction honeypots are set up in key points of the second defense zone.
- A deceptive network of high interaction honeypots is created in the third defense zone, emulating the operations of the legitimate nodes.
- Under normal conditions, any ingress or egress traffic captured in honeypots should be considered malicious.

Proposed Security Architecture

Detection Layer

- In this layer, the intrusion detection system (IDS) resides which analyses the network traffic with a predefined ruleset identifying attempts of attacks.
- The IDS adopted in the security architecture is the open source tool, SNORT.
- In the proposed security architecture, remote sensors are placed in every defense zone in specific points capturing the bidirectional network traffic so as to:
  - increase the accuracy of detection and
  - decrease the false positives.
- The management server which controls the logs and alerts, is placed in a secure location behind the second stateful inspection firewall.
- The efficiency of intrusion detection is highly connected with the predefined ruleset of the remote sensors.

Proposed Security Architecture

Cryptography Layer

- Cryptographic methodologies are incorporated into the CC environment such as elliptic curve cryptography.
- The procedures and function of cryptography should not contradict with the operations of the other layers.
- In case the encrypted data harden the operation of IDS, then their emplacement should be avoided.
- The detection of an intrusion is more important than the concealment of data.
- The TLS protocol and its suite of cryptographic algorithms should be used to achieve end-to-end encryption between the clients and the web servers on the OpenStack instances.

Proposed Security Architecture

Functional Layers	**Security Systems**
Perimeter Defense	OSSEC, ModSecurity, Openstack Security Groups
Deceptive	Second Generation Honeynet, Honeyd
Detection	Snort
Cryptography	Elliptic Curve Cryptography

Table: Potential Security Systems in Each Layer

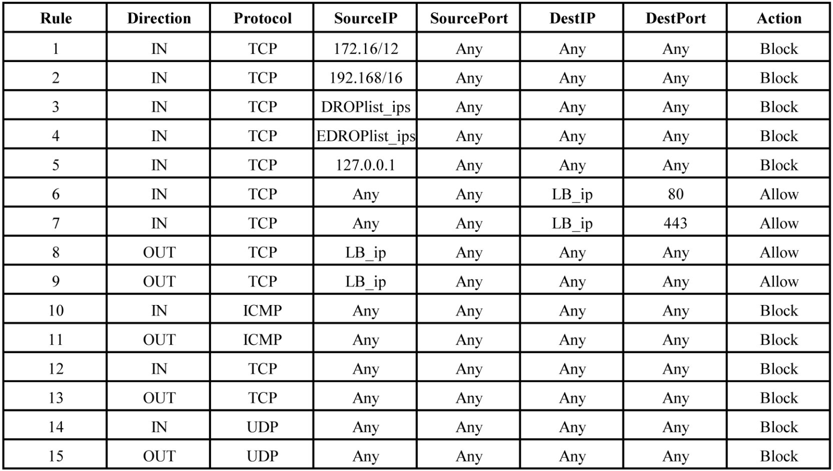
Configuration of Security Systems

- Configuration Choices for border router:
  - The ICMP traffic should be blocked entirely to avoid attacks against the TCP protocol such as:
    - blind connection-reset
    - blind throughput-reduction
    - blind performance-degrading
    - UDP port scans
  - The ip source routing feature should be disabled.
  - The first fragment of a packet should contain a default quantity of information about the transport header.

Configuration of Security Systems

- Configuration Choices for the first stateful inspection firewall:
  - The security policy of the first firewall should contain analytical customizations about:
    - embryonic connections
    - performing session lookups
    - checking TCP sequence numbers
    - verification of IP checksum
  - The first firewall should behave as a redundant system in case of border router failure.
  - Firewall rules should be configured allowing the communication of IDS sensors with the management server.
  - Firewall rules should block network traffic from netblocks of ip addresses defined in DROP and EDROP lists.
  - In order to avoid degradation of the end service the firewall rules should be defined in a specified manner:
    - firstly the deniability rules
    - secondly the allowance rules
    - finally the general decisions rules
  - The first firewall should support a great number of concurrent TCP connections to avoid negative effects on scalability of CC environment.

Configuration of Security Systems



Rule	Direction	Protocol	SourceIP	SourcePort	DestIP	DestPort	Action
1	IN	TCP	172.16/12	Any	Any	Any	Block
2	IN	TCP	192.168/16	Any	Any	Any	Block
3	IN	TCP	DROPlist_ips	Any	Any	Any	Block
4	IN	TCP	EDROPlist_ips	Any	Any	Any	Block
5	IN	TCP	127.0.0.1	Any	Any	Any	Block
6	IN	TCP	Any	Any	LB_ip	80	Allow
7	IN	TCP	Any	Any	LB_ip	443	Allow
8	OUT	TCP	LB_ip	Any	Any	Any	Allow
9	OUT	TCP	LB_ip	Any	Any	Any	Allow
10	IN	ICMP	Any	Any	Any	Any	Block
11	OUT	ICMP	Any	Any	Any	Any	Block
12	IN	TCP	Any	Any	Any	Any	Block
13	OUT	TCP	Any	Any	Any	Any	Block
14	IN	UDP	Any	Any	Any	Any	Block
15	OUT	UDP	Any	Any	Any	Any	Block

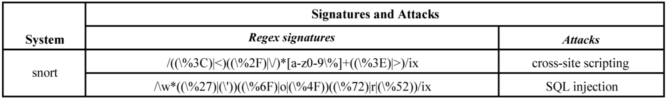
Figure: Indicative Firewall Rules

Configuration of Security Systems

- Configuration Choices for the second stateful inspection firewall:
  - The second firewall protects the Mail Server and the Management Server of the IDS.
  - The administration practise followed for the configuration of the second firewall is whitelisting due to the fact that the network traffic is finite.
  - The second firewall should be product of different vendor than the first so as to avoid exploitation of common vulnerabilities to overcome it.

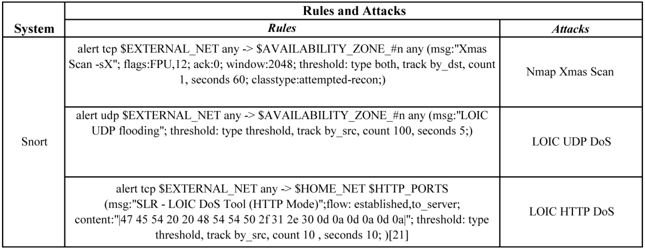
- Configuration Choices for the IDS sensors:
  - Continuous update of signatures on each ruleset in order to identify every new attack.
  - The sensors should follow dynamic detection technique in order to identify attacks in real time.
  - Perl compatible regular expressions should be used so as to create signatures for attacks.

Configuration of Security Systems



<table>
<tr><th rowspan="2">System</th><th colspan="2">Signatures and Attacks</th></tr>
<tr><th><em>Regex signatures</em></th><th><em>Attacks</em></th></tr>
<tr><td rowspan="2">snort</td><td>/((\%3C)|<)((\%2F)|\/)*[a-z0-9\%]+((\%3E)|>)/ix</td><td>cross-site scripting</td></tr>
<tr><td>/\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix</td><td>SQL injection</td></tr>
</table>

Figure: Indicative Snort REGEX Signatures



<table>
<tr><th rowspan="2">System</th><th colspan="2">Rules and Attacks</th></tr>
<tr><th><em>Rules</em></th><th><em>Attacks</em></th></tr>
<tr><td rowspan="3">Snort</td><td>alert tcp $EXTERNAL_NET any -> $AVAILABILITY_ZONE_#n any (msg:"Xmas Scan -sX"; flags:FPU,12; ack:0; window:2048; threshold: type both, track by_dst, count 1, seconds 60; classtype:attempted-recon;)</td><td>Nmap Xmas Scan</td></tr>
<tr><td>alert udp $EXTERNAL_NET any -> $AVAILABILITY_ZONE_#n any (msg:"LOIC UDP flooding"; threshold: type threshold, track by_src, count 100, seconds 5;)</td><td>LOIC UDP DoS</td></tr>
<tr><td>alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SLR - LOIC DoS Tool (HTTP Mode)";flow: established,to_server; content:"|47 45 54 20 20 48 54 54 50 2f 31 2e 30 0d 0a 0d 0a 0d 0a|"; threshold: type threshold, track by_src, count 10 , seconds 10;)[21]</td><td>LOIC HTTP DoS</td></tr>
</table>

Figure: Indicative Snort Rules

Configuration of Security Systems

- Configuration Choices for the Web Application Firewalls:
  - WAFs are placed into the availability zones of the CC environment and consist scaling entities.
  - WAFs are configured using ModSecurity Core Rule Set following network based deployment.
  - The httpOnly flag should be set so as to mitigate the XSS attacks.
  - Content injection should be performed into http responses in order to achieve in browser inspection capabilities.
  - An ideal number of OpenStack instances should be assigned in each WAF to avoid adding extra overhead delay.

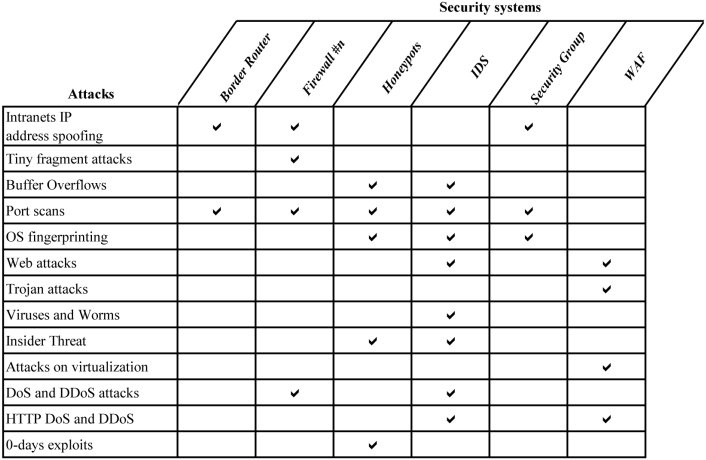
Security Architecture Evaluation

Theoretical Background

- DoS, DDoS and flood attacks are strictly connected to embryonic connections and ip spoofing and can be treated by the systems of the perimeter defense layer.
- WAFs provide HTTP protection against HTTP DoS attacks, XSS attacks and SQL-injection.
- WAFs offer Trojan protection, Webshell detection and Anti-Virus scanning of file attachments.
- IDS protect the CC environment against:
  - buffer overflow attacks
  - stealth port scans
  - OS fingerprinting
  - vulnerabilities scans
  - viruses and worms
- The honeynet has the ability to adentify new vectors of attacks, malicious behavior and 0-day exploits.

Security Architecture Evaluation

The following figure presents attacks that target CC environments and the security systems of the proposed security architecture which mitigate them.



Attacks	Security systems					
	Border Router	Firewall #n	Honeypots	IDS	Security Group	WAF
Intranets IP address spoofing	✓	✓			✓	
Tiny fragment attacks		✓				
Buffer Overflows			✓	✓		
Port scans	✓	✓	✓	✓	✓	
OS fingerprinting			✓	✓	✓	
Web attacks				✓		✓
Trojan attacks						✓
Viruses and Worms				✓		
Insider Threat			✓	✓		
Attacks on virtualization						✓
DoS and DDoS attacks		✓		✓		
HTTP DoS and DDoS				✓		✓
0-days exploits			✓			

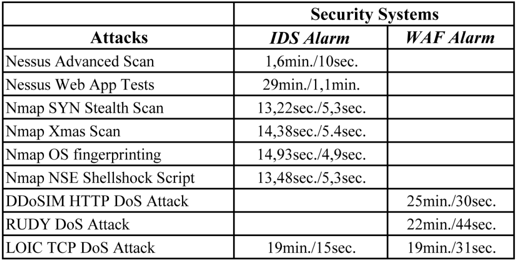
Figure: Attacks and Security Systems

Security Architecture Evaluation

- The evaluation of the CC environment performed by automated tools namely:
    - DDoSim
    - R-U-Dead-Yet (RUDY)
    - LOIC
    - Nmap
    - Nessus
    - Tcpdump
- Nmap and Nessus stealth port scans identified by the IDS sensors.
- A DoS attack using LOIC on the ip address of LoadBalancer identified by the IDS.
- The WAF identified an HTTP DoS attack with valid requests performed by DDoSim on the end-service.
- The WAF identified an HTTP DoS attack performed by RUDY on the end-service

Security Architecture Evaluation

- The average duration of attacks or scans as well as the time required by the security systems to identify the threats is presented in the following table.
- The response time of the security systems is highly associated with the magnitude of the ruleset and the network throughput.



	Security Systems	
Attacks	***IDS Alarm***	***WAF Alarm***
Nessus Advanced Scan	1,6min./10sec.	
Nessus Web App Tests	29min./1,1min.	
Nmap SYN Stealth Scan	13,22sec./5,3sec.	
Nmap Xmas Scan	14,38sec./5.4sec.	
Nmap OS fingerprinting	14,93sec./4,9sec.	
Nmap NSE Shellshock Script	13,48sec./5,3sec.	
DDoSIM HTTP DoS Attack		25min./30sec.
RUDY DoS Attack		22min./44sec.
LOIC TCP DoS Attack	19min./15sec.	19min./31sec.

Figure: Response Time to Attacks and Scans

Security Architecture Evaluation

- The following figure presents the response time of the distributed IDS system for various Nmap scans targeting the second and the third defense zone under different conditions of the CC environment concerning the CPU load and the network throughput.

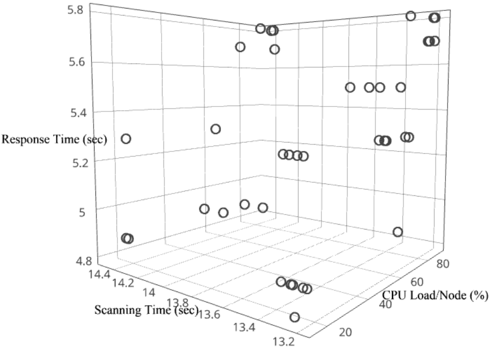


Figure: 3D plot for the scanning and response time of Nmap under different CPU loads

Security Architecture Evaluation

- The network throughput of the management and tunneling network were 900 Mbits/sec. and 1,2 Gbits/sec. respectively with deviation of 30 Mbits/sec.
- The results show that there is a pattern of metrics which could be used by the security administrator so as to improve the operation of the security mechanisms.
- The specified improvement would take place by modifying the IDS sensors' ruleset.
- Additional metrics to configure the IDS:
    - top 20 alarming signatures
    - top 20 alerts by date metric
    - alerts by source ip
    - alerts by destination ip
    - alerts categorized by severity
    - number of alerts by signature

Conclusions

- The presented CC security architecture propose the adaptation of the concept of defence in depth in a CC environment.
- The evaluation of the multilayered security architecture established that leads to mitigation of serious threats of this environment.
- The presented security architecture eases the task of securing the data in a CC environment by using legacy and CC security mechanisms.

End of presentation