Large-scale coordinated attacks: Impact on the cloud security

Damien Riquet  Gilles Grimaud  M. Hauspie

Team 2xS
Université Lille 1, France

MCNCS, Palermo, 2012
Study on the impact of distributed attacks on Cloud Computing

- Cloud Computing: a popular model to process large data set
- Several layers according to the needs of customers
- Store confidential data
- Growing concern about its security

Attacks on the cloud

- Distributed attacks to evade security solutions
- Weaknesses of cloud structure
D. Riquet, G. Grimaud, M. Hauspie

How Cloud Computing can be secured
Distributed portscan
Experimental protocol
Results
Conclusion

Large-scale coordinated attacks: Impact on the cloud
Goals of this paper

- Study security solutions used by Cloud Computing
- Show that distributed attacks could be very efficient
- 1-path architecture
- Use case: distributed portscan
Outline

1. How Cloud Computing can be secured
2. Distributed portscan
3. Experimental protocol
4. Results
Outline

1. How Cloud Computing can be secured
   - Security solutions commonly used
   - Detection methods

2. Distributed portscan

3. Experimental protocol

4. Results
Cloud security - Security solutions commonly used

Firewalls [BC94]
- At the border of the network
- Analyze traffic between two networks
- Security policies

Intrusion Detection System (IDS) [Ped05]
- Network or Host based
- Passive device: raise alarms
- Pattern-matching, analyze traffic
Detection methods

**Misuse detection**
- Look for known patterns of misuse
- Pattern-matching
- Need constant update of the database

**Anomaly detection**
- Knowledge of standard
- Raise an alarm when an anomaly is detected
- Detect unknown attacks
- May raise a lot of false positive
Outline

1. How Cloud Computing can be secured

2. Distributed portscan
   - Definition
   - Distribution methods

3. Experimental protocol

4. Results
Distributed portscan: a use case

[Shi00] A portscan is ...

«an attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service.»

Usage and goals

- Reconnaissance phase
- Discover weaknesses of a network
- Used by worms, malicious hackers
How to distribute a portscan

**Naive distribution [KCS07]**
- Sequential utilization of scanners
- Use a scanner until it is detected then select another one

**Parallel distribution**
- Distribute ports among scanners
- Execute portscan on scanners
- Process results afterwards
How Cloud Computing can be secured

2 Distributed portscan

3 Experimental protocol
   • Security solutions
   • Network architecture
   • Benchmark configurations

4 Results
Tested security solutions

**Snort**
- Popular open source IDS
- Detection methods
  - Signature-based (written by the community)
  - Threshold-based (sfPortscan module)

**Commercial firewall**
- United Threat Management (network firewall and an IDS)
- Detection methods
  - Anomaly-based (TCP Automaton)
  - Threshold-based
Network architecture

Cloud Computing

Internet host

Firewall / IDS

Cloud host
Benchmark configurations

### Network architecture
- Number of scanners: $2^n$, with $1 \leq n \leq 6$
- Number of targets (Snort): $2^n$, with $1 \leq n \leq 6$
- Number of targets (Commercial): 4
- Security solution configuration: default

### Portscan
- Portscan timing: | insane | aggressive | normal | polite |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5 ms</td>
<td>10 ms</td>
<td>0.4 s</td>
<td>0.4 s</td>
</tr>
</tbody>
</table>
- Number of ports: 100 per target (most used ports)
- Distribution methods: Naive and Parallel
- Portscan techniques: Connect, SYN, RPC, FIN, Xmas and Null
Outline

1. How Cloud Computing can be secured
2. Distributed portscan
3. Experimental protocol
4. Results
   - Evaluation
   - Connect scanning
   - Null scanning
   - Results wrap up
## Evaluation

### Attacker Success Rate

\[ n = \text{Number of ports successfully scanned before detection} \]
\[ T = \text{Total number of ports to scan} \]

\[ ASR = \frac{n}{T} \]

The lower is the ASR, the better is the security solution

Successful portscan:
- undetected
- correct port state
- generated traffic reaches targets
Connect scanning - 4 targets

Snort

Commercial firewall
How Cloud Computing can be secured
Distributed portscan
Experimental protocol
Results
Conclusion

Connect scanning - 4 targets

[Chart Showing ASR for Connect scanning with different protocols and numbers of targets]

Snort

Commercial firewall

[Charts for Snort and Commercial firewall showing ASR for various protocols]

D. Riquet, G. Grimaud, M. Hauspie
Large-scale coordinated attacks: Impact on the cloud ...18/26
Connect scanning - Snort

Snort - 8 targets

Snort - 32 targets
Connect scanning - Snort

Snort - 8 targets

Snort - 32 targets
Null scanning - 4 targets

![Graph showing ASR for Naive and Parallel Scanning for Snort and Commercial firewall.]

D. Riquet, G. Grimaud, M. Hauspie  Large-scale coordinated attacks: Impact on the cloud ...20/26
Null scanning - 4 targets

Evaluation
Connect scanning
Null scanning
Results wrap up

Commercial firewall

D. Riquet, G. Grimaud, M. Hauspie
Large-scale coordinated attacks: Impact on the cloud...
Distributed attacks could be very efficient:
- 32/64 scanners are enough to remain undetected
- Weaknesses of security solution (timing, outdated database)
- Parallel distribution succeeds in obfuscating the attack
- Commercial firewall has better results
Conclusion

- Study of security solutions commonly used
- Impact of distributed attacks on Cloud Computing
- 32 scanners are enough to remain undetected
- No network noise

Future work

- Multipath attacks
- Collaborative IDS using virtual and physical probes
Questions

Large-scale coordinated attacks: Impact on the cloud security

Damien Riquet - damien.riquet@lifl.fr
Gilles Grimaud - gilles.grimaud@lifl.fr
Michaël Hauspie - michael.hauspie@lifl.fr

http://www.lifl.fr/~riquetd/
References


Multipath attacks
Collaborative security system

D. Riquet, G. Grimaud, M. Hauspie

Large-scale coordinated attacks: Impact on the cloud ...26/26