Attacks on Cloud Computing

Nadra Waheed

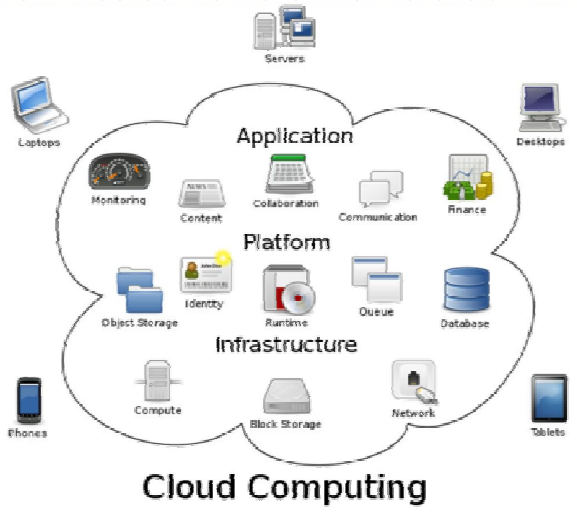
Content

- 1. Introduction
- 2. Cloud computing attacks
- 3. Cloud TraceBack
- 4. Evaluation
- 5. Conclusion

Introduction

- Today, cloud computing systems are providing a wide variety of services and interfaces to enable vendors to rent out spaces on their physical machines at an hourly rate for a tidy profit.

- The services that are provided by these vendors can vary from dynamically virtual machines to flexible hosted software services.



INTRODUCTION

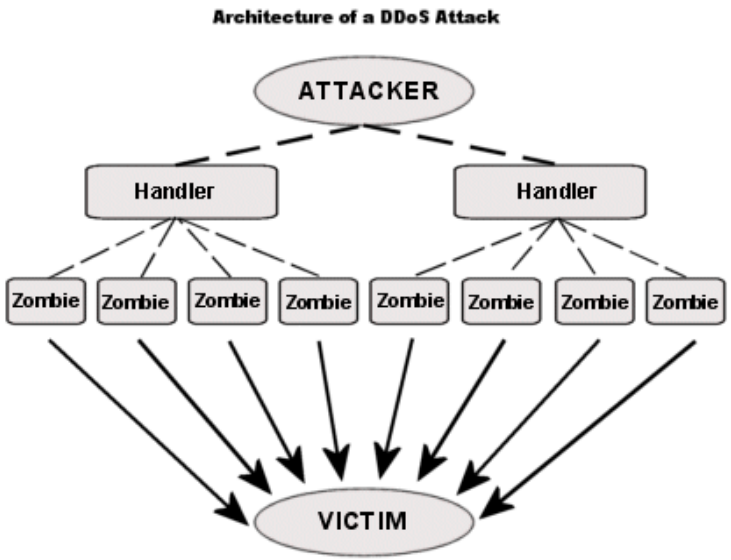
- With the emergence of cloud computing, multi-billion dollar organizations like IBM, Amazon, Google and Ebay have already invested in cloud technology.

- Threats
  - Extortionists
    - Using DDoS attack to exhaust server resources
  - Competitors
    - Using known vulnerabilities to interrupt services

- Distributed Denial of Service (DDoS) attack, which means many nodes systems attacking one node all at the same time with a flood of messages

INTRODUCTION

- The DDos Attack Tools
  - complex
    - Agobot
    - Mstream
    - Trinoo



  - Simple
    - Extensible Markup Language (XML) based Denial of Service (X-DoS)
    - Hypertext Transfer Protocol (HTTP) based Denial of Service (H-DoS)

INTRODUCTION

- X-DoS
  - Coercive Parsing attack
    - Open xml tags
    - Exhaust CPU usage
- H-DoS
  - Using HTTP Flooder
    - starts up 1500 threads
    - send randomized HTTP requests to the victim web server
    - exhaust victim's communication channels

INTRODUCTION

- Cloud TraceBack, CTB
  - service-oriented traceback architecture
  - to defend against X-DoS attacks the area of cloud computing.
- H-DoS attack
  - affected Iran
  - using the attack as an example of bringing down a cloud system
  - train our back propagation neural network called Cloud Protector
- Cloud Protector
  - back propagation neural network

Cloud computing attacks

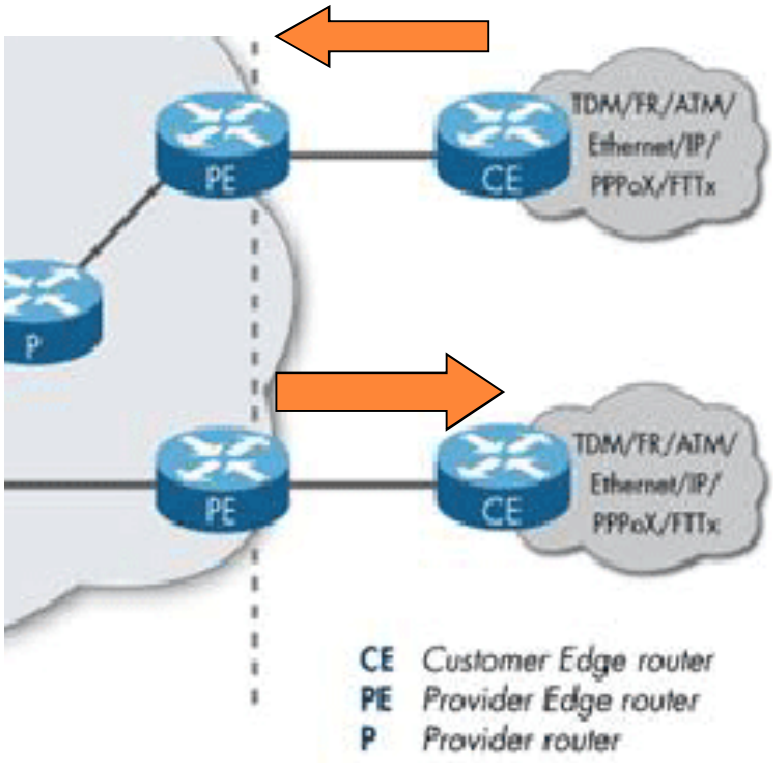
- Two security areas
  - VM vulnerabilities
  - Message integrity

Cloud computing attacks

- Service-oriented traceback architecture, SOTA
  - A web security service application
  - Apply a SOA approach to traceback methodology
  - Identify a forged message identity
  - Using ID field and reserved flag within the IP header

Cloud computing attacks

DPM methodology



As each incoming packet enters the edge ingress router it is marked. The marked packets will remain unchanged as they traverse the network.

Outgoing packets are ignored

*http://www.ixiacom.com/images/library/test_plans/edge-router/img1.gif

Cloud computing attacks

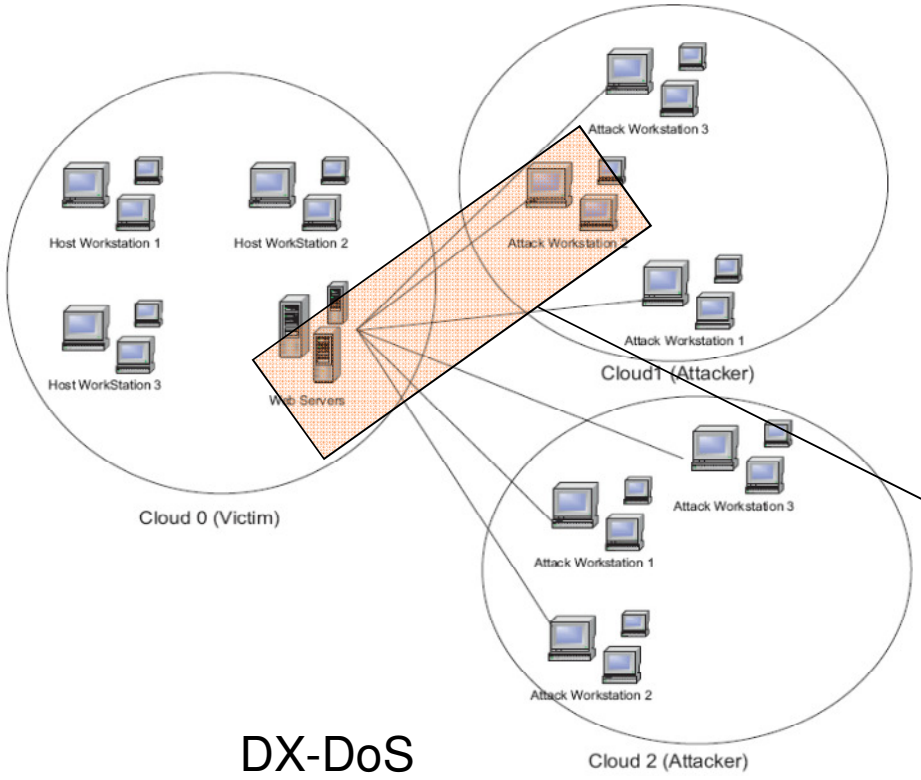
- DPM + SOTA = SOTM
- by placing the Service- Oriented Traceback Mark (SOTM) within web service messages
- Other web security services
  - SOTM would replace the 'token' that contains the client identification

Cloud computing attacks

- The main objectives of X-DoS and DX-DoS
  - Exploit a known vulnerability
  - Flood the system with useless messages to exhaust the web server's resources
  - Attackers who try to hide their identities.
  - cover their crime or to bypass a known defence that is in place to prevent it.

Cloud computing attacks

- XML-based denial of service (X-DoS) attacks



DX-DoS

a network is flooded with XML messages instead of packets in order to prevent legitimate users to access network communications.

X-DoS

CLOUD TRACEBACK

- Attackers can target
  - Bandwidth
  - Processing power
  - Storages capacities of a cloud network

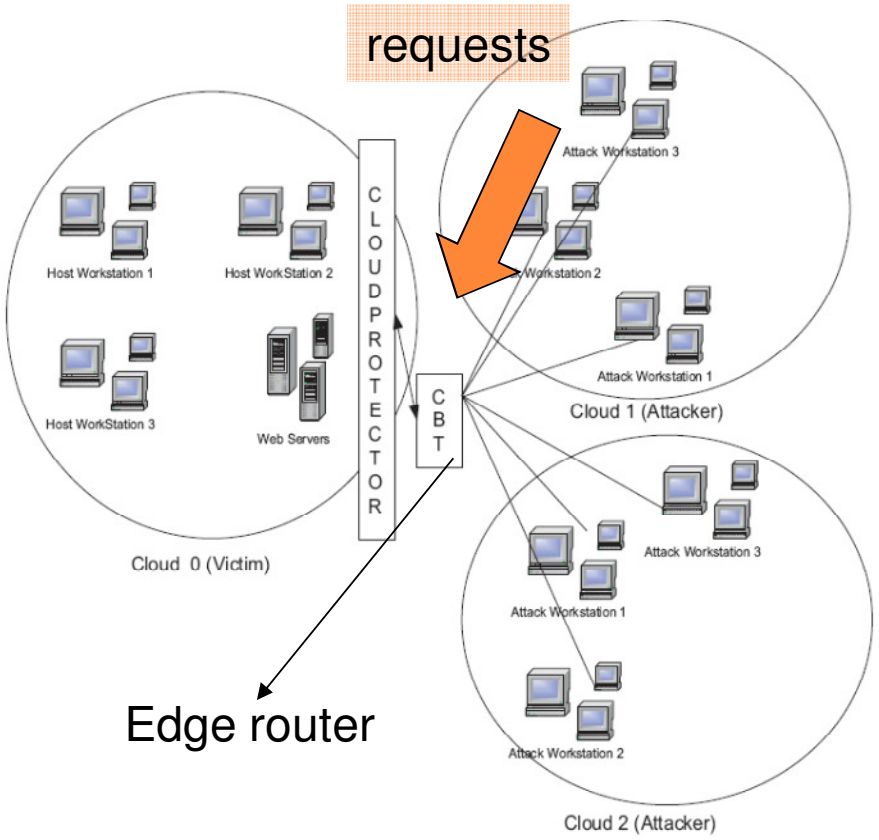
- Cloud computing
  - limited resources
  - has to provide a highly quality service

Cloud TraceBack

- Cloud traceback description
  - Cloud TraceBack (CTB) can be used in
    - LAN
    - Grid network structure
  - CTB is made within a virtual machine
    - Compatible
    - Flexible
    - Scalable

CLOUD TRACEBACK

- CTB placement within cloud system infrastructure



place a Cloud Traceback Mark (CTBM) tag within the CTB header.

CTB marks all requests to
(1) Prevent attack
(2) Hide server address
(3) Identify request sources

CLOUD TRACEBACK

- Cloud Protector
  - A trained back propagation neural network (NN)
  - To help detect and filter out X-DoS messages

Cloud TraceBack

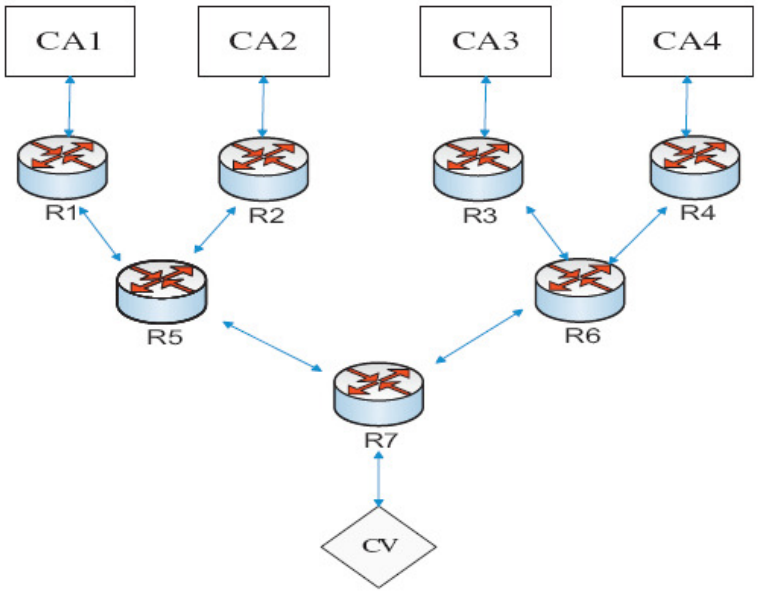
- Properties and Characteristics of CTB
  - Loosely coupled
  - Dynamic discovery
  - Late binding
  - Policy based behavior

CLOUD TRACEBACK

- CTB's algebraic approach to determining path and reconstruction

attacker

router

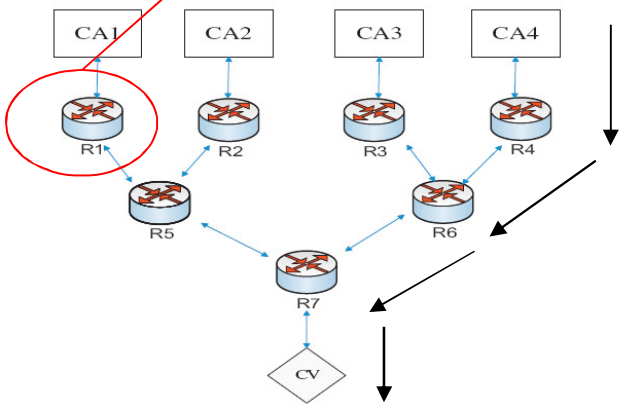


victim

The Path CA1 to CV
R1R5R7

CLOUD TRACEBACK

Algebraic Coding of Paths schemes are based on the principal of reconstructing a polynomial in a prime field. The basic idea is that for any polynomial $f(x)$ of degree d in the prime field $GF(p)$, we can recover $f(x)$ given $f(x)$ evaluated at $(d+1)$ unique points. Let $A_1, A_2, \ldots, A_n$ be the 32-bit IP addresses of the routers on path P. Let $f_P(x) = A_1 x^{n-1} + A_2 x^{n-2} + \ldots + A_{n-1} x + A_n$. We associate a packet id x_j with the jth packet. We then somehow evaluate $f_P(x_j)$ as the packet travels along the path,



A path

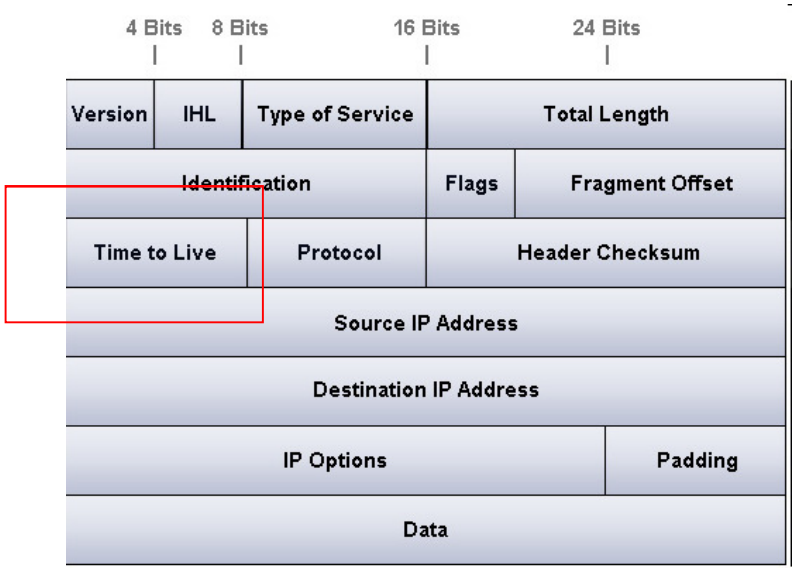
$$\begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{pmatrix} = \begin{pmatrix} FullPath_{n,1} \\ FullPath_{n,2} \\ \vdots \\ FullPath_{n,3} \end{pmatrix}$$

Cloud TraceBack

Approaches for encoding traceback information

- Algebraic Coding of Paths
- Deterministic Path Encoding
- Randomized Path Encoding
- Edge Encoding

CLOUD TRACEBACK



a distance field can also be introduced via the use of the time-to-live value within the packet that the message comes in.

With this distance field, it simplifies path reconstruction

*http://www.learn-networking.com/wp-content/oldimages/ip-header-diagram.jpg

EVALUATION

- The experiment and evaluation of CTB
  - The simulation of how a CTB works
  - How accurate CTB is at identifying the source of where the message comes from

EVALUATION

- HTTP DoS attack experiment and evaluation
  - Simulate the DDoS attacks on Iran
  - Attackers using web-based attack tools
    - Page Rebooter
    - IFrames
    - Do-It-Yourself (DIY)

EVALUATION

- Experiments using CTB
  - Dell Dimension DM501
  - Intel Pentium single-core CPU,3.0GHz,
  - 2GB RAM
  - 2300 GB SATA hard-drives.
  - The software that was installed was .NET Web Services along with VB.Net

Evaluation

- Experiments using CTB
- The first group of experiments were broken up into two sections:
  - The first section of experiments simulated X-DoS attacks against a cloud service provider
  - The second section of the experiments is done to compare CTB against SOAP authentication and WS-Security

EVALUATION

- To simulate the success of an attack
  - Not crash
    - The service provider was able to trace the message source and initiate filtering procedures.
  - Crash
    - Assumed the service provider would restart services.
    - Access CTB reconstruction and find the source of the attack.
    - Filtering of the X-DoS traffic is left to the experiments and evaluation section of the Cloud Protector.

EVALUATION

```
CTBM procedure at CTB, edge Interface I

For each incoming request message w
If no header then
   create SoapHeaderAttribute("client id")
   Invoke Header new SoapHeaderAttribute
Else
   get WSSusernameToken(xx)
   WSSusername = new client id
```

Fig. 8. Pseudocode to extract Header of the message that is coming into CTB.

With or without header ?

The establishment of the id attribute

Use the id as the user name

```
Identification reconstruction procedure at web server
For each message request w from source Sx
        Create a table array
        Ws.tx = extract Transactioninfo()
        Ws.tx.time_and_date = timestamp
        Ws.tx.usernameId = usernameID
        Table_array[]+ = Ws.txusernameID
End
Display of username at particular time of the attack
For each Table_array[]
        Get what time of attack
        Get usernameID from Table_array[]
Display usernameID
```

Fig. 9. Pseudocode to extract, store and display username identification.

Storing user information

Displays the information of the attacker Time id

EVALUATION

- Cloud Protector experiments
  - The datasets were split into two groups
    - a training set (1000 data points)
    - a test set (1000 data points).
    - the Cloud Protector will firstly be trained with the trained dataset and then tested against the test dataset.
  - Cloud Protector for X-DoS attacks
  - Cloud Protector for H-DoS attacks

Conclusion

- Trace and Protect
  - CTB
    - can be used in an actual X-DoS attack
    - trace the attack back to the source.
    - our results showed that CTB is able to find the source of an attack within a matter of seconds
  - Cloud Protector
    - a neural network that was trained to detect and filter X-DoS attacks.
    - the result we achieved was around 98–99% of the attack traffic within an average of 10–135 ms.

REFERENCES:

- http://www.beknowledge.com/wp-content/uploads/2010/10/eccbcCloud-security-defence-to-protect-cloud-computing-against-HTTP-DoS-and-XML-DoS-attacks_(pub_year)_Journal-of-Network-and-Computer-Applications.pdf
- http://dro.deakin.edu.au/eserv/DU:30018209/Zhou-protectingwebservices-2008.pdf
- http://en.wikipedia.org/wiki/Homomorphic_encryption
- http://articles.latimes.com/2011/jun/17/business/la-fi-cloud-security-20110617
- http://www.ists.dartmouth.edu/docs/HannaCloudComputingv2.pdf
- https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
- http://www.zdnet.com/news/cryptography-experts-debate-cloud-computing-risks/290726
- http://www.cs3-inc.com/images/attack.gif

Quiz

QUESTIONS:

1- List two DDoS attack complex tools.

2- Which DoS attack affected Iran?

3- What are the two main areas need to be secured in a cloud system?

4- List three Properties and Characteristics of CTB.

5- Is CTB able to find the source of an attack within a matter of seconds?

ANSWERS:

1-Agobot, Mstream, Trinoo

2-H-DoS

3-VM vulnerabilities and Message integrity

4-

- Loosely coupled
- Dynamic discovery
- Late binding
- Policy based behavior

5- Yes

The End