AN TOÀN DỊCH VỤ MẠNG LỚP ỨNG DỤNG: ADDRESS AND NAME ATTACK

PTITHCM

Nguyen Hong Son

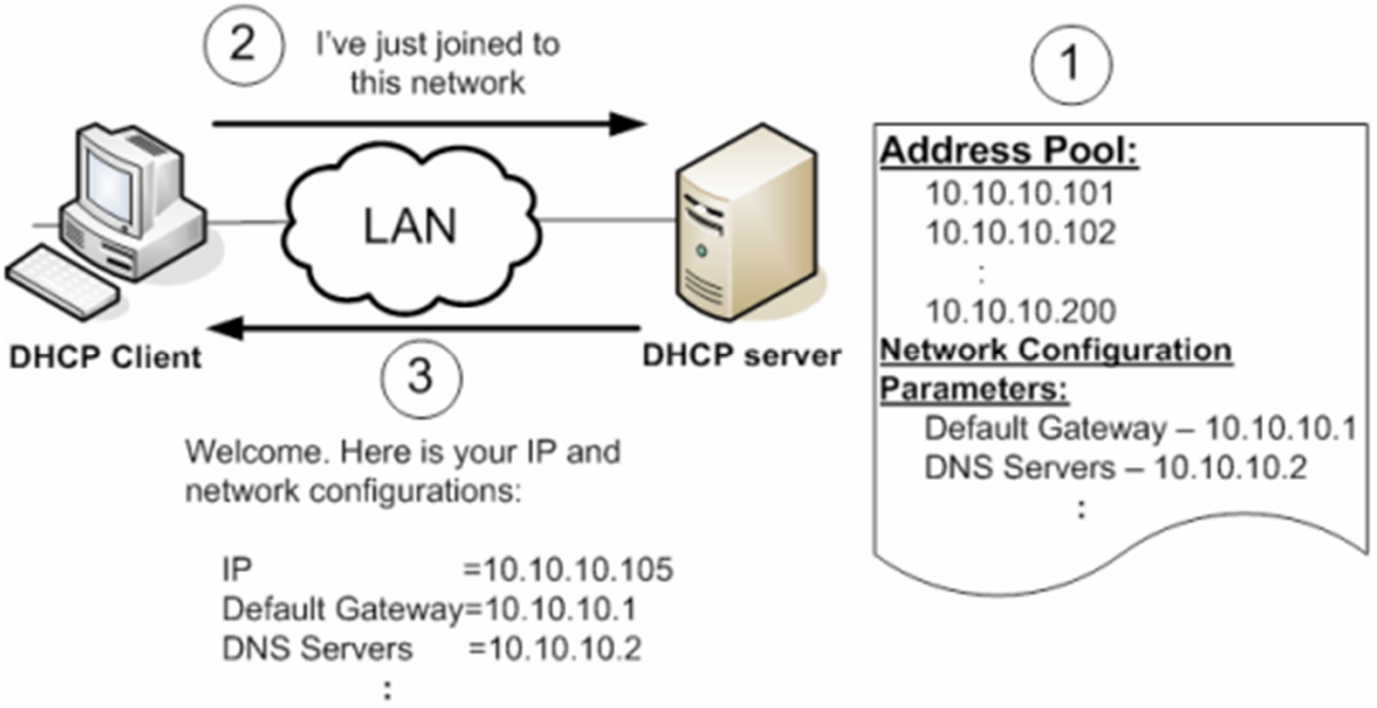
DHCP Attack

- DHCP concept
- DHCP operation
- Attacks

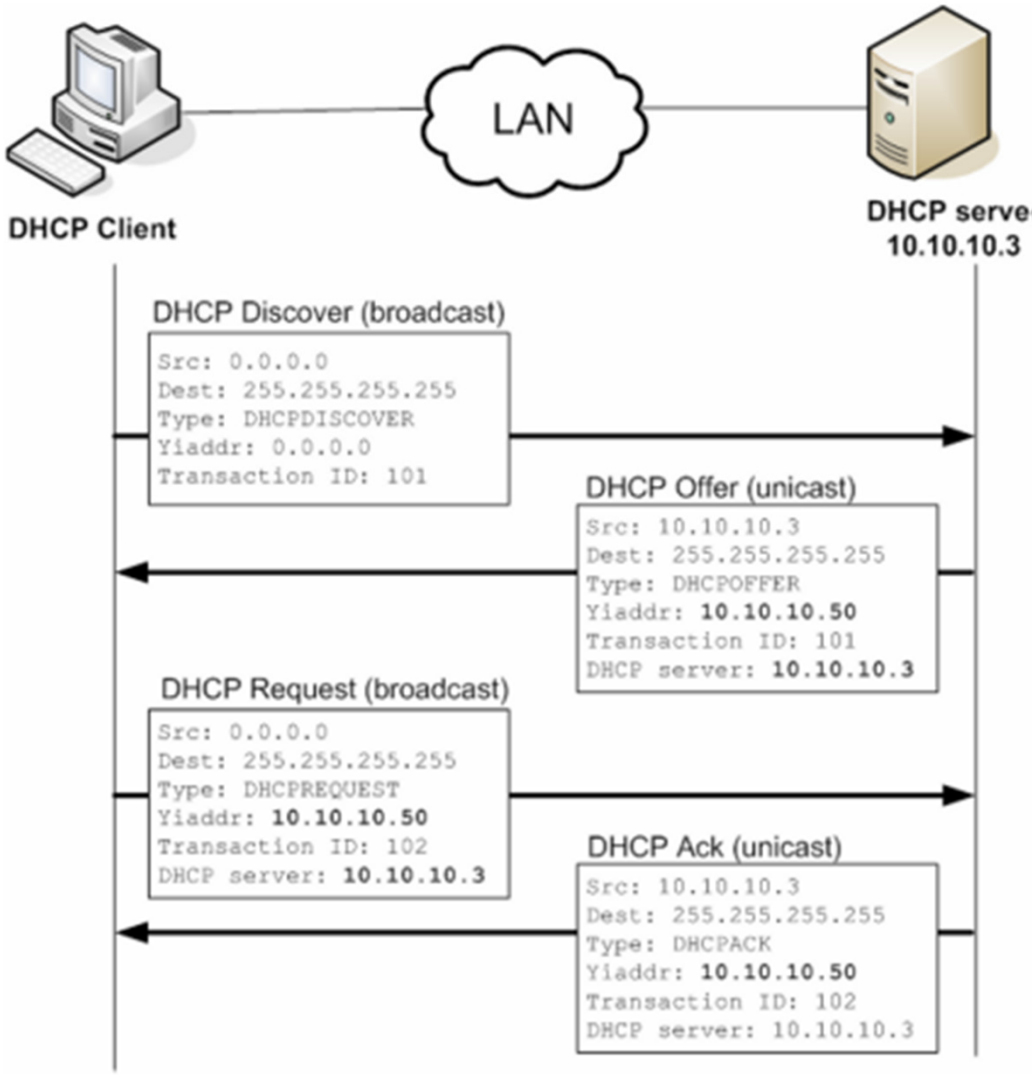
DHCP Concept

- Dynamic Host Configuration Protocol (DHCP) is used to automatically configure client machines with a dynamically assigned IP address and other network configuration parameters, such as the default gateway and DNS server addresses, during their boot time. It eliminates the need for network administrators to keep track of individual client IP addresses

DHCP Operations



DHCP Operations

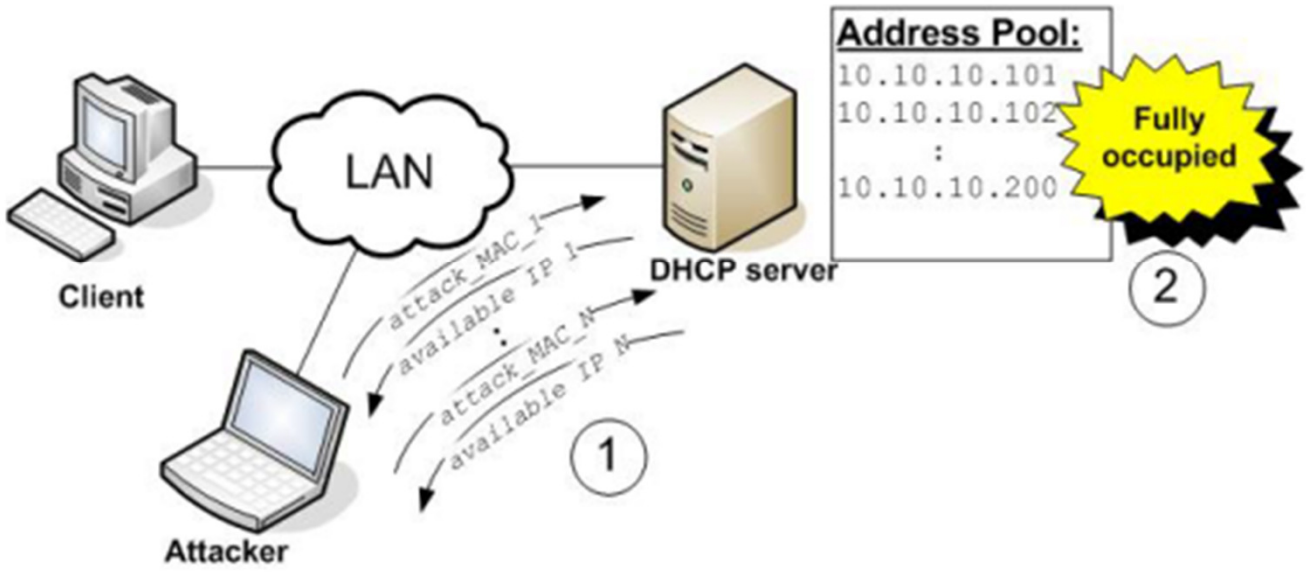


Attacks

- Address starvation
- Server impersonation

Denial of Service Attack using Address Starvation

- The principle of the former is to request all of the available DHCP addresses so that new clients are not able to get IP addresses
- Sending a large number of DHCP requests with different (forged) MAC addresses to the DHCP server


Address Pool:
10.10.10.101
10.10.10.102
:
10.10.10.200
Fully occupied
LAN
Client
DHCP server
Attacker
attack_MAC_1
available IP 1
attack_MAC_N
available IP N
1
2

Countermeasures

- The attack can be easily mitigated with the security functions in today's sophisticated switches
- Cisco switches can limit the number of MAC addresses a switch port can use

Man-in-the-middle Attack using Rogue DHCP server (1/2)

- Set up a rogue DHCP to return fake network information to clients so that man-in-the-middle attacks can be achieved

Man-in-the-middle Attack using Rogue DHCP server (2/2)

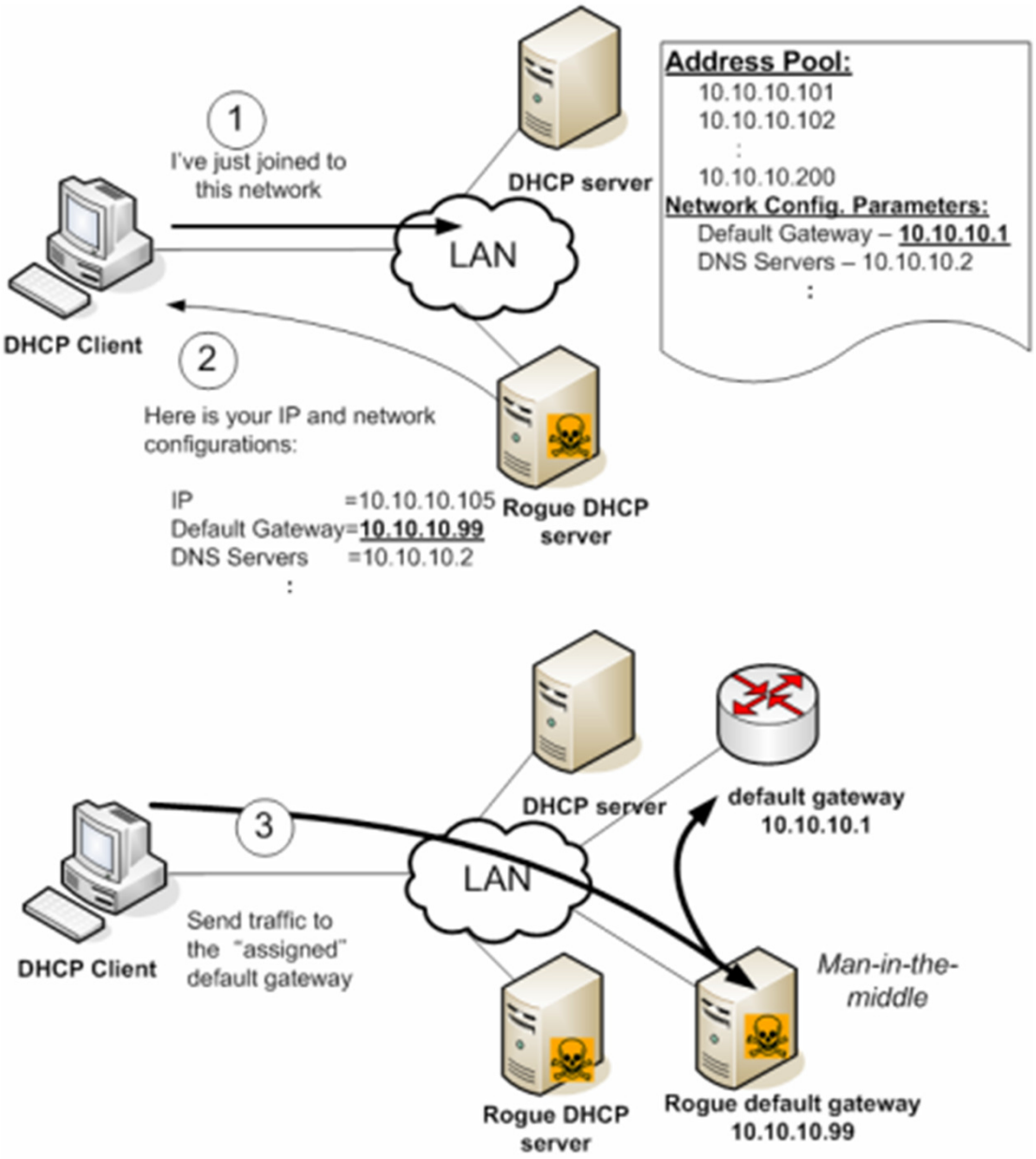
1.The attacker first grabs an IP address from the legitimate DHCP server for the future use. It runs its rogue DHCP server.

2. When a DHCP client broadcast a DHCPDISCOVERY packet, both the legitimate and the rogue servers send a DHCPOFFER to the client.

3. The client accepts the response from whichever DHCP responds first.To ensure the client accept the respond from the rogue server, the attacker can first deny the service from the legitimate server using the address starvation attack mentioned above.

4.In the rogue server's response, the default gateway address points to the attacker's own machine.

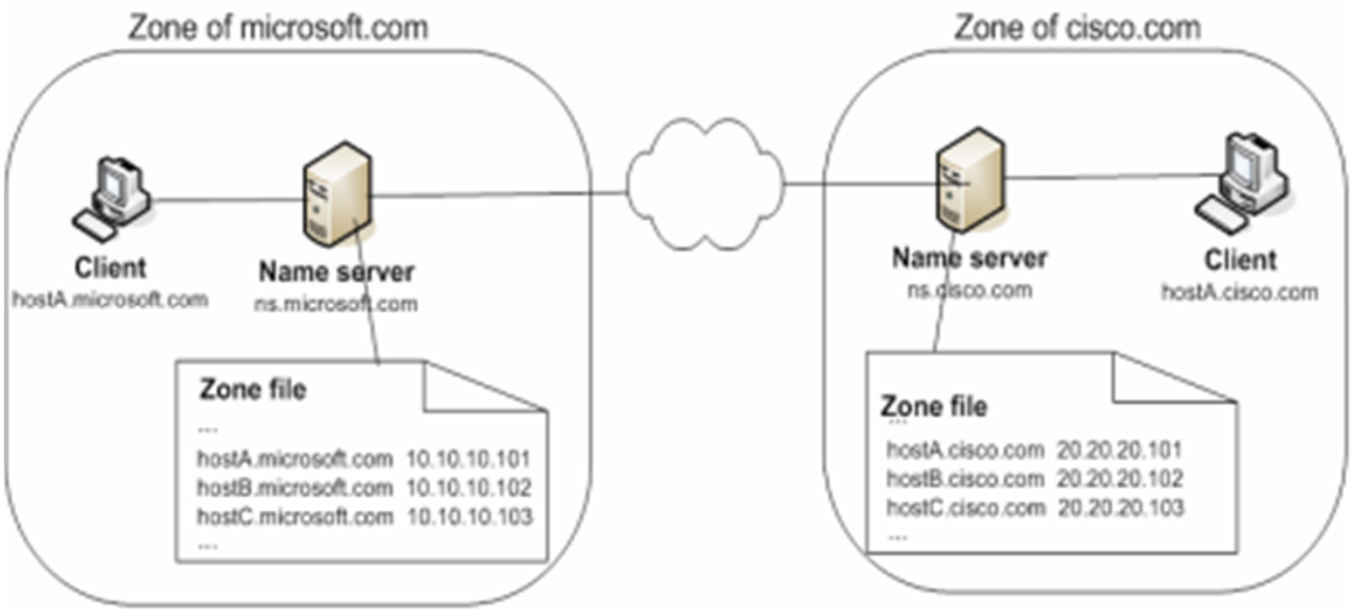
5.Then, whenever the client has packets to the destinations outside the local network, the packets will be sent to the rogue default gateway that would capture the content of the packets.


Address Pool:
10.10.10.101
10.10.10.102
:
10.10.10.200
Network Config. Parameters:
Default Gateway – 10.10.10.1
DNS Servers – 10.10.10.2
:
1
I've just joined to this network
DHCP server
LAN
DHCP Client
2
Here is your IP and network configurations:
IP =10.10.10.105
Default Gateway=10.10.10.99
DNS Servers =10.10.10.2
:
Rogue DHCP server
DHCP server
default gateway 10.10.10.1
3
LAN
DHCP Client
Send traffic to the "assigned" default gateway
Man-in-the-middle
Rogue DHCP server
Rogue default gateway 10.10.10.99

DNS Attack

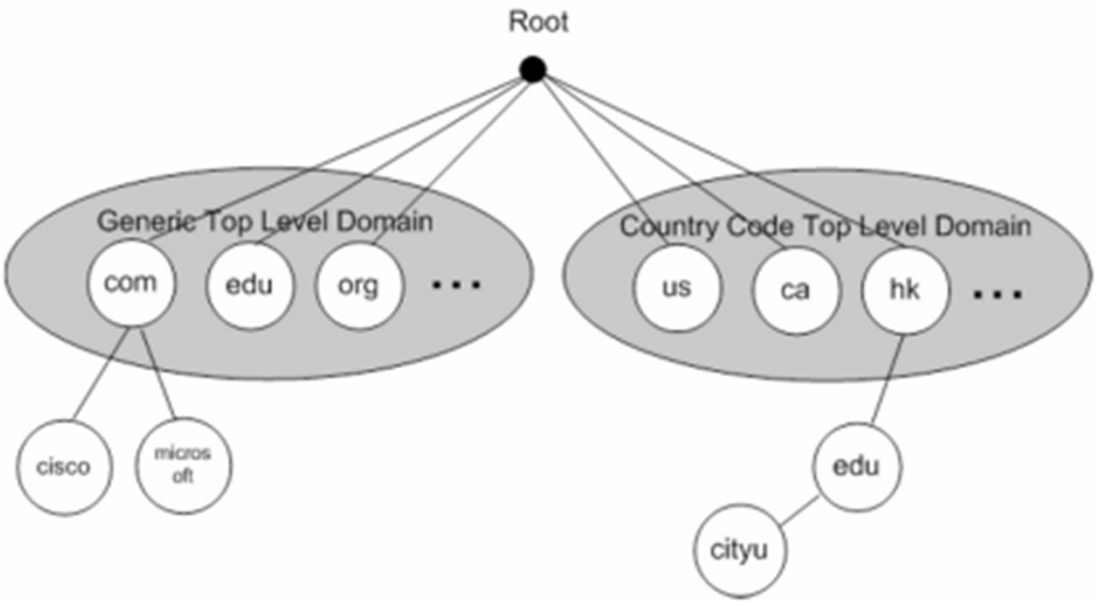
- DNS Basic
- DNS Vulnerabilities
- DNSSEC

DNS Concept


Zone of microsoft.com
Zone of cisco.com
Client
hostA.microsoft.com
Name server
ns.microsoft.com
Zone file
...
hostA.microsoft.com 10.10.10.101
hostB.microsoft.com 10.10.10.102
hostC.microsoft.com 10.10.10.103
...
Name server
ns.cisco.com
Client
hostA.cisco.com
Zone file
...
hostA.cisco.com 20.20.20.101
hostB.cisco.com 20.20.20.102
hostC.cisco.com 20.20.20.103
...

DNS Space

- The TLDs can be classified as the following three types:
  - Country-code TLDs (ccTLDs) – domains established for countries and territories, which include .hk, .mo, and .uk.
  - Sponsored generic TLDs (gTLDs) – specialized domains with a sponsor representing the narrower community that is most affected by the TLD. These TLDs include .edu, .gov, .int, .mil, .aero, .coop, and .museum.
  - Unsponsored generic TLDs (gTLDs) – domains without a sponsoring organization. These TLDs include .com, .net, .org, .biz, .info, .name, and .pro.



DNS Components

- As defined in RFC 1034, has three major components:
  - Zone files: Zone files are the text files containing the IP-host mappings for all nodes or hosts within the zone, defined in RFC 1035
  - Name servers
  - Resolvers: A resolver can be a background process, or just a set of library routines that is embedded in the application programs, e.g., Web browser and FTP client

DNS packet format and valid response (1/2)

0	15	16	31
Transaction ID		Flags	
Total Questions		Total Answer RRs	
Total Authority RRs		Total Additional RRs	
Questions			
Answer Resource Record structures			
Authority Resource Record structures			
Additional Resource Record structures			

DNS packet format and valid response (2/2)

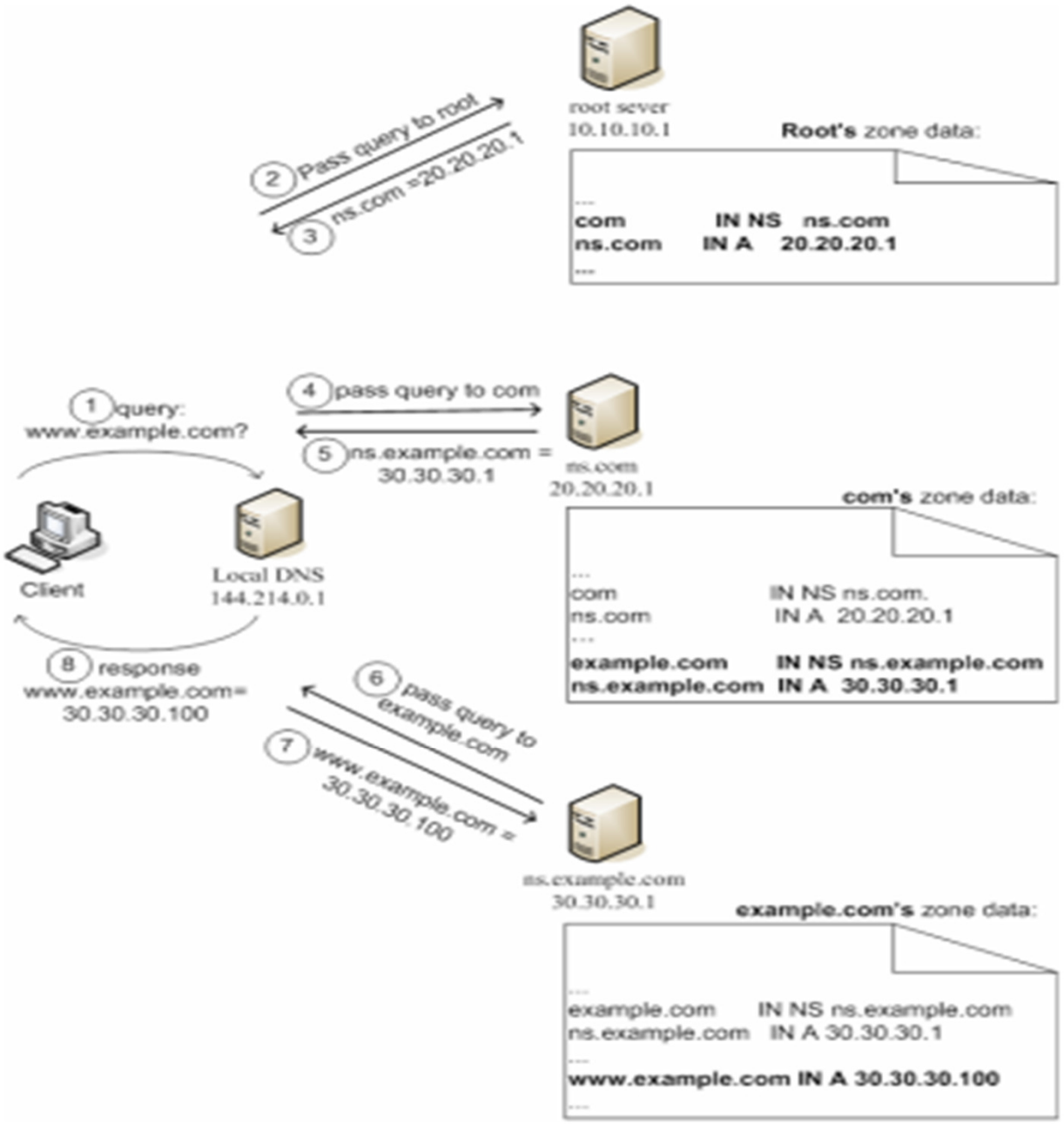
- The client only accepts the responses with the same IP address, port number and transaction ID as the ones in its query. An example of valid response is shown below

Query	Response
Transaction ID : **5858**	Transaction ID : **5858**
Source IP : **12.12.12.12**	Destination IP : **12.12.12.12**
Source Port : **36**	Destination Port : **36**
Que: IP of www.cityu.edu.hk?	Ans: www.cityu.edu.hk=144.214.5.218

Zone transfer

- Each zone can have more than one name server, but only one name server can be the master server for the zone. Other servers are referred to as slaves or secondary servers.
- The master server is where the actual changes to the zone data take place. The slave servers will maintain copies of the master's zone data. When the master server is down, a slave server will take over its tasks.
- A slave server updates the entire content of its zone file from the master server. This process is to keep the slave's zone file in synchronization with the master's one

Na


root sever
10.10.10.1
Root's zone data:
...
com IN NS ns.com
ns.com IN A 20.20.20.1
...
2 Pass query to root
3 ns.com =20.20.20.1
1 query:
www.example.com?
4 pass query to com
5 ns.example.com =
30.30.30.1
ns.com
20.20.20.1
com's zone data:
...
com IN NS ns.com.
ns.com IN A 20.20.20.1
...
example.com IN NS ns.example.com
ns.example.com IN A 30.30.30.1
Client
Local DNS
144.214.0.1
8 response
www.example.com=
30.30.30.100
6 pass query to
example.com
7 www.example.com =
30.30.30.100
ns.example.com
30.30.30.1
example.com's zone data:
...
example.com IN NS ns.example.com
ns.example.com IN A 30.30.30.1
...
www.example.com IN A 30.30.30.100
...

Caching

- The cost of name resolution for non-local hosts is very high, which involves a number of round trips between name servers on the Internet.
- Therefore, name servers use cache to make the DNS service more efficient.
- Name servers will store the DNS answers locally for a specified TTL (time to live) period

DNS Vulnerabilities (1/2)

- Client commonly trusts its preconfigured DNS server, it will regard all resolution response from the server valid
- There are three approaches to return fake information:
  1. To modify the zone file
  2. To synchronize a slave server with fake zone files
  3. To return fake IP information to clients

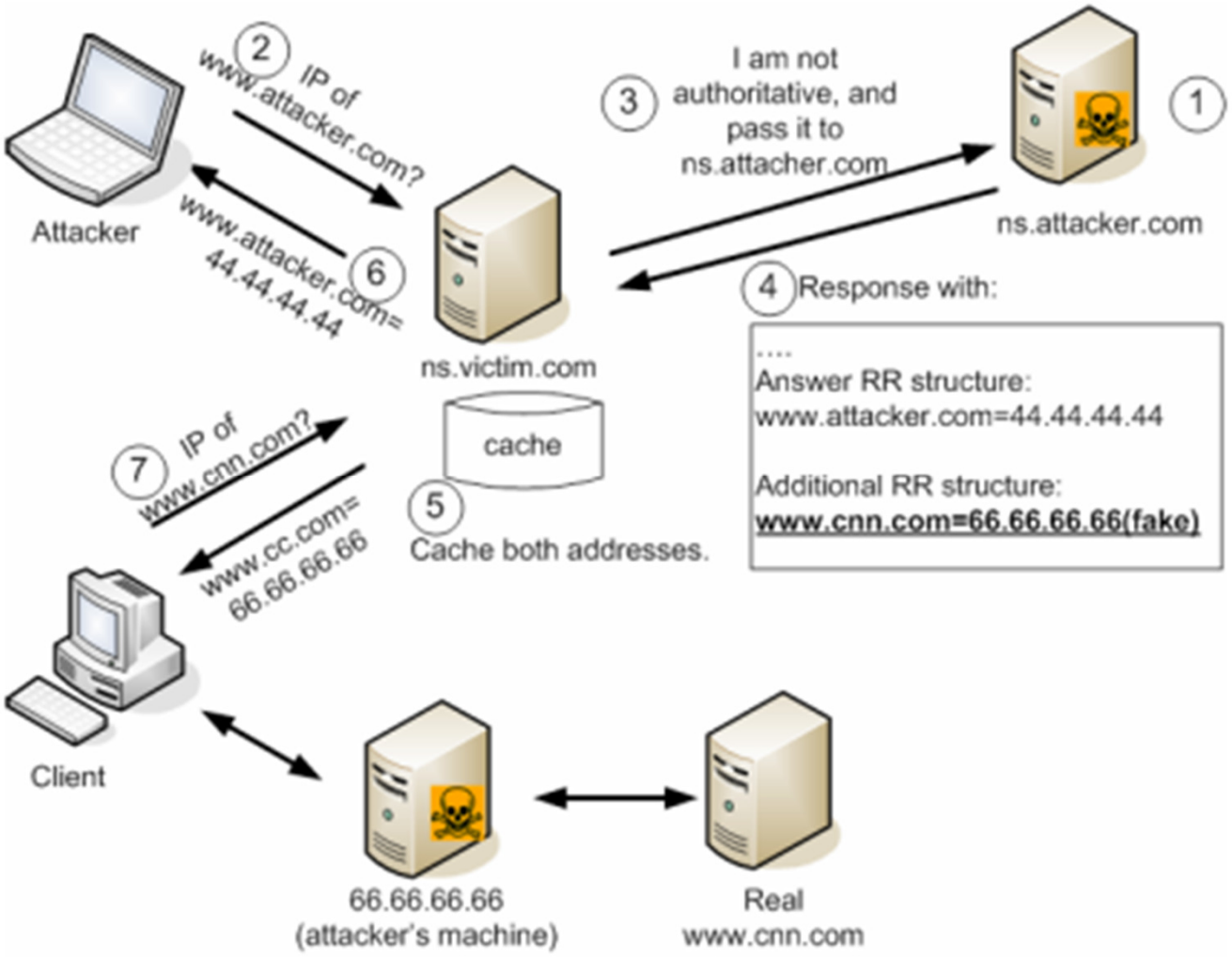
DNS Vulnerabilities (2/2)

- To modify the zone data, the most direct way is to compromise the DNS server and gain the command-level access, which involves host security.
- Can also send incorrect zone data to a DNS server (slave) through a normal zone transfer process.
- Another approach is to return fake IP information to clients during the name resolution process, which can be achieved by a number of ways

Cache Poisoning Attack

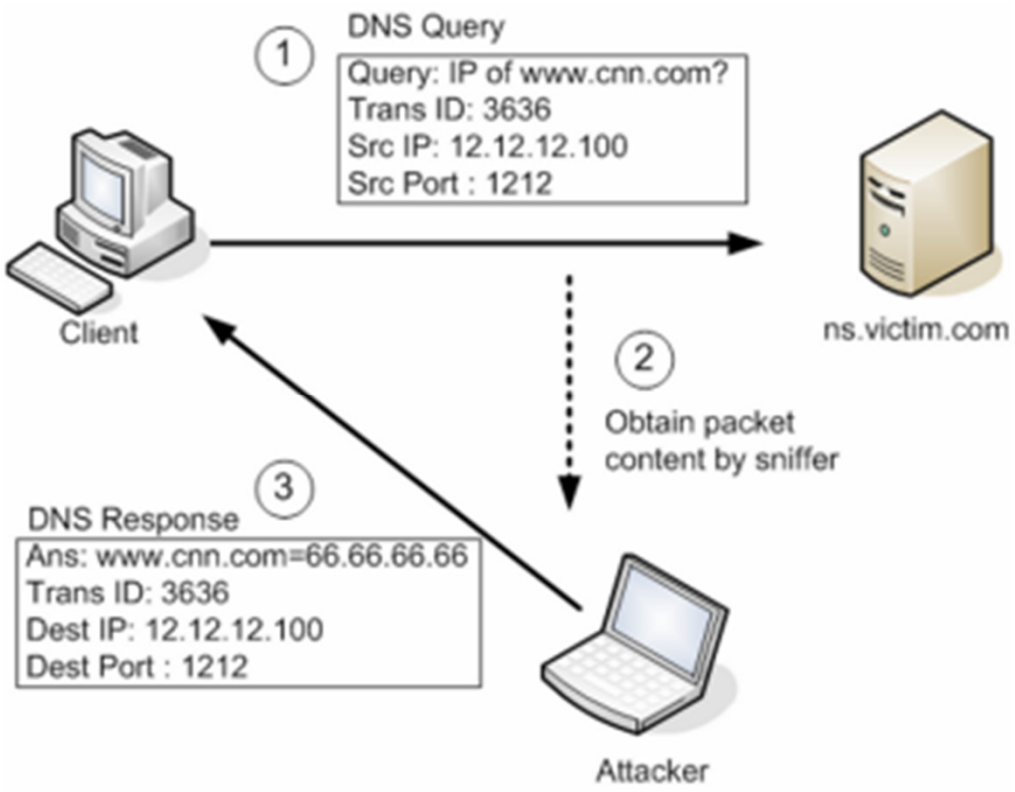
- Attackers can abuse the cache function by putting incorrect information in a DNS server's cache
- There are a number of ways to perform cache poisoning

Set up a rogue DNS server with malicious records



Send a spoofed reply to the victim client with the help of a sniffer

- The attacker is able to place himself between the client and the DNS server, it could intercept the DNS request and send a reply with false information the client
- To know this ID, the attacker can run a sniffer that captures all network packets
- The attacker must reply before the legitimate DNS server does. The attacker can use DoS attacks to slow down the legitimate DNS server

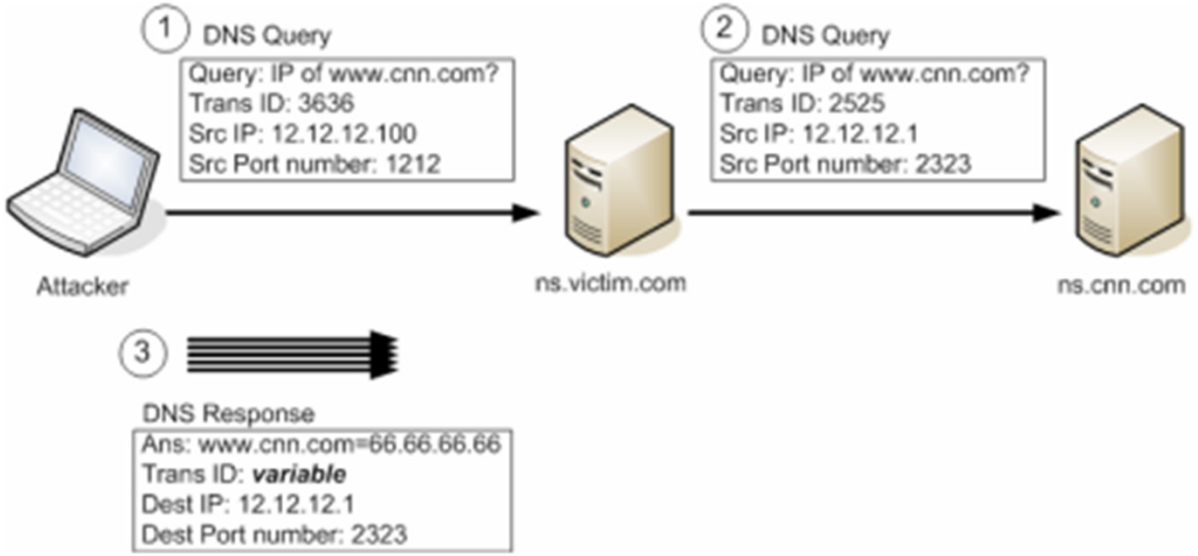

1
DNS Query
Query: IP of www.cnn.com?
Trans ID: 3636
Src IP: 12.12.12.100
Src Port : 1212
Client
ns.victim.com
2
Obtain packet
content by sniffer
3
DNS Response
Ans: www.cnn.com=66.66.66.66
Trans ID: 3636
Dest IP: 12.12.12.100
Dest Port : 1212
Attacker

Send a large number of spoofed replies to the victim client

- The attack of DNS ID spoofing requires the attacker to know the transaction ID first. It can be done by sending a large number of replies using various values of transaction ID, hoping that any one of them would match the one the client is using.

Send a large number of spoofed replies to the victim DNS server

- The attacker can make his own query and then send its malicious reply to the DNS server. Then, the DNS server will contain a fake DNS entry



- The attacker has to tackle two technical difficulties:
  - ID transaction
  - DNS's port number

Buffer Overflow Attack

- To make use of the buffer-length computation bug in DNS server implementation to execute unpredictable commands on the server
- A malicious DNS response packet with unreasonable values (e.g., contains a very long hostname or a very large value of packet length) may cause some server implementations to overwrite data outside their buffer, allowing the attacker to gain command-level access

Zone Transfer Attack

The aim of this attack is to place the incorrect data in the slave server through the normal zone transfer process between the master and slave servers.

1. The attacker first performs a man-in-the-middle attack and becomes capable of intercepting the traffic between the master and slave servers.
2. When the slave asks the master server to perform a zone transfer, the attacker can intercept the query, and then return fake data to the slave server.
3. The slave now contains incorrect data.
4. The attacker then performs a DoS attack to make the master server out of service.
5. The slave server now acts as the master server and starts to serve its clients.
6. The clients would then receive the incorrect data from the server

Denial of Service Attack

- Another form of DoS can be achieved by making use some of the resource record types in zone file.
- For example, Name Server (NS) record: attacker can poison the cache of a DNS server with a NS record such as “ibm.com. IN NS ns.attacker.com”, the server will refer ns.attacker.com to the clients querying any host of ibm.com. It denies the clients from having the correct name service provided by ibm.com.
- For example, Canonical Name (CNAME) record: attacker can poison the cache of a DNS server with a CNAME record “www.cityu.edu.hk IN CNAME www.cityu.edu.hk”, which refers to itself as the canonical name

Dynamic Update Attack

- After manually editing the zone file, the name server has to be restarted to make the changes effective. When the volume of changes is high, this can become operationally unacceptable.
- To efficiently change zone data, the dynamic update function (RFC 2136) is used.
- The process of dynamic update is insecure. An attacker can easily change a server's zone data by send forged dynamic update packets (which is UDP).

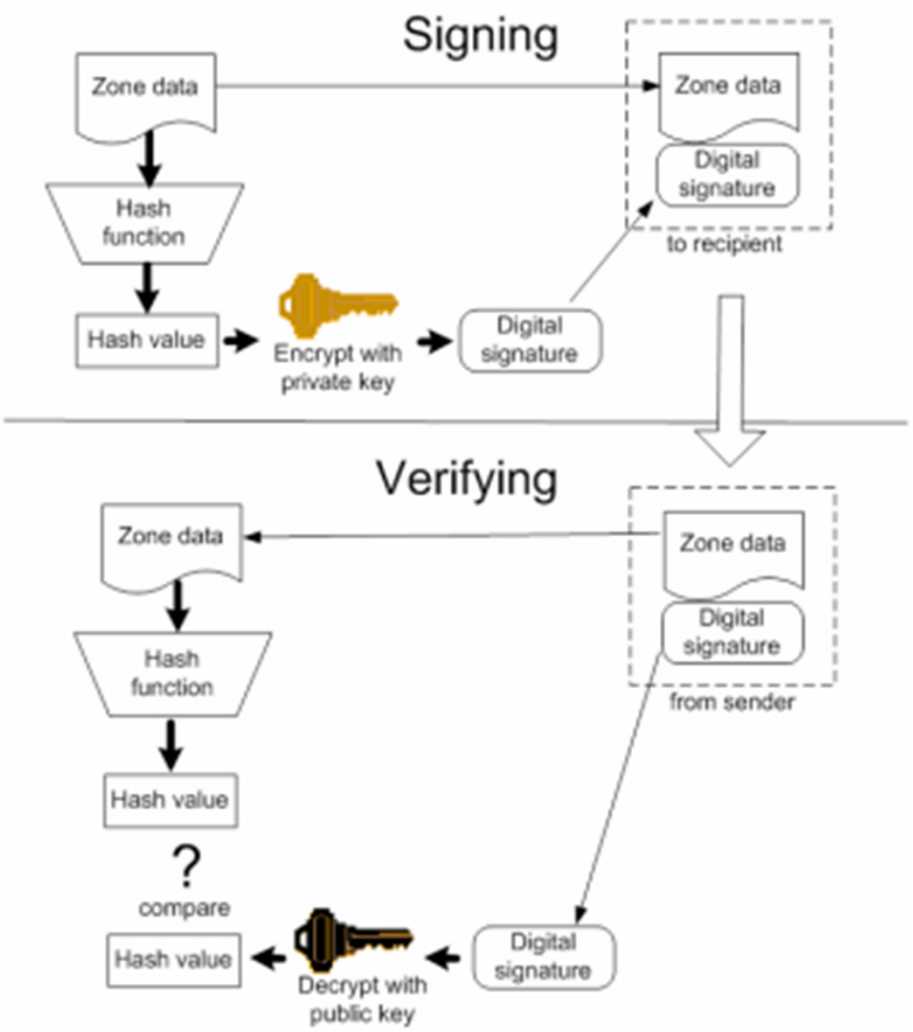
DNSSEC

- One technique for securing DNS is through the use of DNS Security Extensions (DNSSEC)
- http://www.dnssec.net

DNSSEC background

- The most important thing is to ensure that the requesting client receives the right response from the right name server
- The objectives of DNSSEC are to provide origin authentication and data integrity, which is achieved by using digital signature.
- It can detect most information integrity related attacks, such as cache poisoning, and zone transfer
- DNSSEC is not to provide confidentiality to the DNS. The reason is that, since name service is considered as public service and DNS data is considered as public data, access control or any confidentiality should not be imposed

Public-key Cryptography in DNSSEC (1/2)



Public-key Cryptography in DNSSEC (2/2)

- Instead of signing individual resource records, DNSSEC signs a group of resource records having the same owner, class and type.
- For example, all address records (type “A”) in a zone file will be signed together, whereas all name server records (type “NS”) in a zone file will be signed together

New Resource Record (RR) Types in DNSSEC

- DNSSEC adds four new resource records to provide the security functions

DNSKEY	(DNS Public Key)	To store the actual key string about the zone's public key
RRSIG	(Resource Record Signature)	To store the digital signatures of resource record sets
NSEC	(Next Secure)	To store the next domain name
DS	(Delegation Signer)	To store the signature of the public key of the child zone

DNSKEY

- Public key is stored in the DNSSEC record, so that one can learn a zone's public key through normal DNS resolution
- Example of DNSKEY RR for example.com

```
example.com. 86400 IN DNSKEY 256 3 5 (CDGGJUdsfsggYUYnv015UG2DeIQ3
                                      454SDFDvsCb/0Pfdkw44bfgfc8no
                                      dSfsdfioi+6hjhJHJVMfzj31GajI
                                      bWqTqXQpftf6zgiaogmMf6ZEzODz
                                      74M9vJVM7ffgHJe4KHJ7za6dfdEz
                                      7Mgv/TpPdfghh98NKifjhfsppn1U
                                      baTxyw==)
```

The meaning of these field values can be found in RFC 4034

Limitations of DNSSEC

- First, it requires better knowledge and administration skills to maintain a DNSSEC server.
- Second, performance issues and operational overhead are of the major concerns
- DNSSEC is not designed to provide confidentiality and access control lists, it provides no protection against denial of service attacks. DNSSEC does not prevent attacks. It is only able to detect attacks

Fast Flux technology

- **Fast flux** is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies
- The basic idea behind Fast flux is to have numerous IP addresses associated with a single fully qualified domain name, where the IP addresses are swapped in and out with extremely high frequency, through changing DNS records
- Internet users may see fast flux used in phishing attacks linked to criminal organizations, including attacks on social network services.

The End