

ECE/COMPSCI 356 Computer Network Architecture

Lecture 24: DNS and its Security

Neil Gong
neil.gong@duke.edu

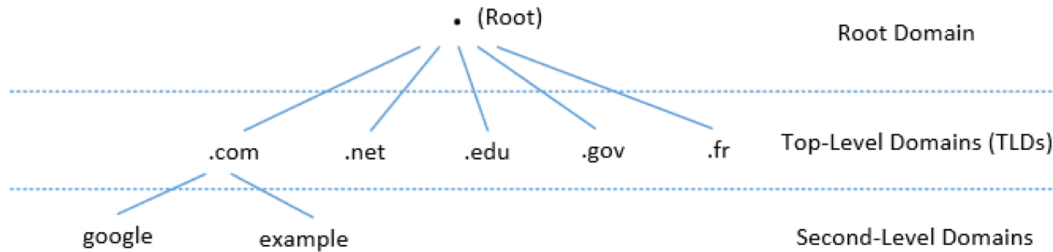
Outline

- How DNS works
- Spoofing Attacks on DNS
 - Local DNS cache poisoning attacks
 - Remote DNS cache poisoning attacks
 - Reply forgery attacks
- Defense against DNS spoofing attacks
 - DNSSEC
 - TLS/SSL
- Denial of Services on DNS

Why DNS

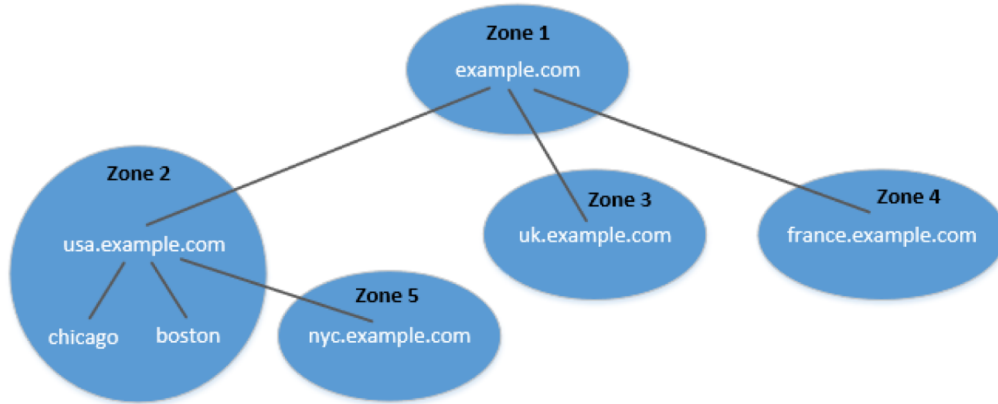
- Hosts are identified by IP addresses in TCP/IP
- IP addresses are hard for human to remember
 - What is google's IP address when doing google search?
- Assign easy-to-remember name
 - E.g., www.google.com
 - Called domain name
- DNS maps domain name to IP address

DNS Domain Hierarchy



- Below ROOT, we have Top-Level Domain (TLD). Ex: In www.example.com, the TLD is .com.
- The next level of domain hierarchy is second-level domain which are usually assigned to specific entities such as companies, schools etc
- Domain namespace is organized in a hierarchical tree-like structure.
- Each path from root is called a domain, or subdomain.
- The root of the domain is called ROOT, denoted as ' . '.

DNS Zone



- DNS is organized according to zones.
 - A zone groups contiguous domains and subdomains on the domain tree and assign management authority to an entity.
-
- The tree structure depicts subdomains within example.com domain.
 - In this case, there are multiple DNS zones one for each country. The zone keeps records of who the authority is for each of its subdomains.
 - The zone for example.com contains only the DNS records for the hostnames that do not belong to any subdomain like mail.example.com

Authoritative Name Servers

- Each DNS zone has at least one authoritative nameserver that publishes information about the zone.
- It provides the original and definitive answers to DNS queries.

DNS ROOT Servers

- The root zone is called ROOT.
- There are 13 authoritative nameservers (DNS root servers) for this zone.
- They provide the nameserver information about all TLDs
 - <https://www.internic.net/domain/root.zone>
- They are the starting point of DNS queries.

13 DNS Root Servers

List of Root Servers

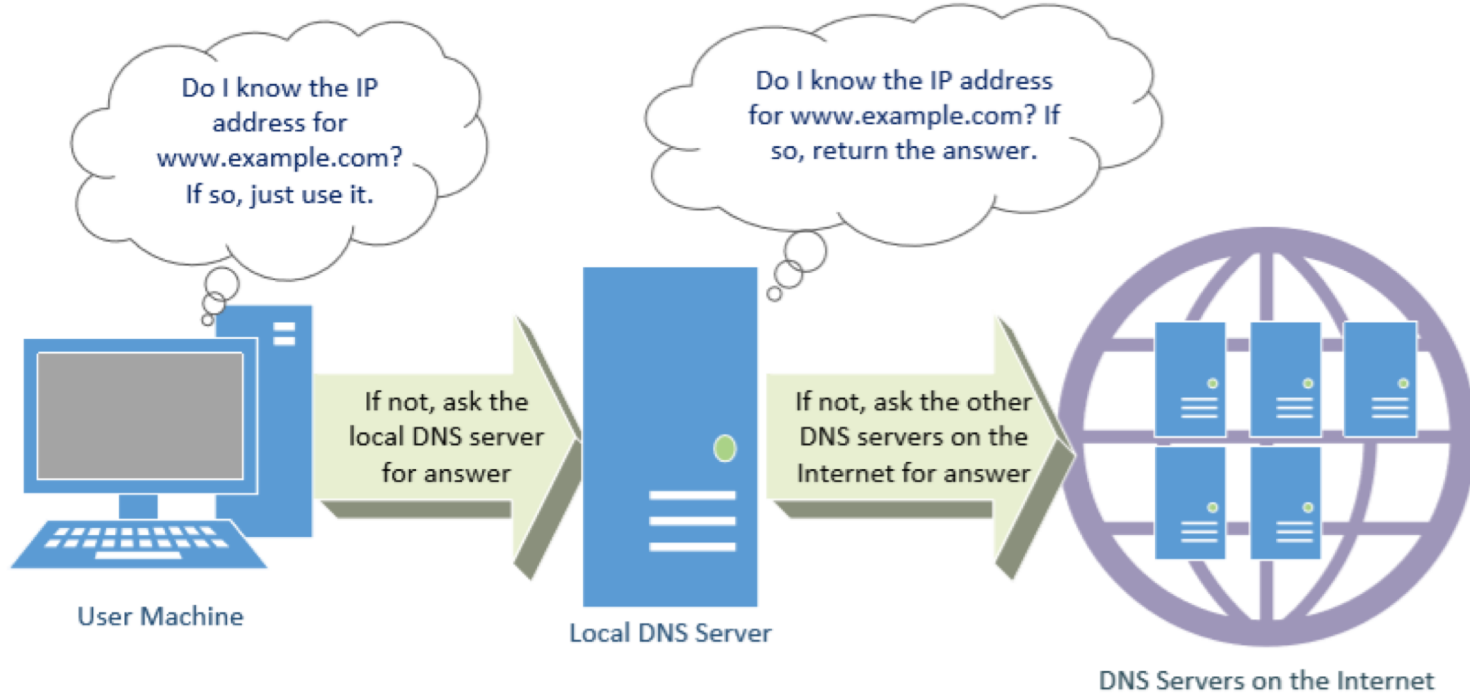
HOSTNAME	IP ADDRESSES	MANAGER
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

They are the most critical infrastructure on the Internet.

Top Level Domain (TLD)

- Infrastructure TLD: .arpa
- Generic TLD (gTLD): .com, .net,
- Sponsored TLD (sTLD): These domains are proposed and sponsored by private agencies or organizations that establish and enforce rules restricting the eligibility to use the TLD: .edu, .gov, .mil, .travel, .jobs
- Country Code TLD (ccTLD): .au (Australia), .cn (China), .fr (France)
- Reserved TLD: .example, .test, .localhost, .invalid

DNS Query Process



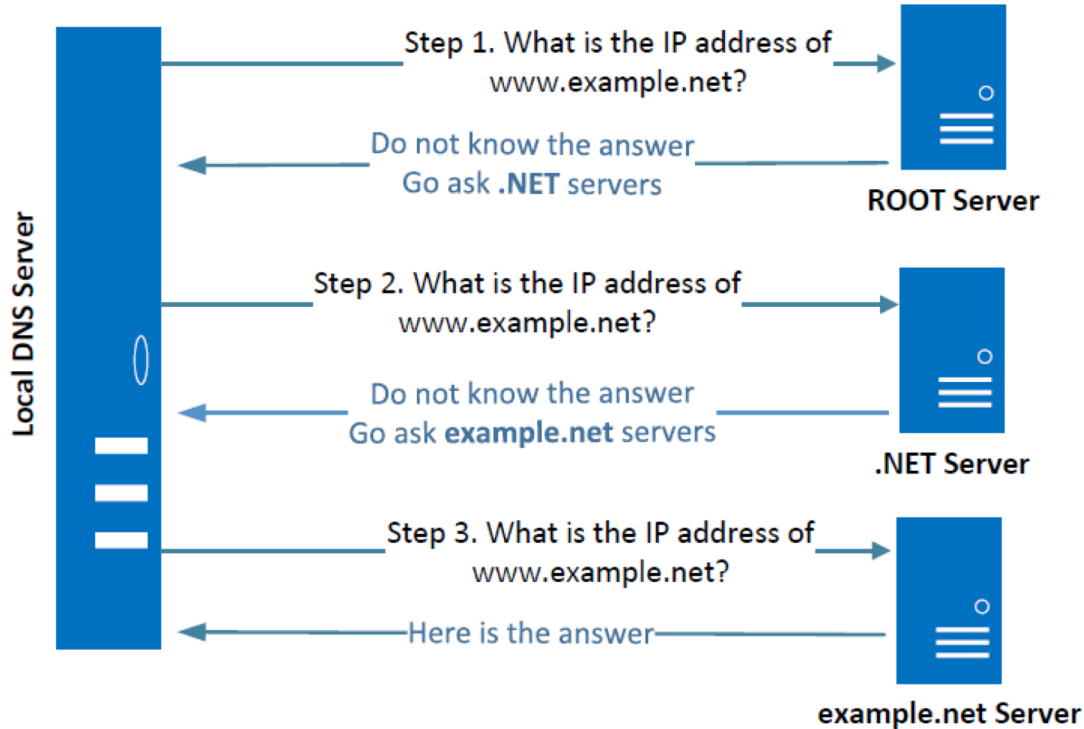
Local DNS Files

- `/etc/host`: stores IP addresses for some hostnames. Before machine contacts the local DNS servers, it first looks into this file for the IP address.

```
127.0.0.1    localhost
127.0.0.1    www.CSRFLabAttacker.com
127.0.0.1    www.CSRFLabElgg.com
127.0.0.1    www.XSSLabElgg.com
```

- `/etc/resolv.conf`: provide information about the IP address of the local DNS server.

Local DNS Server and Iterative Query Process



- The iterative process starts from the ROOT Server. If it doesn't know the IP address, it sends back the IP address of the nameservers of the next level server (.NET server) and then the last level server (example.net) which provides the answer.

Resource Records

- Implements zone information
- (Name, TTL, Class, Type, Value)
 - Name: domain
 - TTL: How long should the record be cached.
 - Value: DNS server domain name or IP address
 - Class: Internet (IN). Allow an entity to redefine record
 - Type: define how to interpret Value. A: Value is IP address. NS: Value is DNS server domain name.

DNS Response

There are 4 types of sections in a DNS response :

- Question section : Describes a question to a nameserver
- Answer section : Records that answer the question
- Authority section : Records that point toward authoritative nameservers
- Additional section : Records that are related to the query.

Emulating Local DNS Server (Step 1: Ask ROOT)

Directly send the query to this server.

```
seed@ubuntu:~$ dig @a.root-servers.net www.example.net
```

(Only a portion of the reply is shown here)

;; QUESTION SECTION:

www.example.net. IN A

;; AUTHORITY SECTION:

net. 172800 IN NS m.gtld-servers.net.

net. 172800 IN NS l.gtld-servers.net.

net. 172800 IN NS k.gtld-servers.net.

;; ADDITIONAL SECTION:

m.gtld-servers.net. 172800 IN A 192.55.83.30

l.gtld-servers.net. 172800 IN A 192.41.162.30

k.gtld-servers.net. 172800 IN A 192.52.178.30

No answer
(the root does
not know the
answer)

Go ask them!

Steps 2-3: Ask .net & example.net servers

```
seed@ubuntu:~$ dig @m.gtld-servers.net www.example.net
```

```
;; QUESTION SECTION:
```

```
;www.example.net.          IN      A
```

```
;; AUTHORITY SECTION:
```

```
example.net.      172800  IN      NS      a.iana-servers.net.
```

```
example.net.      172800  IN      NS      b.iana-servers.net.
```

```
;; ADDITIONAL SECTION:
```

```
a.iana-servers.net. 172800  IN      A      199.43.132.53
```

```
b.iana-servers.net. 172800  IN      A      199.43.133.53
```

← Ask a .net nameservers.

← Go ask them!

```
seed@ubuntu:$ dig @a.iana-servers.net www.example.net
```

```
;; QUESTION SECTION:
```

```
;www.example.net.          IN      A
```

```
;; ANSWER SECTION:
```

```
www.example.net.      86400   IN      A      93.184.216.34
```

← Ask an example.net nameservers.

← Finally got the answer

DNS cache

- When the local DNS server gets information from other DNS servers, it caches the information.
- Each piece of information in the cache has a time-to-live value, so it will be eventually time out and removed from the cache.

DNS Attacks

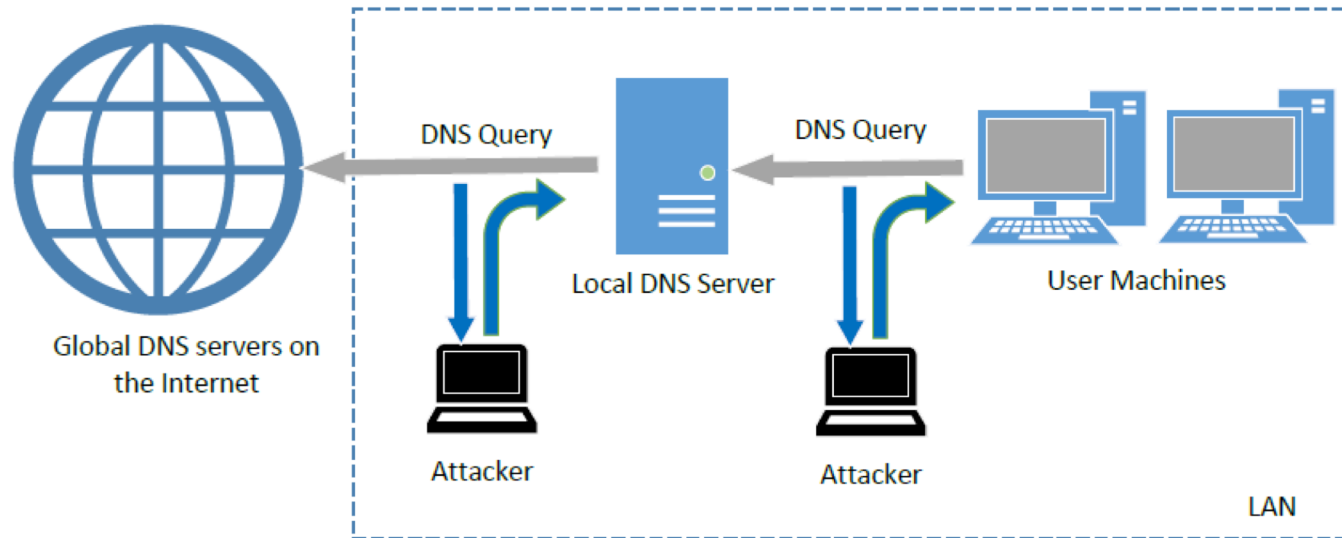
- **Spoofing Attacks:**

- Primary goal: provide a fraudulent IP address to victims, tricking them to communicate with a machine that is different from their intention.
- Example: If a user's intention is to visit a bank's web site to do online banking, but the IP address obtained through the DNS process is attacker's machine, the user machine will communicate to the attacker's web server.

- **Denial-of-Service Attacks (DoS):** When the local DNS servers and the authoritative nameservers do not respond to the DNS queries, the machines cannot retrieve IP addresses which essentially cuts down the communication

Local DNS Cache Poisoning Attack

Spoofing DNS Replies (from LAN)



Remote DNS Cache Poisoning Attack

Challenges

Challenges: For remote attackers who are not on the same network as the local DNS server, spoofing replies is much more difficult, because they need to guess two random numbers used by the query packet:

- Source port number (16-bit number)
- Transaction ID (16-bit number)

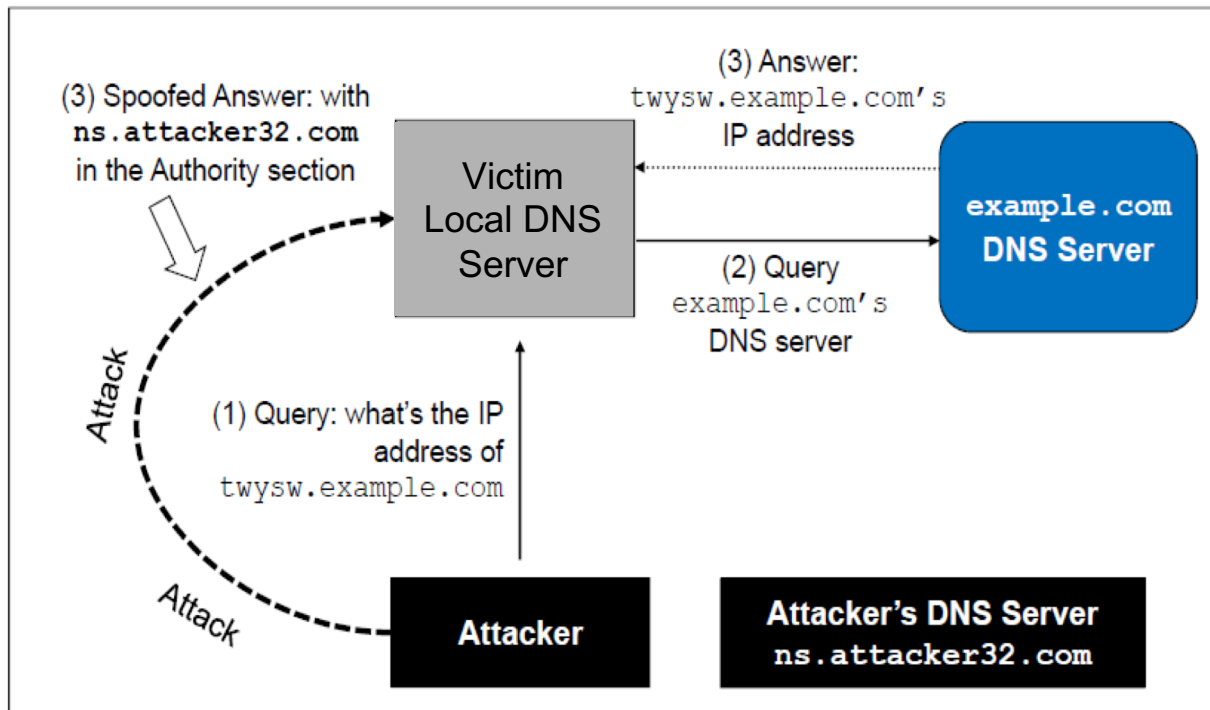
Cache effect: If one attempt fails, the actual reply will be cached by local DNS server; attacker need to wait for the cache to timeout for the next attempt.

The Kaminsky Attack

How can we keep forging replies without worrying about the cache effect?

Kaminsky's Idea:

- Ask a different question every time, so caching the answer does not matter, and the local DNS server will send out a new query each time.
- Provide forged answer in the Authority section



The Kaminsky Attack: A Sample Spoofed Answer

This random name will change for each attack attempt



```
;; QUESTION SECTION:
;twysw.example.com.      IN      A
```

This answer does not matter



```
;; ANSWER SECTION:
twysw.example.com.      259200  IN      A      1.2.3.4
```

```
;; AUTHORITY SECTION:
example.com.            259200  IN      NS      ns.attacker32.com
```

NS ns.attacker32.com



This is what we want the local DNS server to cache



Tell the DNS server to use this one as the nameserver for the example.com domain

Attacks from Malicious DNS Server

Attacks from Malicious DNS Server

When a user visits a website, such as attacker32.com, a DNS query will eventually come to the authoritative nameserver of the attacker32.com domain. In addition to providing an IP address in the answer section of the response, DNS server can also provide information in the authority and additional sections. Attackers can use these sections to provide fraudulent information.


Fake Data in the Additional Section

```
;; QUESTION SECTION:
;www.example.net.          IN      A

;; ANSWER SECTION:
www.example.net.          259200  IN      A      192.168.0.101

;; ADDITIONAL SECTION:
www.gmail.com.            259200  IN      A      192.168.0.201
www.facebook.com.         259200  IN      A      192.168.0.202
```

Additional
information is
provided



They will be discarded: out of zone. They will cause security problems if not discarded.

Fake Data in the Authority Section

This one is
allowed

```
;; QUESTION SECTION:
;www.example.net.          IN      A

;; ANSWER SECTION:
www.example.net.          259200 IN      A      192.168.0.101

;; AUTHORITY SECTION:
example.net.              259200 IN      NS      ns.example.net.
facebook.com.            259200 IN      NS      ns.example.net.
```

This one is
out of zone,
and should
be discarded

Reply Forgery Attacks from Malicious DNS Servers

```
;; QUESTION SECTION:
;www.example.net.          IN      A

;; ANSWER SECTION:
www.example.net.          259200  IN      A      192.168.0.101

;; AUTHORITY SECTION:
example.net.              259200  IN      NS      www.facebook.com.

;; ADDITIONAL SECTION:
www.facebook.com.         259200  IN      A      192.168.0.201
```

This one
is allowed

This one is not allowed (out of zone). The local DNS server will get the IP address of this hostname by itself.

Protection Against DNS Cache Poisoning Attacks

DNSSEC

- DNSSEC is a set of extension to DNS, aiming to provide authentication and integrity checking on DNS data.
- With DNSSEC, all answers from DNSSEC protected zones are digitally signed.
- By checking the digital signatures, a DNS resolver is able to check if the information is authentic or not.
- DNS cache poisoning will be defeated by this mechanism as any forged replies will be detected because they will fail the signature checking.

Protection Using TLS/SSL

Transport Layer Security (TLS/SSL) protocol provides a solution against the cache poisoning attacks.

- After getting the IP address for a domain name (www.example.net) using DNS protocol, a computer will ask the owner (server) of the IP address to prove that it is indeed www.example.net.
- The server has to present a public-key certificate signed by a trusted entity and demonstrates that it knows the corresponding private key associated with www.example.net (i.e., it is the owner of the certificate).
- HTTPS is built on top of TLS/SSL. It defeats DNS cache poisoning attacks.

Denial of Services Attacks on DNS via Sending Massive Queries to DNS Servers

Denial of Service Attacks on Root Servers

Attacks on the Root and TLD Servers :

Root nameservers: If the attackers can bring down the servers of the root zone, they can bring down the entire Internet. However, attack root servers is difficult:

- The root nameservers are highly distributed. There are 13 (A,B....M) root nameservers (server farm) consisting of a large number of redundant computers to provide reliable services.
- As the nameservers for the TLDs are usually cached in the local DNS servers, the root servers need not be queried till the cache expires (48 hrs). Attacks on the root servers must last long to see a significant effect.

Attacks on Nameservers of a Particular Domain

UltraDNS: DNS provider for many major e-commerce companies such as Amazon, Walmart, Expedia. In 2004, DOS against this provider was launched which suffered an outage for an hour.

DDoS attack hobbles sites, including Amazon

By **Tom Krazit**, CNET

December 24, 2009 -- Updated 1900 GMT (0300 HKT)



Amazon was one of the Internet's larger companies hit by a DDoS attack Wednesday evening.

(CNET) -- An attack directed at the DNS provider for some of the Internet's larger e-commerce companies -- including Amazon, Wal-Mart, and Expedia -- took several Internet shopping sites offline Wednesday evening, two days before Christmas.

Neustar, the company that provides DNS services under the UltraDNS brand name, confirmed an attack took place Wednesday afternoon, taking out sites or rendering them extremely sluggish for about an hour. A

Attacks on Nameservers of a Particular Domain

Dyn network : In 2016, multiple DDoS attacks were launched against a major DNS service provider for companies like CNN, BBC, HBO, PayPal etc. The attacks are believed to have been launched through botnet consisting of different IoT devices like IP cameras, baby monitors etc. It caused major Internet services unavailable .



Our DNS provider is under a DDos attack.
Causing connectivity issues for our webpage.
Filtering of Inbox emails has not been affected.



1:17 PM - 21 Oct 2016



PayPal @PayPal · 21 oct

PayPal is experiencing brief interruptions in service due to a widespread issue with our DNS provider. We're sorry for the inconvenience.

Gizmodo @Gizmodo · Oct 22

Yesterday's brutal **DDoS** attack is the beginning of a bleak future
gizmo.do/POR2Sne



Summary

- How DNS works
- Spoofing Attacks on DNS
 - Local DNS cache poisoning attacks
 - Remote DNS cache poisoning attacks
 - Reply forgery attacks
- Defense against DNS spoofing attacks
 - DNSSEC
 - TLS/SSL
- Denial of Services on DNS