DNS Spoofing / Poisoning and Relevant Defences

(CSE 4482: Computer Security Management)

Benjamin Klein & Prakanth Thangeswaran

York University
Department of Computer Science and Engineering

December 7, 2010

Outline

Outline

Domain Name System

Whenever we communicate using IP, we need IP addresses to address the destination.

Do you know the IP of the YorkU webserver?

It's 130.63.236.137 ... easy to remember, isn't it?

- designed by Paul Mockapetris in 1983
- specified in RFC[1] 1034 and 1035
- translates FQDN [2] into IP addresses

[1] Request for Comments

[2] Fully Qualified Domain Name, e.g. www.yorku.ca

Domain Name System

Whenever we communicate using IP, we need IP addresses to address the destination.

Do you know the IP of the YorkU webserver?

It's 130.63.236.137 . . . easy to remember, isn't it?

- designed by Paul Mockapetris in 1983
- specified in RFC[1] 1034 and 1035
- translates FQDN [2] into IP addresses

[1] Request for Comments

[2] Fully Qualified Domain Name, e.g. www.yorku.ca

Domain Name System

Whenever we communicate using IP, we need IP addresses to address the destination.

Do you know the IP of the YorkU webserver?

It's 130.63.236.137 ... easy to remember, isn't it?

- designed by Paul Mockapetris in 1983
- specified in RFC[1] 1034 and 1035
- translates FQDN [2] into IP addresses

[1] Request for Comments

[2] Fully Qualified Domain Name, e.g. www.yorku.ca

Domain Name System

Whenever we communicate using IP, we need IP addresses to address the destination.

Do you know the IP of the YorkU webserver?

It's 130.63.236.137 ... easy to remember, isn't it?

- designed by Paul Mockapetris in 1983
- specified in RFC[1] 1034 and 1035
- translates FQDN [2] into IP addresses

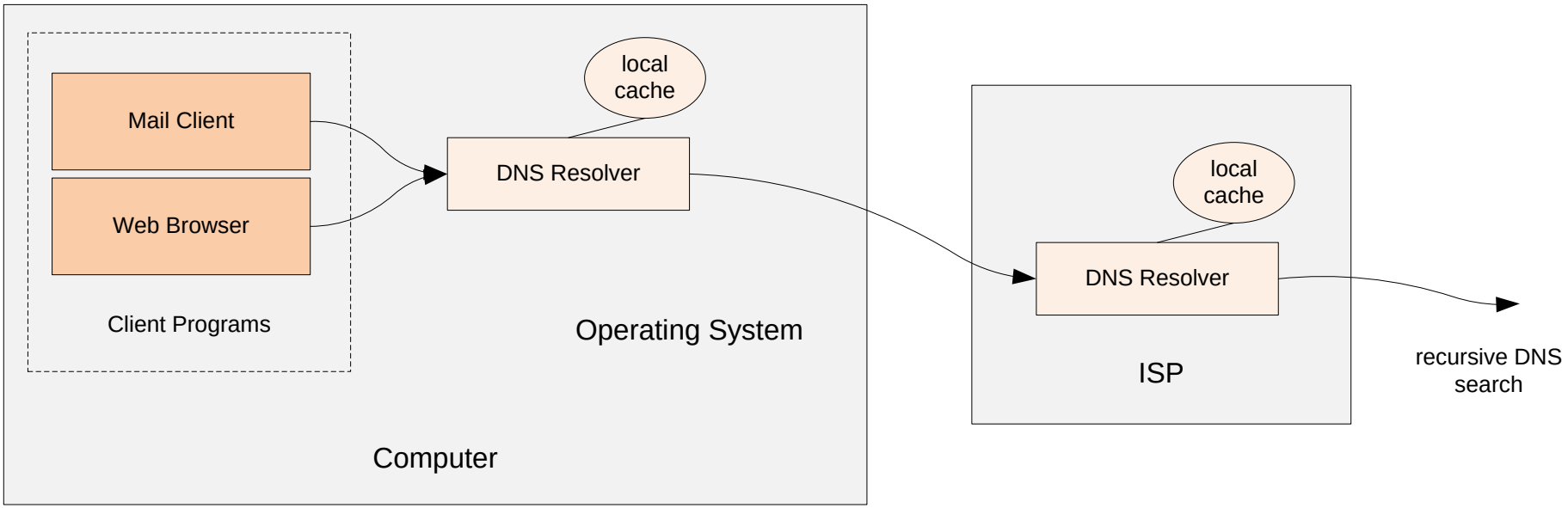
[1] Request for Comments

[2] Fully Qualified Domain Name, e.g. www.yorku.ca

DNS Resolver

Example

You type `http://www.thestar.com` to visit the Toronto Star



DNS Resource Records

- fundamental information unit in DNS
- different types of RR
  - A (IPv4 address)
  - MX (mail exchange server)
  - NS (hostname of authoritative name server)
  - ...

Example A-RR

```
www.yorku.ca.  3600 IN A 130.63.236.137
```

Outline

DNS Cache Poisoning

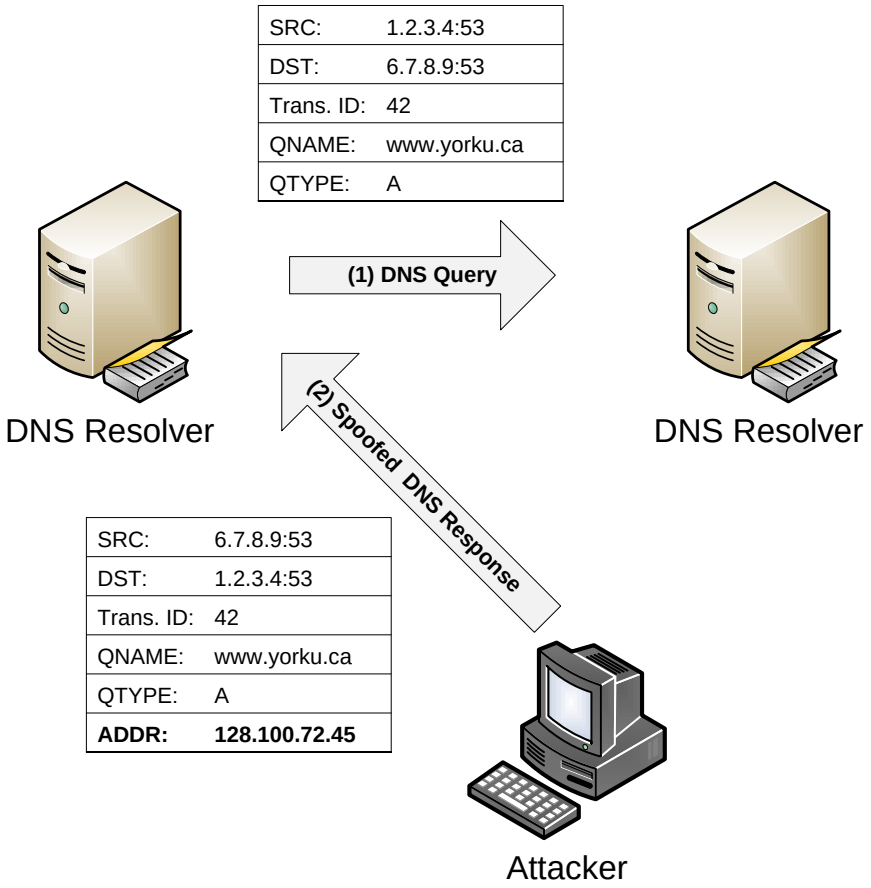
- DNS was **not** designed with security in mind
- classes of transactions: **usage** vs **administrative transactions**

usage transactions (obviously most present in DNS traffic)

- **Query**: A asks B for the IP of a particular FQDN
- **Response**: B gives A the requested IP

- **DNS Cache Poisoning:** An attacker replies to A with a faked IP (to divert traffic to another computer) and A stores it in its cache

Packet Interception



ID Guessing and Query Prediction

If we can't intercept traffic, we still can guess!

- UDP Port and Transaction ID are 16-bit fields each
- 2^{32} possible values $\rightarrow$ suitable for brute-force
- in most cases, the client UDP port can be predicted from previous traffic observations $\rightarrow$ 2^{16} values

- we also have to guess `QNAMEs`[3] and `QTYPEs`[4]

$\Rightarrow$ **attack is only successful if the resolver's behaviour is predictable**

[3] query domain name (e.g. www.yorku.ca)
[4] query type (A, MX, NS,...)

Outline

DNS Security Extension (DNSSEC)

- introduced 1999 in RFC 2535 (updated by RFC 4033 later)
- provides **data integrity and authentication**
- all replies in DNSSEC are digitally signed using public-key cryptography

- required no change to the DNS protocol beyond the addition of **new resource types**

DNSSEC Resource Records

- `RRSIG`: stores the signature
- `DNSKEY`: stores the public key that was used
- ...

References

RFC 1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

http://www.ietf.org/rfc/rfc1035.txt

RFC 4033: DNS Security Introduction and Requirements

http://www.ietf.org/rfc/rfc4033.txt

Kim Davies: 2008 DNS Cache Poisoning Vulnerability

http://www.iana.org/about/presentations/davies-cairo-vulnerability-081103.pdf

Q & A

Any questions left?

Benjamin Klein <bklein@yorku.ca>
Prakanth Thangeswaran <prakanth@yorku.ca>