Lecture 23 – DNS Security

University of Illinois

ECE 422/CS 461

Learning Objectives

- Understand the high-level workings of DNS
- Learn how name server can be polluted by spoofed DNS queries
- Evaluate defenses for DNS cache poisoning and learn how they avoid a full redesign of the existing DNS infrastructure

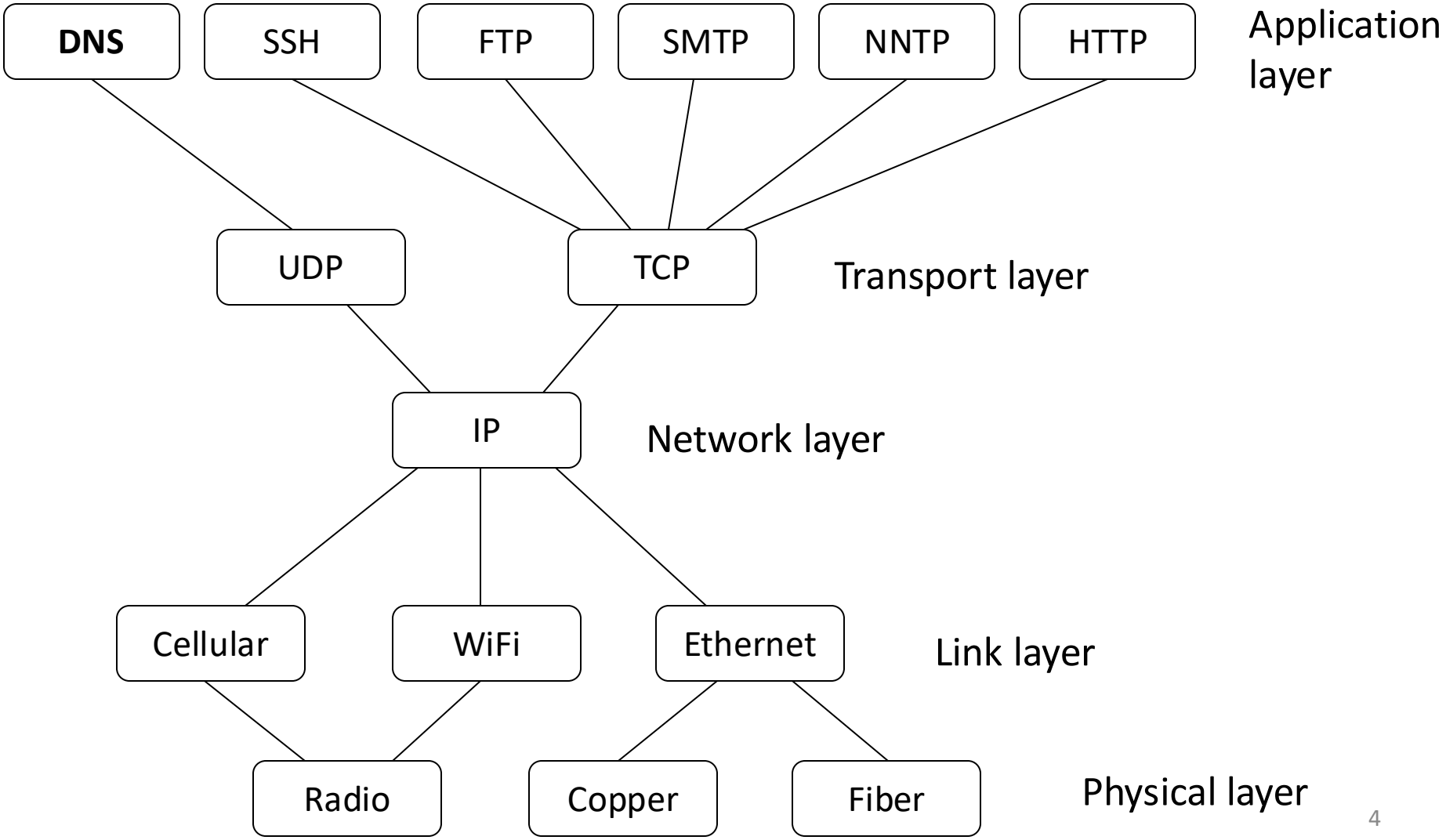
Domain Name System

- Applications and people usually refer to Internet host by *host name*

http:// ece.illinois.edu

http:// 130.126.151.27

Layering of protocols

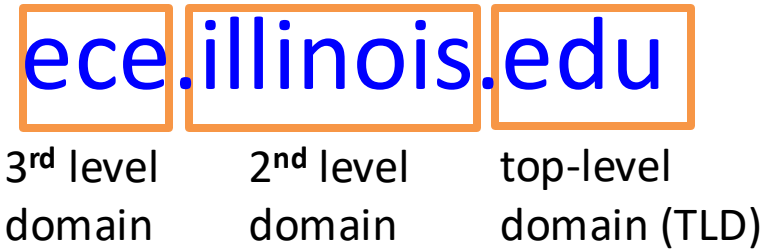


Domain Name System

- **Domain Name System (DNS)** is at once:
  - Administrative structure for controlling names
  - Global distributed database of names
  - Protocol for interacting with database

DNS Hierarchy

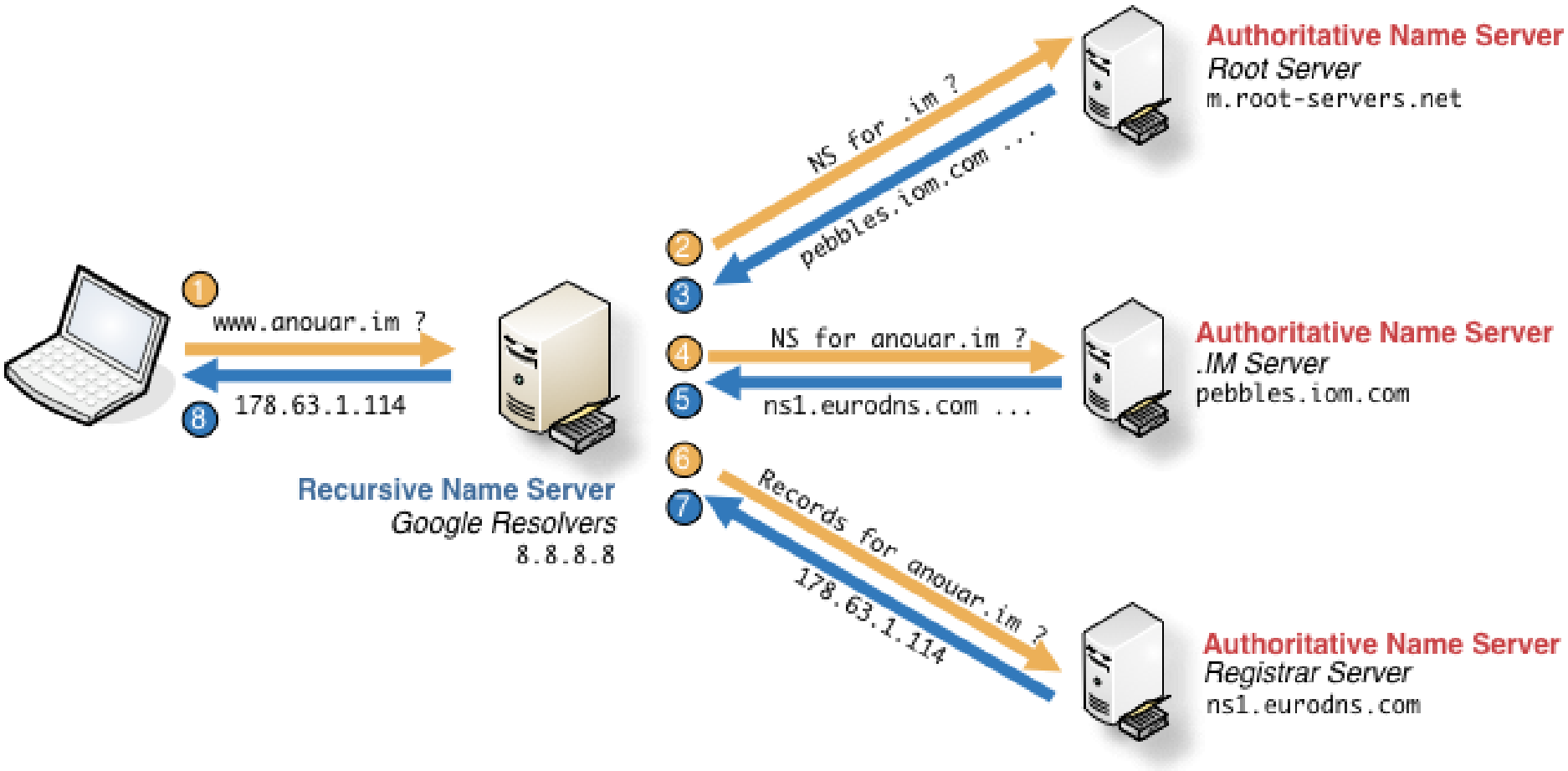
- Host names organized into hierarchy



DNS Hierarchy

- Each level allocates names to next level
- ICANN allocates top-level domains (TLD)
  - Country-code, two letters, e.g., `.us`
  - Generic, 3+ letters, e.g. `.com`
    - VeriSign controls `.com` and `.net`
- Individuals and organizations control subdomains
  - You can rent `yourname.com` from VeriSign
  - UIUC controls `.illinois.edu`

DNS Name Resolution



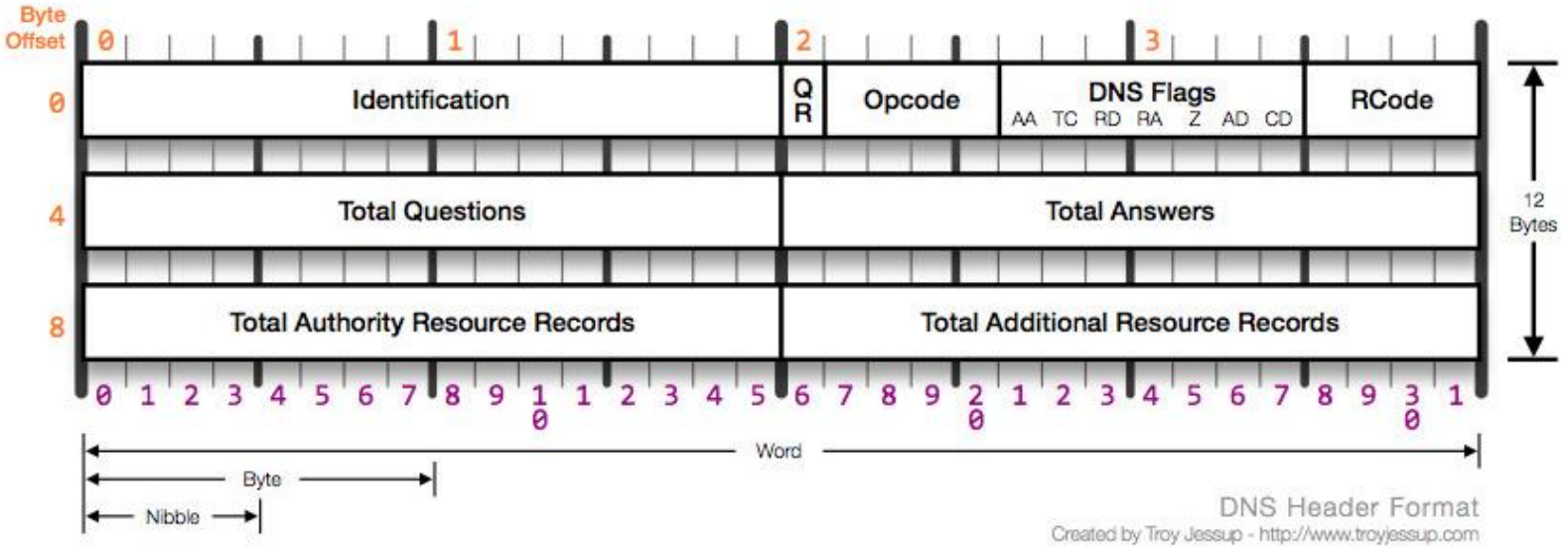
source: http://anouar.adlani.com/2011/12/useful-dig-command-to-troubleshot-your-domains.html

DNS Server Roles

- **Authoritative server:** provides authoritative information for a set of domains
- **Recursive resolver:** provides recursive resolution of a domain to return requested record to client
- Same protocol and packet format for both

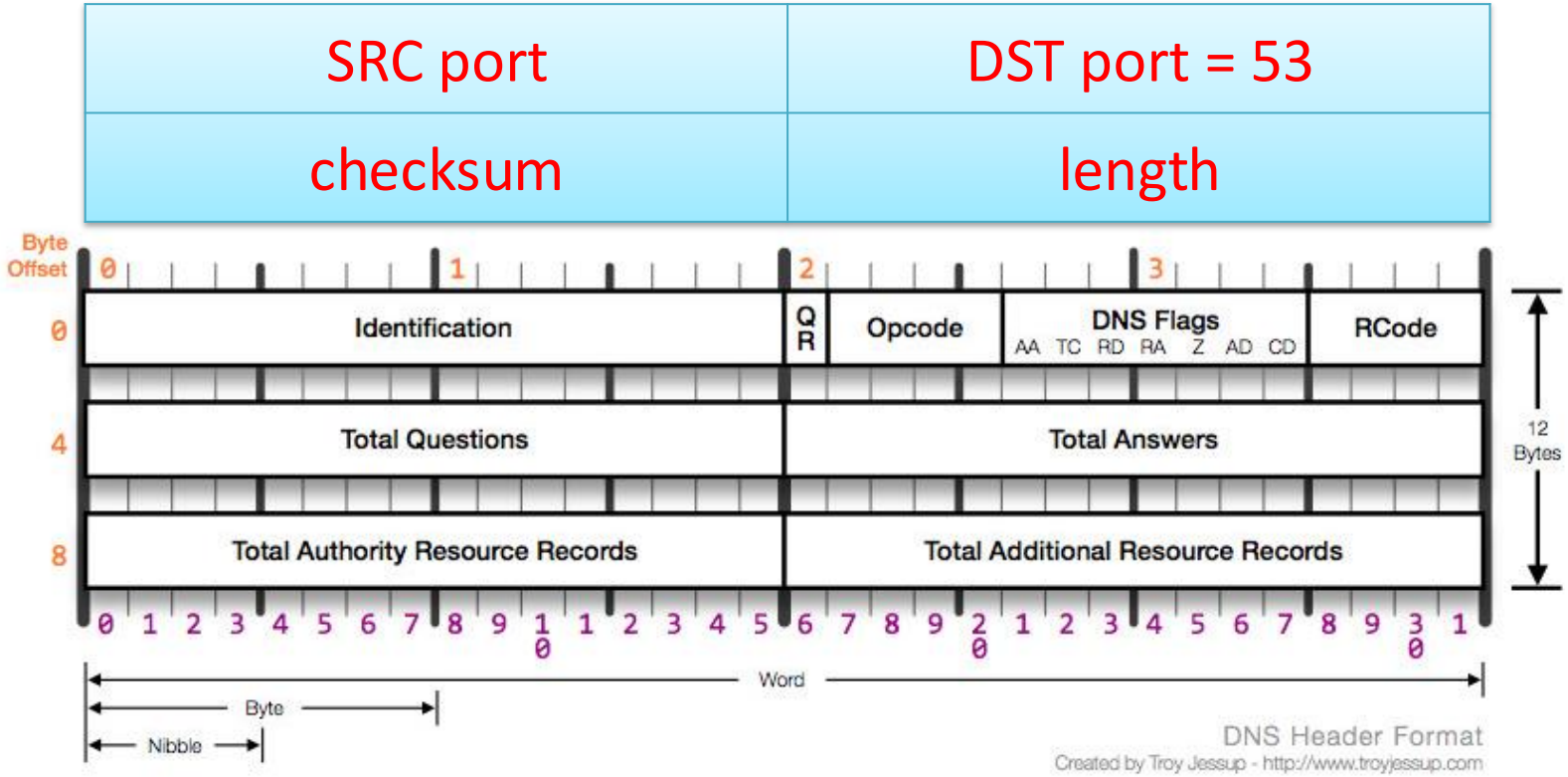
DNS Protocol

- DNS query contains a 16-bit query ID to match response to query
- No encryption or authentication



DNS Protocol

- Uses UDP as transport



DNS Protocol

- Four sections: *questions*, *answers*, *authority*, *additional records*

```
$ dig bob.ucsd.edu

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30439
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 6

;; QUESTION SECTION:
;bob.ucsd.edu.                IN   A

;; ANSWER SECTION:
bob.ucsd.edu.      3600 IN   A    132.239.80.176

;; AUTHORITY SECTION:
ucsd.edu.      3600 IN   NS   ns0.ucsd.edu.
ucsd.edu.      3600 IN   NS   ns1.ucsd.edu.
ucsd.edu.      3600 IN   NS   ns2.ucsd.edu.
```

DNS Protocol

- Four sections: *questions*, *answers*, *authority*, *additional records*

```
$ dig bob.ucsd.edu

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30439
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 6

;; QUESTION SECTION:
;bob.ucsd.edu.          IN   A

;; ANSWER SECTION:
bob.ucsd.edu.     3600 IN   A    132.239.80.176

;; AUTHORITY SECTION:
ucsd.edu.      3600 IN   NS   ns0.ucsd.edu.
ucsd.edu.      3600 IN   NS   ns1.ucsd.edu.
ucsd.edu.      3600 IN   NS   ns2.ucsd.edu.
```

TTL: Time to Live

Type

DNS Record Types

- Many types of DNS records, the commons ones are:
  - **A record:** IPv4 address for a host name
  - **AAAA record:** IPv6 address for a host name
  - **NS record:** Authority name server for a domain
  - **MX record:** SMTP (mail) server for domain
  - …

DNS Cache

- Recursive resolvers cache DNS records to avoid repeating queries
  - Cached entries can be evicted due to limited cache size
  - If not evicted, expire after TTL (Time to Live)

DNS Security Properties

	Passive	Off-Path	MitM
Availability	—		
Confidentiality		—	
Integrity	—	—	
Authenticity	—		

- What is the damage for losing each property?
  - Availability: as usual
  - Confidentiality: reveal browsing history
  - Integrity/authenticity: visit fake website

DNS Security Properties

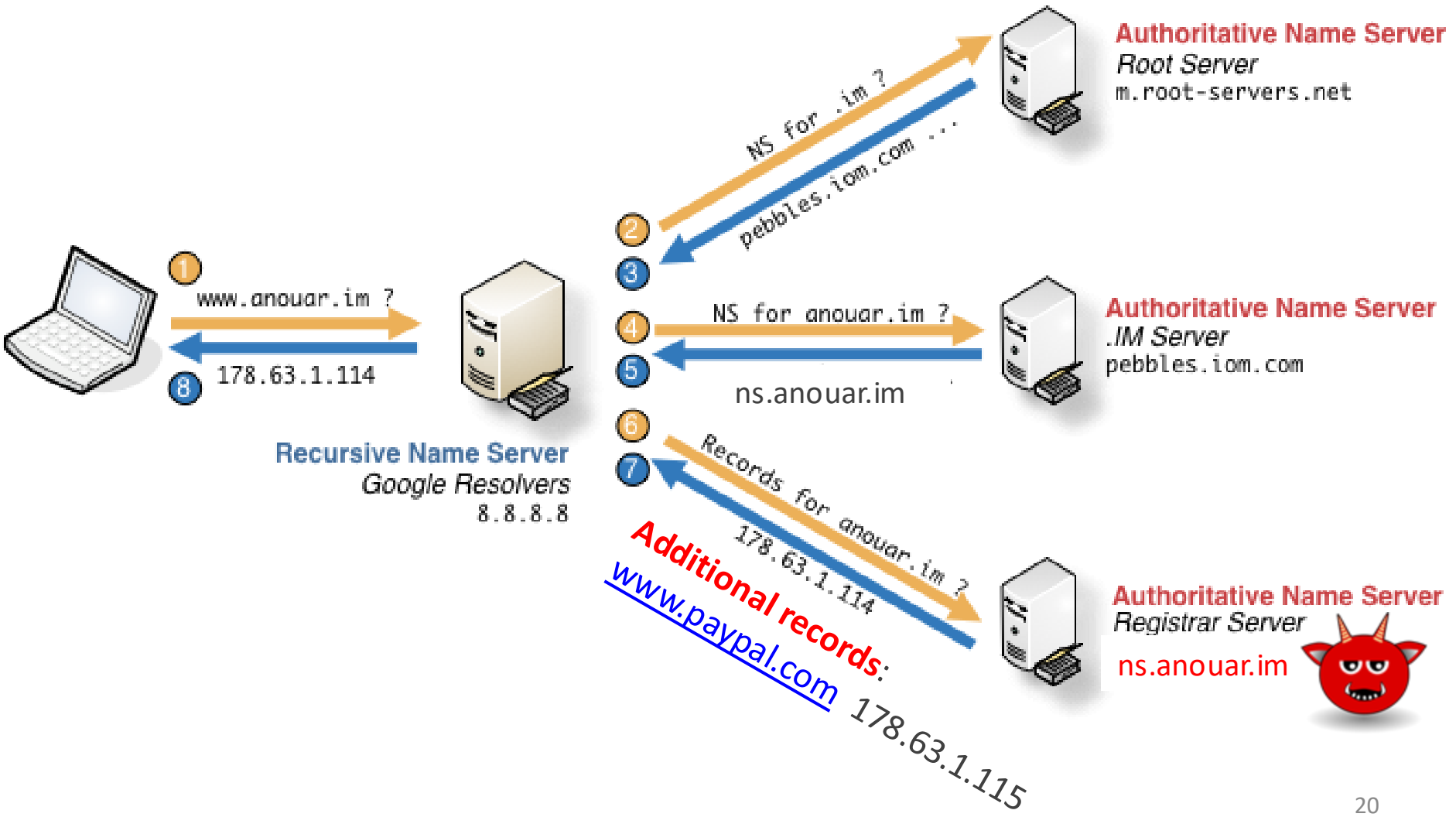
	Passive	Off-Path	MitM
Availability	–	✗	✗
Confidentiality	✗	–	✗
Integrity	–	–	✗
Authenticity	–	?	✗

- **MitM:** no protection
- **Passive:** no protection
- What about off-path attacker?

Off-Path Authenticity Attacks on DNS

- Scenario 1: an off-path attacker injects a fake reply after client issues a DNS query
  - Need to time the fake reply perfectly: too early → query not sent; too late → real response accepted
  - Recall attacker is off-path and does not see query

DNS Cache Poisoning



source: http://anouar.adlani.com/2011/12/useful-dig-command-to-troubleshot-your-domains.html

Off-Path Authenticity Attacks on DNS

- Scenario 1: an off-path attacker injects a fake reply after client issues a DNS query
  - Need to time the fake reply perfectly: too early → query not sent; too late → real response accepted
  - Recall attacker is off-path and does not see query

- Scenario 2: a malicious authoritative server injects fake records into resolver's cache
  - Off path for the injected records

DNS Cache Poisoning

- DNS query results include Additional Records section for anticipated next resolution steps
- Early servers accepted and cached all additional records provided in query response.

- Can we just stop using additional section?
  - Not with the current design. Need “glue” records for recursive dependency.

```
; <<>> DiG 9.6-ESV-R4-P3 <<>> @192.5.6.30 ucsd.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12781
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 4
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;ucsd.edu.                      IN      A

;; AUTHORITY SECTION:
ucsd.edu.               172800  IN      NS      ns1.ucsd.edu.
ucsd.edu.               172800  IN      NS      ns2.ucsd.edu.
ucsd.edu.               172800  IN      NS      ns0.ucsd.edu.

;; ADDITIONAL SECTION:
ns1.ucsd.edu.           172800  IN      A       128.54.16.2
ns2.ucsd.edu.           172800  IN      A       132.239.1.52
ns0.ucsd.edu.           172800  IN      A       132.239.1.51
ns0.ucsd.edu.           172800  IN      AAAA    2607:f720:100:100::231
```

edu authority

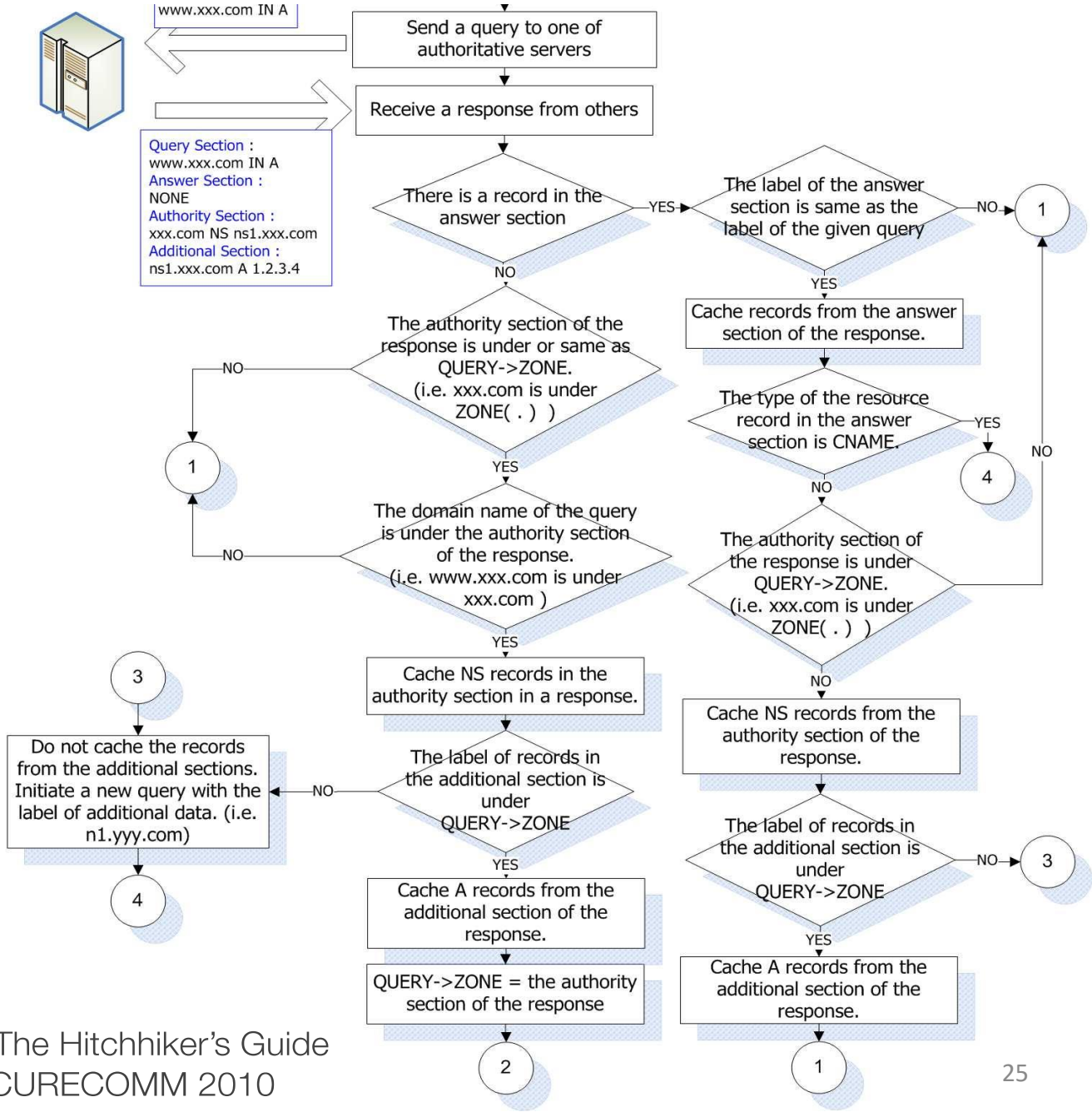
Names of ucsd.edu authoritative servers

Glue records for authoritative servers

Bailiwick Rules

- General meaning: the area of authority of a legal officer, e.g., a set of territories
  - Synonym: Jurisdiction
- Meaning in DNS: set of domains about which a server has direct or indirect authority to speak
  - Translation: records should be relevant

Bailiwick Checking Rule from BIND



source: Son and Shmatikov, “The Hitchhiker’s Guide to DNS Cache Poisoning” SECURECOMM 2010

Off-Path Authenticity Attacks on DNS

- Scenario 1: an off-path attacker injects a fake reply after client issues a DNS query
  - Need to time the fake reply perfectly: too early → query not sent; too late → real response accepted
  - Recall attacker is off-path and does not see query

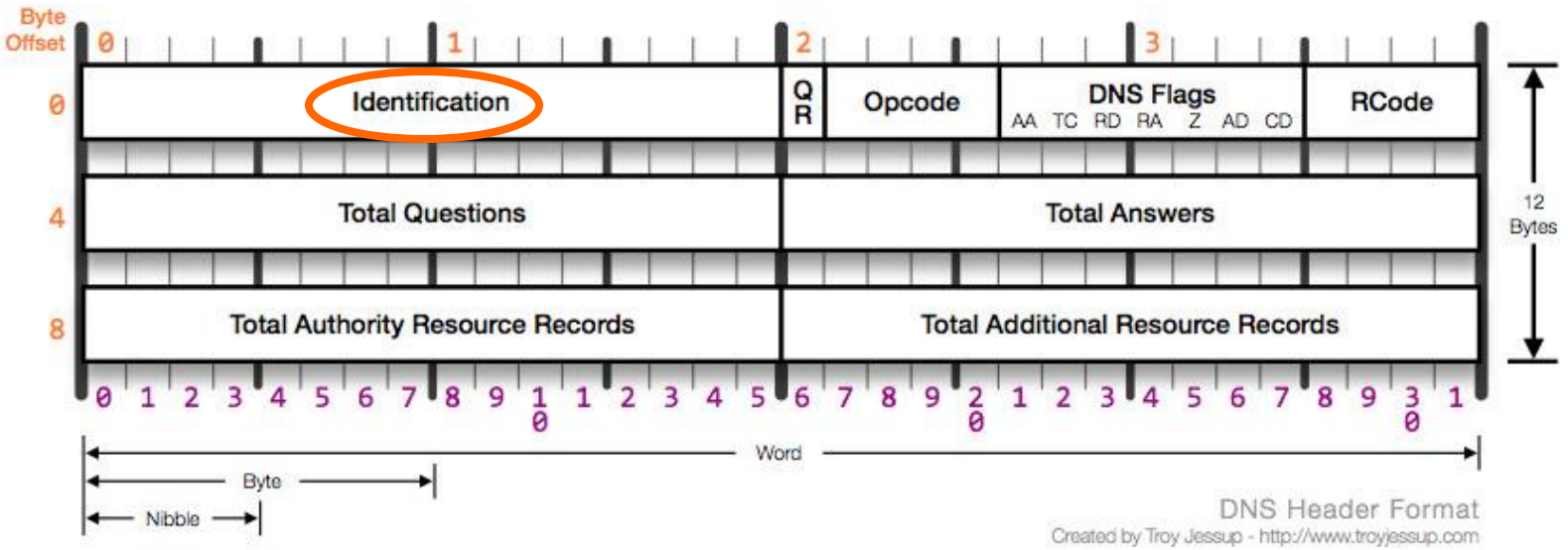
- Scenario 2: a malicious authoritative server injects fake records into resolver's cache
  - Off path for the injected records

Timing the Fake Reply

- Trick user to visit attacker's website containing <img src="http"//www.paypal.com/xyz.jpg">
- User issues DNS query for www.paypal.com immediately after visiting attacker's website
- Inject fake DNS reply for www.paypal.com

DNS Spoofing

- How likely will this attack succeed?
  - 2^{-16} if the 16-bit query ID is generated randomly
  - Originally, an incrementing query ID is used, easy to guess



DNS Spoofing

- How likely will this attack succeed?
  - 2^{-16} if the 16-bit query ID is generated randomly
- Usually not a safe threshold, **but** the resolver will cache a reply until TTL (Time To Live)
  - In other words, the attack is throttled by TTL!

- DNS spoofing thought to be mitigated

Kaminsky's Attack

- Bypasses TTL throttling with parallel attempts
- Trick user to visit attacker's website containing
  <img src="http"//aaa.paypal.com/xyz.jpg">
  <img src="http"//aab.paypal.com/xyz.jpg">
  <img src="http"//aac.paypal.com/xyz.jpg">
  ……
  <img src="http"//zzz.paypal.com/xyz.jpg">
  - Additional records for www.paypal.com are considered "relevant" to query for aaa.paypal.com by the Bailiwick rule

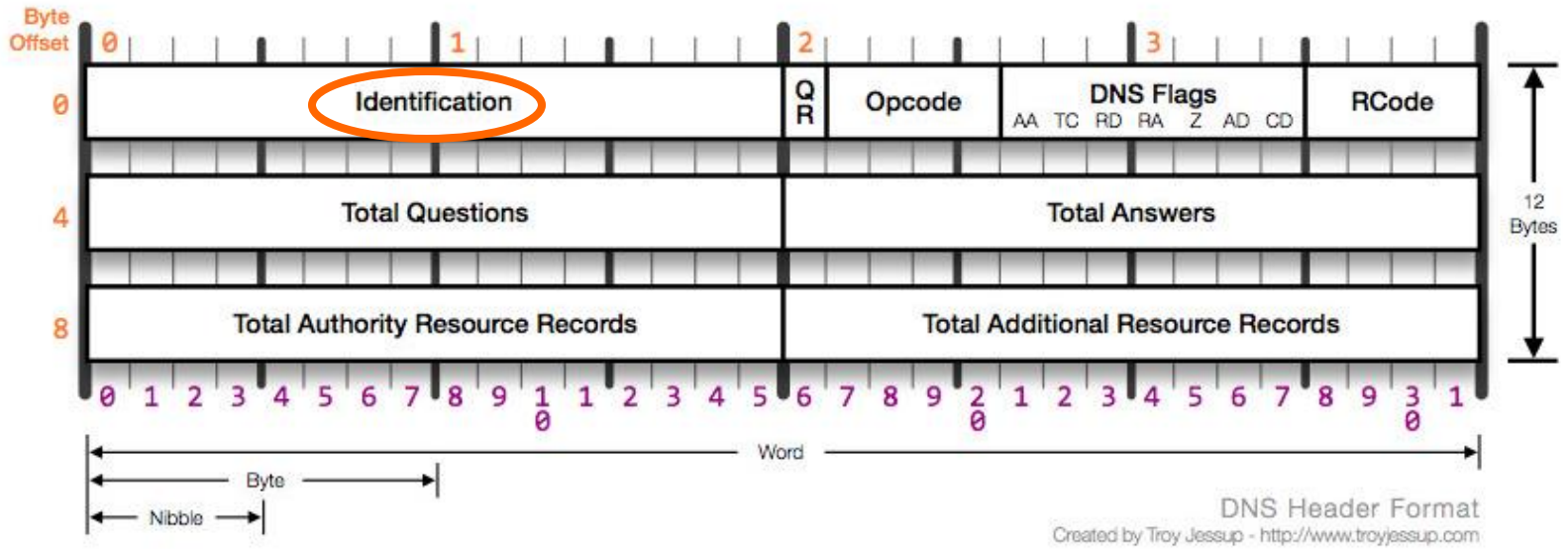
Kaminsky's Attack

- If attacker triggers *N* queries and sends *N* spoofed replies, chance of success = $N \times 2^{-16}$

- Can immediately repeat attack, not throttled by TTL!

Defense against Kaminsky's Attack

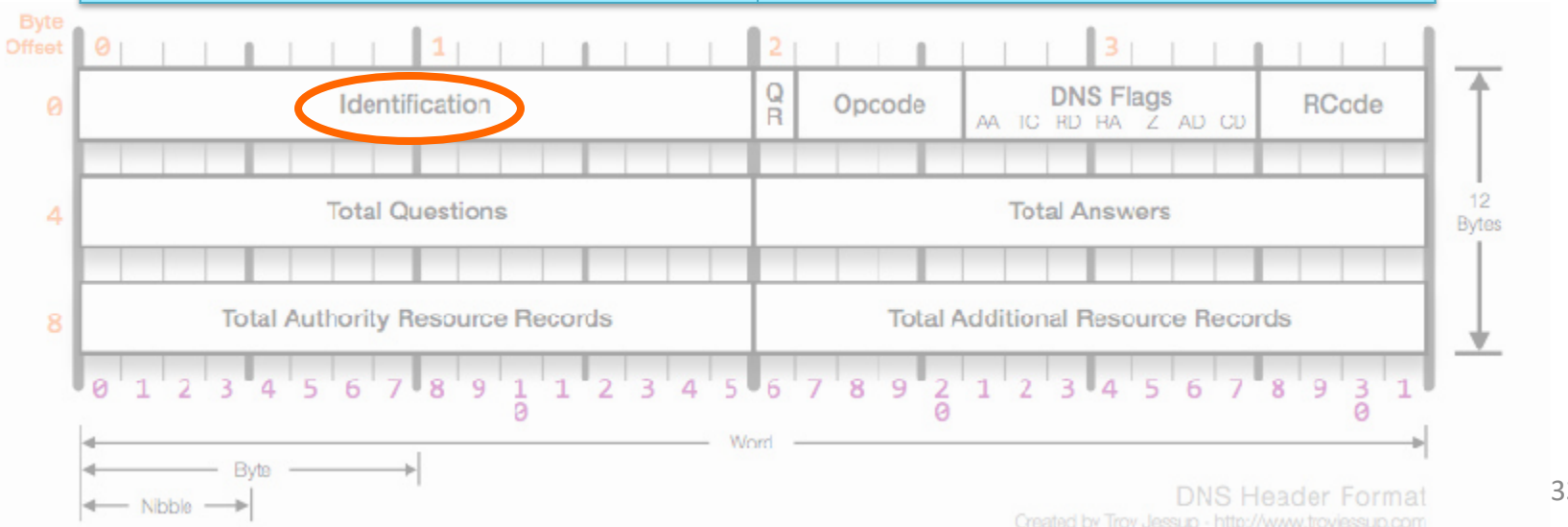
- Add more randomness to make guessing harder
  - While staying compatible with current DNS design



Defense against Kaminsky's Attack

- Add more randomness to make guessing harder
- Randomize UDP source port (16-bit)

SRC port = random	DST port = 53
checksum	length



Defense against Kaminsky's Attack

- Add more randomness to make guessing harder
- Randomize UDP source port (16-bit)
- Randomize capitalization in domain name
  - aaa.paypal.com → aAA.PaYpAL.cOm
  - Called 0x20 encoding, adds additional entropy

Defense against Kaminsky's Attack

- The attacker has to guess
  - Query ID (16-bit)
  - UDP source port (16-bit)
  - Capitalization in query (12-bit for aaa.paypal.com)
- Chance of success: $N \times 2^{-44}$
- Kaminsky's attack needs very large N

DNS Security Properties

	Passive	Off-Path	MitM
Availability	–	✗	✗
Confidentiality	✗	–	✗
Integrity	–	–	✗
Authenticity	–	✓	✗

- With these defenses, DNS enjoys reasonable authenticity against off-path attackers
- Can we achieve better security against MitM?

DNSSEC

- Digitally sign DNS records
  - As opposed to signing DNS replies
    - (Why? What's the difference?)
  - Need root of trust and certificates
- First proposed in 1997, current version 2005, adoption rate today not great (in contention)
- Slow adoption partly because TLS provides reasonable security even if DNS is broken

DNSSEC Security Properties

	Passive	Off-Path	MitM
Availability	–	✗	✗
Confidentiality	✗	–	✗
Integrity	–	–	✓
Authenticity	–	✓	✓

- Assumptions: crypto + public verification keys
- Why not try to protect confidentiality as well?