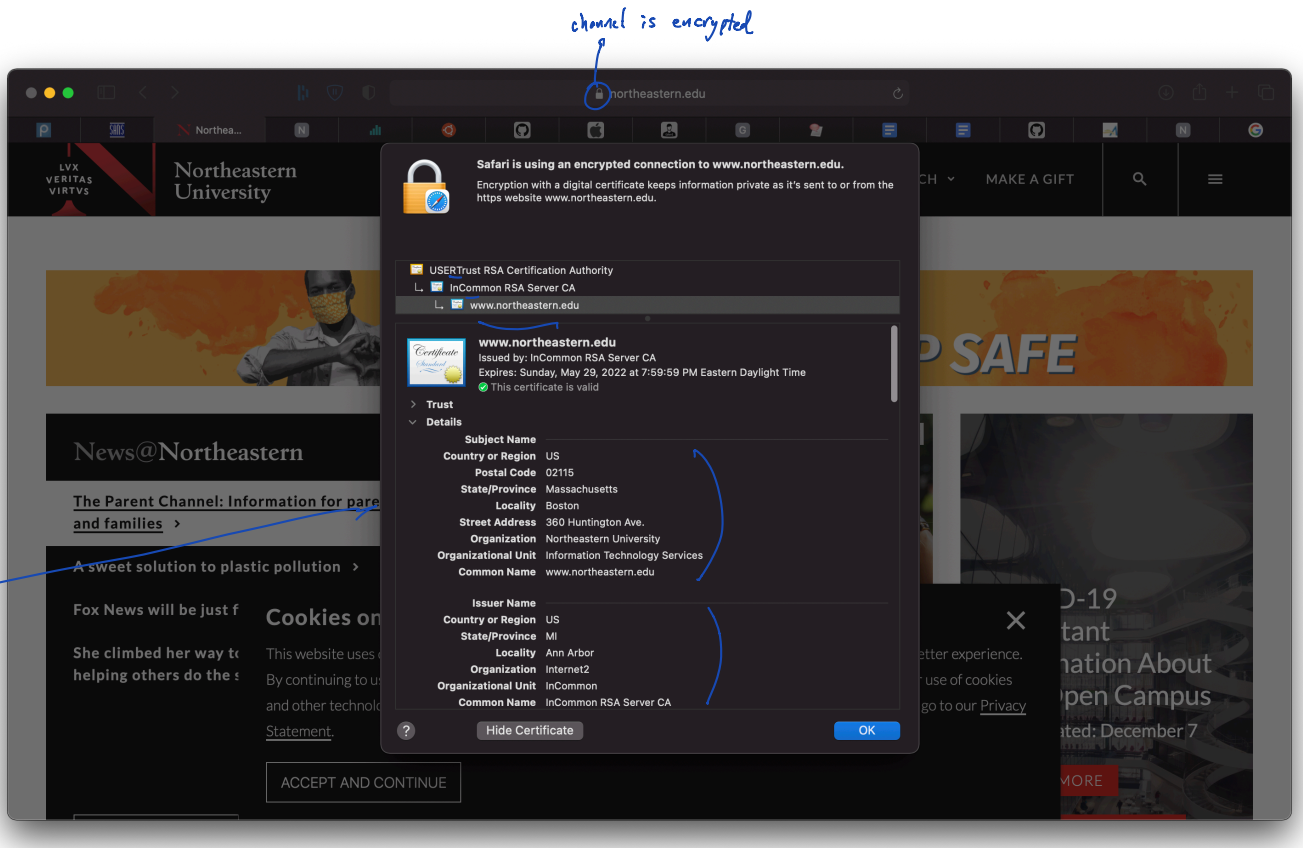
2550 Intro to cybersecurity

L26: Networking

abhi shelat

https

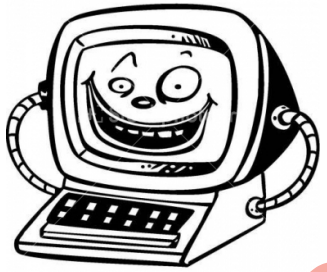
TLS



why do we need this info in certs??

Goal of https: setup an encrypted channel

TLS



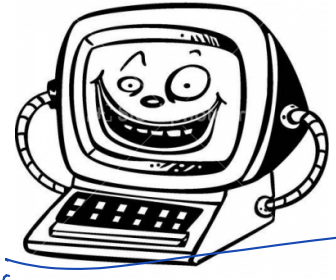
encrypted channel
(symmetric key for speed)

browser

Tool to use:

uses public key encryption to exchange server a secret key which can be used for symmetric encryption.

Goal of https: setup an encrypted channel



Alice

problem: how do I know Bob's public key to begin with??

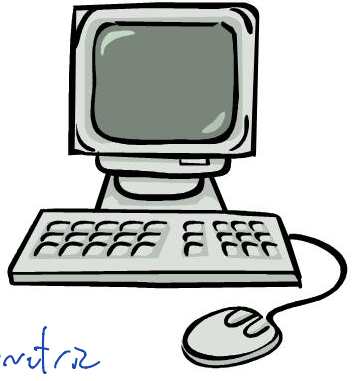
"Get / http/1.0"

$Enc(PK_{bob}, msg)$

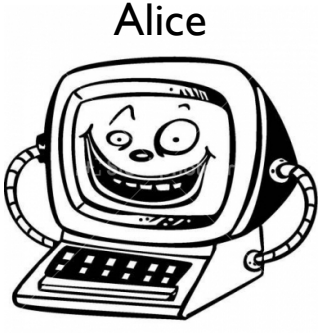
also be a shared secret key to use for symmetric encryption

PK_{bob}

bob.com



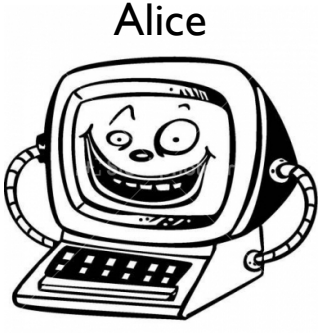
Goal of https: setup an encrypted channel



$Enc(PK_{bob}, msg)$

But what if Alice doesn't know PKbob yet?
Say it is the first time Alice is connecting to bob.com

Goal of https: setup an encrypted channel



"Hello. Send me your key?" →

← PK_{bob}

$Enc(PK_{bob}, \text{"GET / http/1.0"})$ →

PK_{bob}

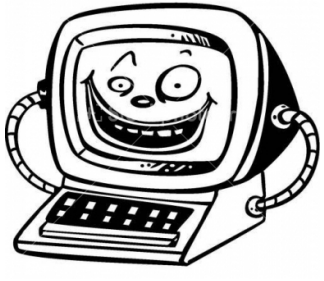
bob.com

So Alice can ask for Bob's key first.

Basic TLS flow (Totally broken!)

e.g. includes Bob's pk.

Alice



Alice switches to the negotiated cipher

secret key

<ClientHello>

optional

<ServerHello>, [Cert],[ServerKeyExch], [CertReq], <ServerHelloDone>

[Cert],<ClientKeyExchange>,[CertVerify]

↳ Enc(pk.bob, rand secret key)

<Finished>

<Finished>

PK_{bob}

bob.com

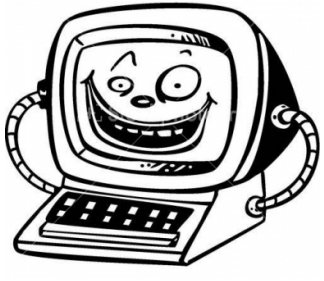
Bob switches to the negotiated cipher

Basic TLS flow

But there is a problem here.

How does Alice know she is communicating with Bob??

Alice



Alice switches to the negotiated cipher

<ClientHello>

<ServerHello>, [Cert],[ServerKeyExch], [CertReq], <ServerHelloDone>

[Cert],<ClientKeyExchange>,[CertVerify]

<Finished>

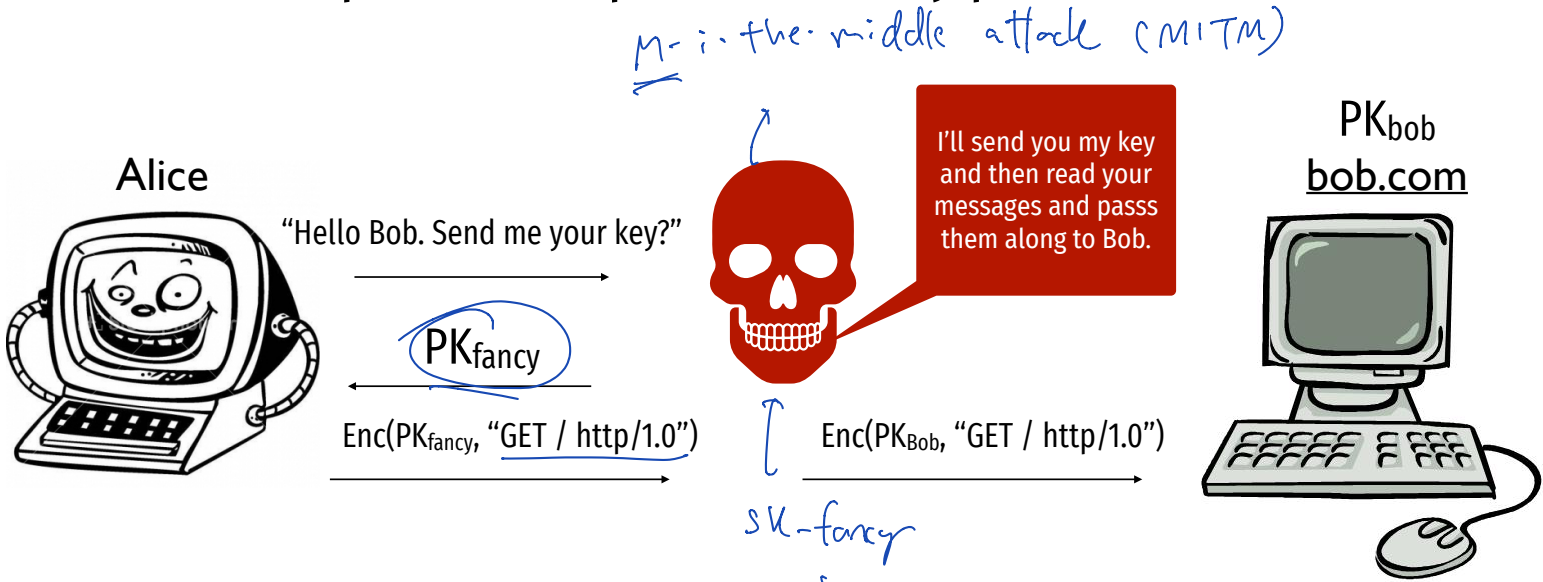
<Finished>

PK_{bob}

bob.com

Bob switches to the negotiated cipher

Goal of https: setup an encrypted channel

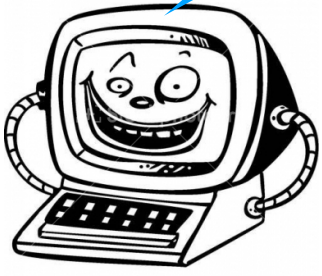


What if FancyBear sits in the middle?

TLS requires "Certificate Authorities"

I trust DigiCert and LetsEncrypt to verify public keys and domains

Alice



$Cert = Sig_{Digicert}(PK_{bob}, \underline{bob.com})$

PK_{bob}

bob.com

"Hello. Send me your key?"

PK_{bob} Certificate for (bob.com, PK_{bob})

Q: fancy bear) can send

PK-fancy, cert for (bob.com, PK-bob) ??

≠ ?

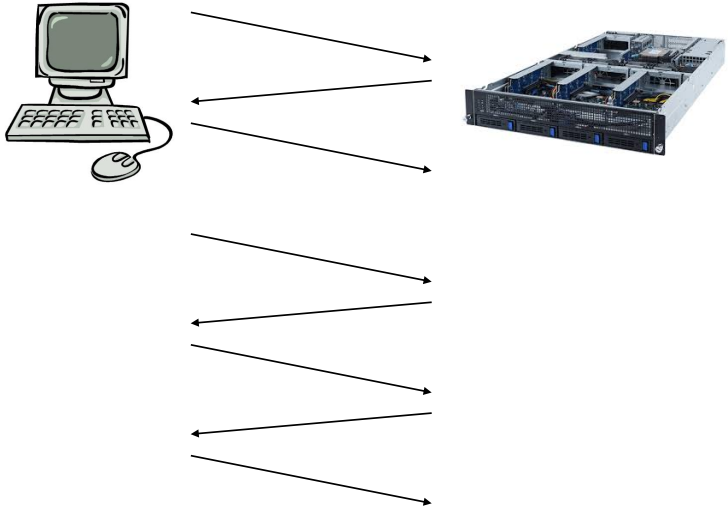
Demo

openssl can help you inspect certs.

openssl x509 -in cert.pem

```
abhi@l21:~/l25$ openssl s_client -connect www.google.com:443 -showcerts
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = GTS CA 1O1
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
verify return:1
---
Certificate chain
 0 s:C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
   i:C = US, O = Google Trust Services, CN = GTS CA 1O1
-----BEGIN CERTIFICATE-----
MIIEyTCCA7GgAwIBAgIRAOWJUBT/plbPAgAAAACAVf4wDQYJKoZIhvcNAQELBQAw
QjELMAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczET
d3cuZ29vZ2xlLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABKLISJuNl7yH
…
4oVg67pw7d42SpfMsYF1j8EC55iuyuLBLgeZ71B37dyGo3ZvfkTdGXwEFAEhn/eC
ne2mhh7QQGKD3Dp5mHmxPXDAQlJ6phDvsHVXCpE=
-----END CERTIFICATE-----
 1 s:C = US, O = Google Trust Services, CN = GTS CA 1O1
   i:OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
-----BEGIN CERTIFICATE-----
MIIESjCCAzKgAwIBAgINAeO0mqGNiqmBJWlQuDANBgkqhkiG9w0BAQsFADBMMSAw
HgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMjETMBEGA1UEChMKR2xvYmFs
…
IRdAvKLWZu/axBVbzYmqmwkm5zLSDW5nIAJbELCQCZwMH56t2Dvqofxs6BBcCFIZ
USpxu6×6td0V7SvJCCosirSmIatj/9dSSVDQibet8q/7UK4v4ZUN80atnZz1yg==
-----END CERTIFICATE-----
---
Server certificate
subject=C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com

issuer=C = US, O = Google Trust Services, CN = GTS CA 1O1

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: ECDSA
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 2640 bytes and written 386 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 256 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
```

```
abhi@l21:~/l25$ openssl s_client -connect www.google.com:443 -showcerts
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = GTS CA 1O1
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
verify return:1
---
Certificate chain
 0 s:C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
   i:C = US, O = Google Trust Services, CN = GTS CA 1O1
-----BEGIN CERTIFICATE-----
MIIEyTCCA7GgAwIBAgIRAOWJUBT/plbPAgAAAACAVf4wDQYJKoZIhvcNAQELBQAw
QjELMAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczET
d3cuZ29vZ2xlLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABKLISJuNl7yH
…
4oVg67pw7d42SpfMsYF1j8EC55iuyuLBLgeZ71B37dyGo3ZvfkTdGXwEFAEhn/eC
ne2mhh7QQGKD3Dp5mHmxPXDAQlJ6phDvsHVXCpE=
-----END CERTIFICATE-----
 1 s:C = US, O = Google Trust Services, CN = GTS CA 1O1
   i:OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
-----BEGIN CERTIFICATE-----
MIIESjCCAzKgAwIBAgINAeO0mqGNiqmBJWlQuDANBgkqhkiG9w0BAQsFADBMMSAw
HgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMjETMBEGA1UEChMKR2xvYmFs
…
IRdAvKLWZu/axBVbzYmqmwkm5zLSDW5nIAJbELCQCZwMH56t2Dvqofxs6BBcCFIZ
USpxu6×6td0V7SvJCCosirSmIatj/9dSSVDQibet8q/7UK4v4ZUN80atnZz1yg==
-----END CERTIFICATE-----
---
Server certificate
subject=C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com

issuer=C = US, O = Google Trust Services, CN = GTS CA 1O1

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: ECDSA
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 2640 bytes and written 386 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 256 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
```



One remaining issue...

HTTP

TLS

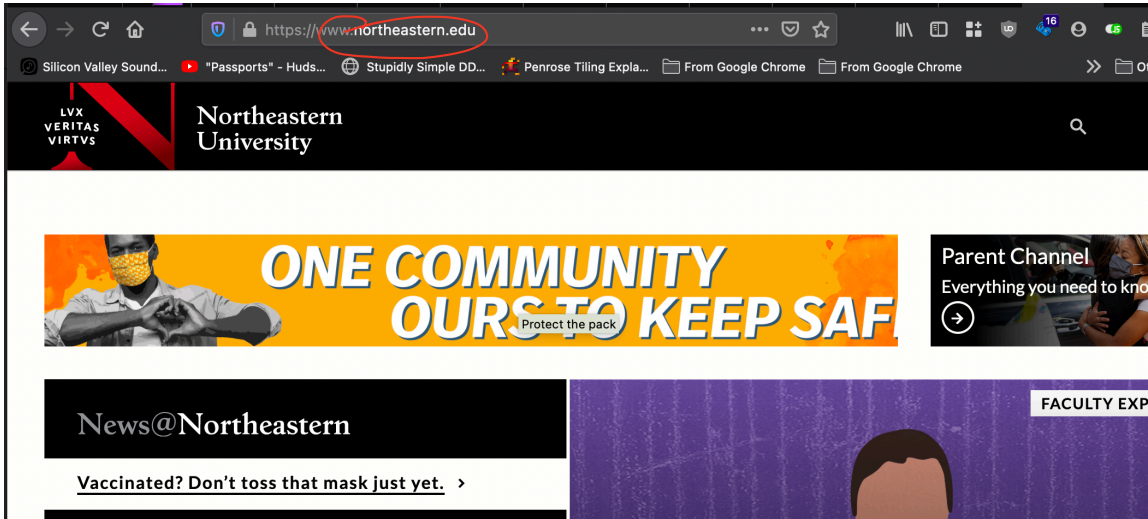
DNS

TCP

IP

192.168.... numerical address

Wifi/Ethernet



How does neu.edu resolve to IP address?

(name) (numerical)

Answer: your computer issues a DOMAIN NAME Service (DNS) query to learn the numerical IP.

Domain name service

```
MacBook-Pro:demos abhi$ dig www.northeastern.edu

; <<>> DiG 9.10.6 <<>> www.northeastern.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47992
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.northeastern.edu.INA

;; ANSWER SECTION:
www.northeastern.edu.          300    IN   CNAME   northeastern.edu.edgekey.net.
northeastern.edu.edgekey.net. 300    IN   CNAME   e12215.dscb.akamaiedge.net.
e12215.dscb.akamaiedge.net.    20     IN   A       23.38.112.43
e12215.dscb.akamaiedge.net.    20     IN   A       23.38.112.27

;; Query time: 31 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Tue Apr 13 06:24:41 EDT 2021
;; MSG SIZE  rcvd: 160
```

address that we want.

How DNS Works

Domain Name Service

DNS is a distributed database

Purpose: map a name to an IP address.

No single database contains all map entries. It is hierarchical.

Database is a “rooted tree”, internal nodes are delegated to domain owners.

Runs over UDP on port 53 (usually).

Queries are usually cached for performance.

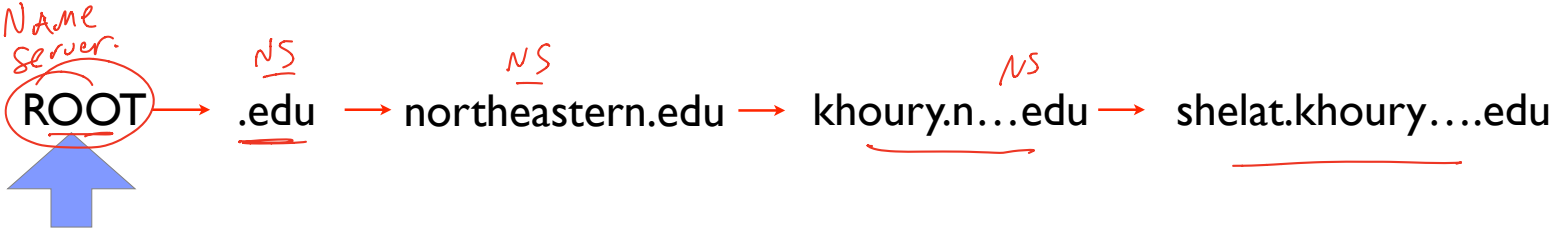
↑ this could create a security attack.

http://shelat.khoury.northeastern.edu

Browser needs to map the name to an IP address.

This process is the domain name service.

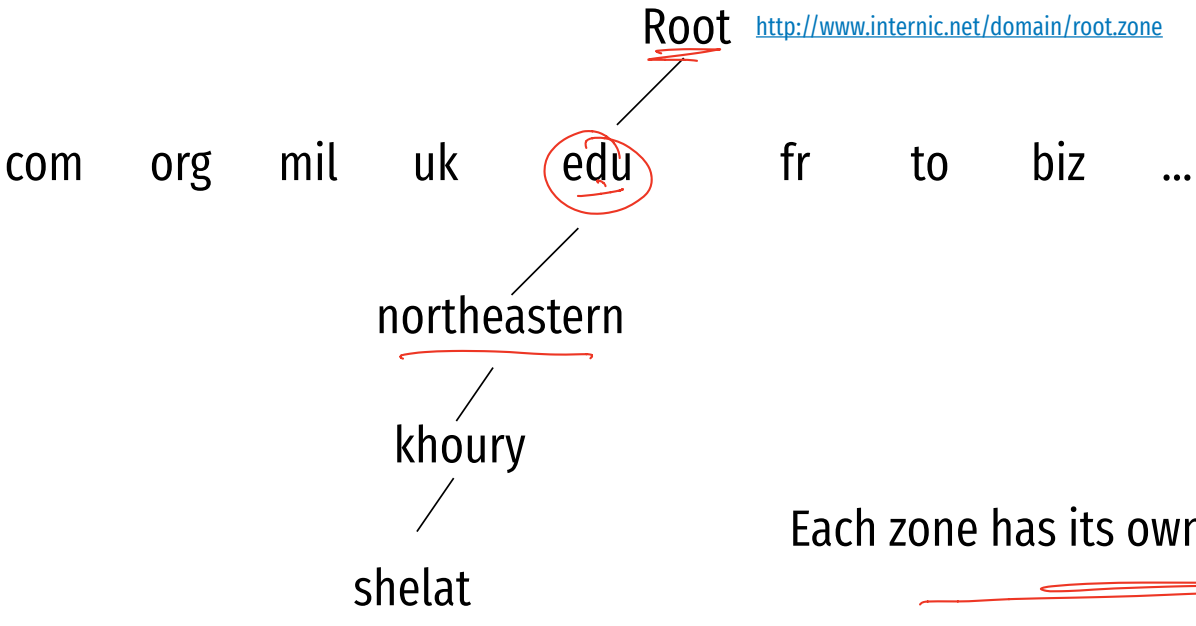
The search is hierarchical, starting from the ROOT



It is bootstrapped by an agreed upon set of ROOT servers.

a.root-servers.net	198.41.0.4
b.root-servers.net	192.228.79.201
c.root-servers.net	192.33.4.12
....	
m.root-servers.net	202.12.27.33

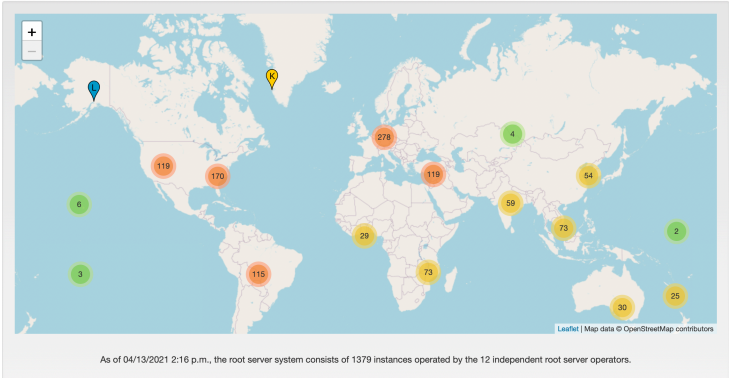
DNS hierarchy



Each zone has its own administrator.

Zone file

```
.     86400 IN  SOA a.root-servers.net. nstld.verisign-grs.com. 2021041300 1800 900 604800 86400
.     86400 IN  RRSIG SOA 8 0 86400 20210426050000 20210413040000 14631 .
TR1THuipZNwnIGYPDUrvwk627UUS0×2tzA34+K3KfC9sujDsgFpiipXEo5R8lLuhwlIG2/
jzxg7UNVlbVk8VytAyQKoPZ3RDM8SqlRRT7h3O7tEKRpQsu+1UwWlPcNMM740lAxRnao/qDEU2P2TvfYn6xTgeiXP/2g0EcPcUb/
fnIbijwbaef07m8OEQBRO/R3Ssr71c0fCJ31fjmw0HHdRpnGEV1fkE4PescB0Qr/
fBn0zL2l2JwY5LpSIsTK9YsxFkEPUAfLmefPGmFWVp2QR2CgMCVBiPZZs4cGuEjHkDdcpL0uIDr80OdmJcOzznAMZPUIv73DGJFcHz
ow==
.     518400  IN  NS  a.root-servers.net.
.     518400  IN  NS  b.root-servers.net.
.     518400  IN  NS  c.root-servers.net.
.     518400  IN  NS  d.root-servers.net.
.     518400  IN  NS  e.root-servers.net.
.     518400  IN  NS  f.root-servers.net.
.     518400  IN  NS  g.root-servers.net.
.     518400  IN  NS  h.root-servers.net.
.     518400  IN  NS  i.root-servers.net.
.     518400  IN  NS  j.root-servers.net.
.     518400  IN  NS  k.root-servers.net.
.     518400  IN  NS  l.root-servers.net.
.     518400  IN  NS  m.root-servers.net.
.     518400  IN  RRSIG NS 8 0 518400 20210426050000 20210413040000 14631 .
rL2H84ehh9QBxCsjSUaEuKoevwQNBT+lEdOX5KRAJvFxSqnjiHLl6c37d8ADrIA7H7/4oasFntGzOJc3vex7MhzvsZiZomJT0vvUCU
TWpyB0429ZEVRuzggI6wulEEc9bdWtERXiDGAFLGGgBorIkDuodIzTCNgzRrK8IFCxDj8B2hZr2djOpWllPms82TfWW3ci+k3Fb0+v
j5Aeo6jL0R5Qha8puyIQWnO31cqGH/2j+VVL0WA0RLgzo4FQkH35Dxs3X+vaYmIQNmDyByjqC39QgT
+Erh35a5IRiQ4cISrf1Q0HcG2Ybd/jmaogTdUyQBZSMKmjywE2Q==
      86400 IN  NSEC  aaa. NS SOA RRSIG NSEC DNSKEY
```



root-servers.org

```
# Version 2012091300, Last Updated Thu Sep 13 07:07:01 2012 UTC
AC
AD
AE
AERO
AF
AG
AI
AL
AM
AN
AO
AQ
AR
ARPA
AS
ASIA
AT
AU
AW
AX
AZ
BA
BB
BD
BE
BF
BG
BH
BI
BIZ
BJ
BM
BN
BO
BR
BS
BT
BV
BW
BY
BZ
CA
CAT
CC
CD
```

```
edu.     172800 IN  NS  a.edu-servers.net.
edu.     172800 IN  NS  c.edu-servers.net.
edu.     172800 IN  NS  d.edu-servers.net.   192.31.80.30
edu.     172800 IN  NS  f.edu-servers.net.
edu.     172800 IN  NS  g.edu-servers.net.
edu.     172800 IN  NS  l.edu-servers.net.
EDU.     86400  IN  DS  28065 8 2
4172496CDE85534E51129040355BD04B1FCFEBAE996DFDDE652006F6
B2CE76
EDU.     86400  IN  RRSIG  DS 8 1 86400 20120920000000
20120912230000 50398 .
D3jwWu5IZxr1TDjtjK5o5eB40XSlyrGBQBkRdpUB3Zoux5NgHssU5vNq
SuNhvhdjMR5fBH9R22r+altDtejWS+l0KxtsjHVb6RpnuA+pHh+z3wkc
ITGtSEqS0WoQhVp+itfiQ8FibdrOZsbJ8U0f3xlP/WtBso1pCKyOxEY=
```

```
MacBook-Pro:go abhi$ dig northeastern.edu @a.edu-servers.net

; <<>> DiG 9.10.6 <<>> northeastern.edu @a.edu-servers.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58429
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;northeastern.edu.      IN  A

;; AUTHORITY SECTION:
northeastern.edu.   172800  IN  NS  nb4276.neu.edu.
northeastern.edu.   172800  IN  NS  nb4277.neu.edu.
northeastern.edu.   172800  IN  NS  a3-64.akam.net.
northeastern.edu.   172800  IN  NS  a1-157.akam.net.
northeastern.edu.   172800  IN  NS  a12-65.akam.net.
northeastern.edu.   172800  IN  NS  a5-65.akam.net.
northeastern.edu.   172800  IN  NS  a24-67.akam.net.
northeastern.edu.   172800  IN  NS  a10-66.akam.net.

;; ADDITIONAL SECTION:
nb4276.neu.edu.     172800  IN  A   155.33.16.201
nb4277.neu.edu.     172800  IN  A   155.33.16.202

;; Query time: 52 msec
;; SERVER: 192.5.6.30#53(192.5.6.30)
;; WHEN: Fri Apr 16 08:54:55 EDT 2021
;; MSG SIZE  rcvd: 255
```

Where is shelat.khoury.northeastern.edu?

Use root to find .edu DNS name server:

use .edu NS to find the northeastern.edu NS

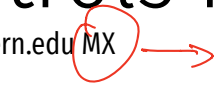
...

to eventually find the A record for

shelat.khoury.neu.edu ...

DNS also controls how email works

```
MacBook-Pro:go abhi$ dig northeastern.edu MX

; <<>> DiG 9.10.6 <<>> northeastern.edu MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30930
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;northeastern.edu.      IN  MX

;; ANSWER SECTION:
northeastern.edu.   3600    IN  MX  20 northeastern-edu.mail.protection.outlook.com.

;; Query time: 49 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Fri Apr 16 08:57:36 EDT 2021
;; MSG SIZE  rcvd: 105
```



Network exploits

Network exploits

Previous insight: security vulnerabilities arise when external input is not verified.

Network insight: security vulnerabilities arise due to failures of design and abstraction.

Networks were designed for convenience.

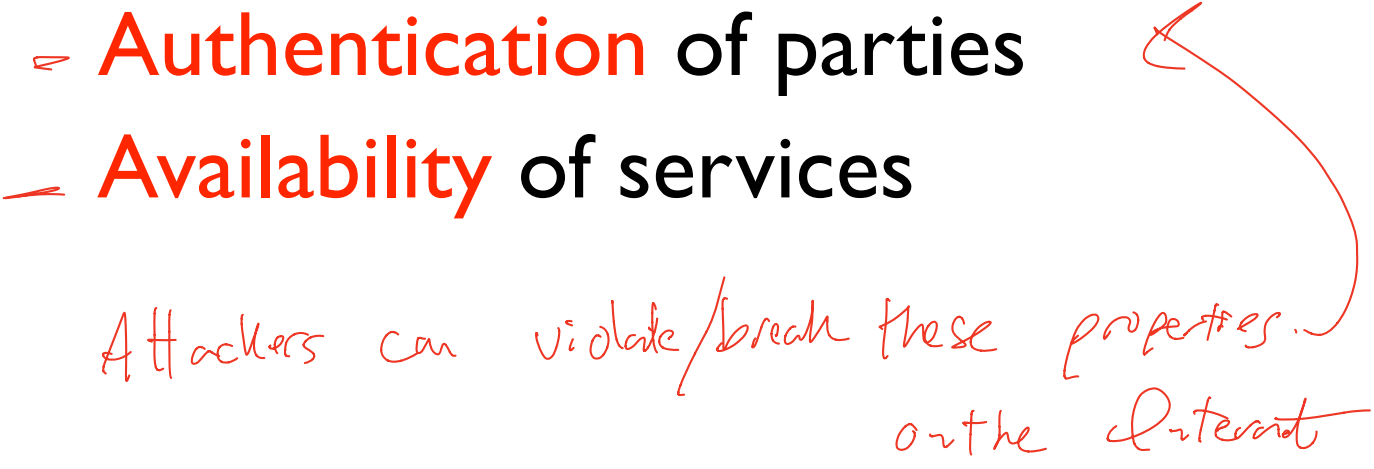
Security was an afterthought.

Networks increase number of possible attackers.
(Attack surface is increased.)

Networks provide some anonymity to the attacker.

Issues with

- Privacy of Information
- Authentication of parties
- Availability of services



Infrastructure attacks

actively listen and modify traffic as it flows across your nodes

denial-of-service

attack the routers that control traffic flow

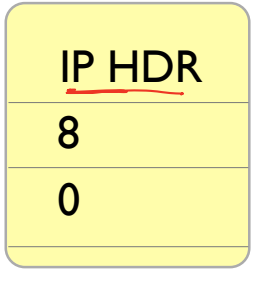
attack the domain naming system to redirect traffic

Availability attacks

ICMP

ECHO request

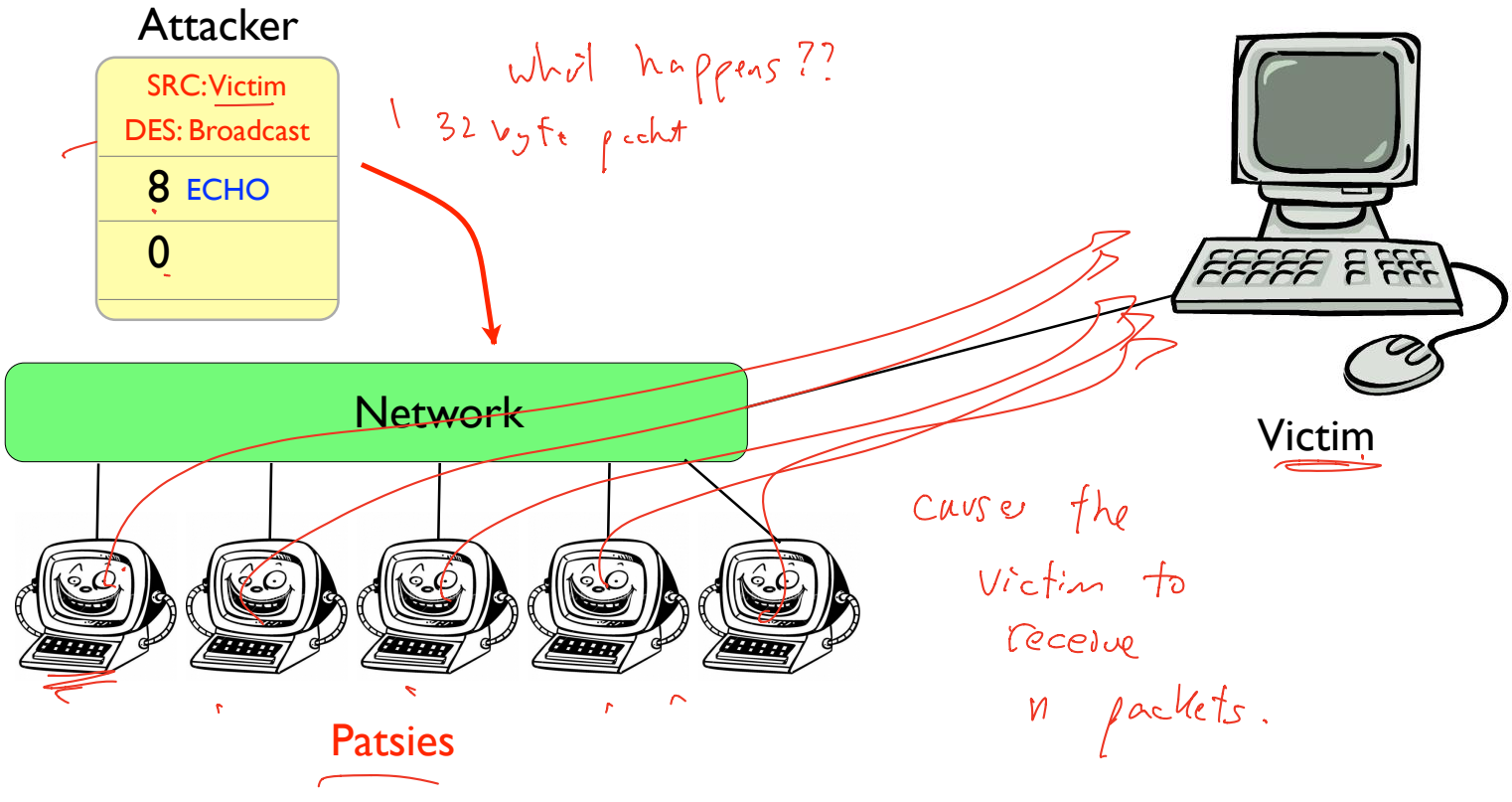
"Ping"



ECHO request

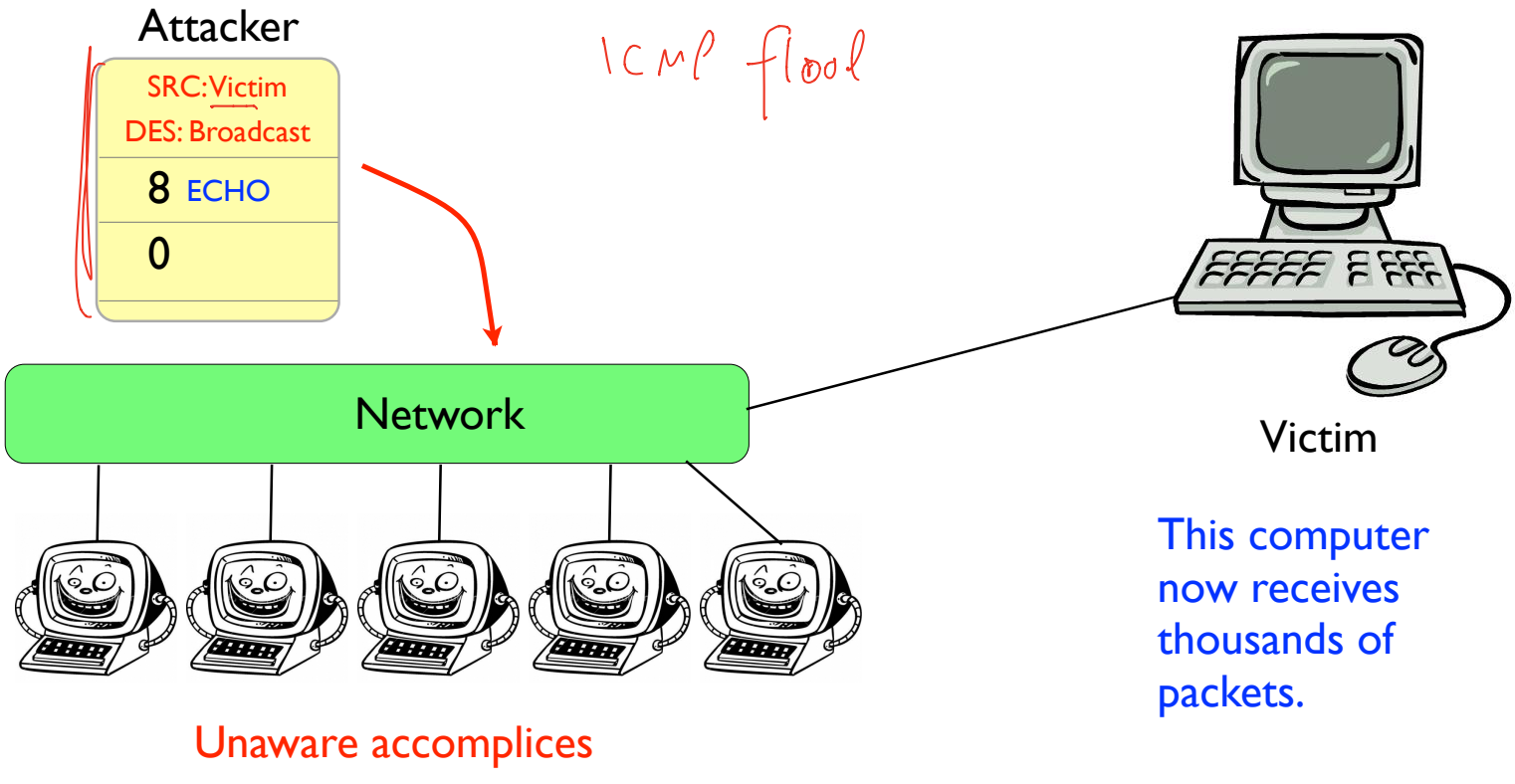
Code 0

ping www.northeastern.edu



http://www.stockphotopro.com/photo_of/cartoon/5809266ZQA/__cartoon__computer_

https://encrypted-tbn3.google.com/images?q=tbn:ANd9GcQGg_2LSF_hJV2xtAzqWY0e_ICU8TIc2fDbZ4n29jZATD4Vzlx8nA



http://www.stockphotopro.com/photo_of/cartoon/5809266ZQA/__cartoon__computer_

https://encrypted-tbn3.google.com/images?q=tbn:ANd9GcQGg_2LSF_hJV2xtAzqWY0e_ICU8TIc2fDbZ4n29jZATD4Vzlx8nA

Example

```
05:53:13.542869 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 0, length 8
05:53:13.542882 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 0, length 8
05:53:13.542925 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 0, length 8
05:53:13.542962 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 0, length 8
05:53:13.542970 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 0, length 8
05:53:13.547162 IP 192.168.1.227 > 192.168.1.179: ICMP echo reply, id 44759, seq 0, length 8
05:53:13.644280 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 256, length 8
05:53:13.644286 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 256, length 8
05:53:13.644371 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 256, length 8
05:53:13.644411 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 256, length 8
05:53:13.644421 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 256, length 8
05:53:13.647841 IP 192.168.1.227 > 192.168.1.179: ICMP echo reply, id 44759, seq 256, length 8
05:53:13.703057 IP 192.168.1.164 > 192.168.1.179: ICMP echo reply, id 44759, seq 0, length 8
05:53:13.703073 IP 192.168.1.164 > 192.168.1.179: ICMP echo reply, id 44759, seq 256, length 8
05:53:13.744700 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 512, length 8
05:53:13.744708 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 512, length 8
05:53:13.744785 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 512, length 8
05:53:13.744826 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 512, length 8
05:53:13.744833 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 512, length 8
05:53:13.748830 IP 192.168.1.227 > 192.168.1.179: ICMP echo reply, id 44759, seq 512, length 8
05:53:13.818953 IP 192.168.1.27 > 192.168.1.179: ICMP echo reply, id 44759, seq 0, length 8
05:53:13.823841 IP 192.168.1.27 > 192.168.1.179: ICMP echo reply, id 44759, seq 256, length 8
05:53:13.823846 IP 192.168.1.27 > 192.168.1.179: ICMP echo reply, id 44759, seq 512, length 8
05:53:13.847079 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 768, length 8
05:53:13.847088 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 768, length 8
05:53:13.847098 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 768, length 8
05:53:13.847145 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 768, length 8
05:53:13.847154 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 768, length 8
05:53:13.851525 IP 192.168.1.227 > 192.168.1.179: ICMP echo reply, id 44759, seq 768, length 8
05:53:13.950009 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 1024, length 8
05:53:13.950015 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 1024, length 8
05:53:13.950098 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 1024, length 8
05:53:13.950144 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 1024, length 8
05:53:13.950153 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 1024, length 8
05:53:13.954522 IP 192.168.1.227 > 192.168.1.179: ICMP echo reply, id 44759, seq 1024, length 8
05:53:13.994912 IP 192.168.1.61 > 192.168.1.179: ICMP echo reply, id 44759, seq 512, length 8
05:53:14.010148 IP 192.168.1.164 > 192.168.1.179: ICMP echo reply, id 44759, seq 512, length 8
05:53:14.010153 IP 192.168.1.164 > 192.168.1.179: ICMP echo reply, id 44759, seq 768, length 8
05:53:14.010154 IP 192.168.1.164 > 192.168.1.179: ICMP echo reply, id 44759, seq 1024, length 8
05:53:14.053406 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 1280, length 8
05:53:14.053415 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 1280, length 8
05:53:14.053504 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 1280, length 8
05:53:14.053568 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 1280, length 8
05:53:14.053577 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 1280, length 8
05:53:14.057849 IP 192.168.1.227 > 192.168.1.179: ICMP echo reply, id 44759, seq 1280, length 8
05:53:14.110572 IP 192.168.1.27 > 192.168.1.179: ICMP echo reply, id 44759, seq 768, length 8
05:53:14.110578 IP 192.168.1.27 > 192.168.1.179: ICMP echo reply, id 44759, seq 1024, length 8
05:53:14.110578 IP 192.168.1.27 > 192.168.1.179: ICMP echo reply, id 44759, seq 1280, length 8
05:53:14.110579 IP 192.168.1.61 > 192.168.1.179: ICMP echo reply, id 44759, seq 768, length 8
05:53:14.110579 IP 192.168.1.61 > 192.168.1.179: ICMP echo reply, id 44759, seq 1024, length 8
05:53:14.110579 IP 192.168.1.61 > 192.168.1.179: ICMP echo reply, id 44759, seq 1280, length 8
05:53:14.158299 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 1536, length 8
05:53:14.158307 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 1536, length 8
05:53:14.158328 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 1536, length 8
05:53:14.158374 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 1536, length 8
05:53:14.158383 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 1536, length 8
05:53:14.161985 IP 192.168.1.227 > 192.168.1.179: ICMP echo reply, id 44759, seq 1536, length 8
05:53:14.259955 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 1792, length 8
05:53:14.259971 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 1792, length 8
05:53:14.260033 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 1792, length 8
05:53:14.260072 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 1792, length 8
05:53:14.260076 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 1792, length 8
05:53:14.264111 IP 192.168.1.227 > 192.168.1.179: ICMP echo reply, id 44759, seq 1792, length 8
05:53:14.317445 IP 192.168.1.164 > 192.168.1.179: ICMP echo reply, id 44759, seq 1280, length 8
05:53:14.317453 IP 192.168.1.164 > 192.168.1.179: ICMP echo reply, id 44759, seq 1536, length 8
05:53:14.317454 IP 192.168.1.164 > 192.168.1.179: ICMP echo reply, id 44759, seq 1792, length 8
05:53:14.361953 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 2048, length 8
05:53:14.361960 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 2048, length 8
05:53:14.362043 IP 192.168.1.179 > 192.168.1.255: ICMP echo request, id 44759, seq 2048, length 8
05:53:14.362083 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 2048, length 8
05:53:14.362091 IP 192.168.1.179 > 192.168.1.179: ICMP echo reply, id 44759, seq 2048, length 8
05:53:14.366664 IP 192.168.1.227 > 192.168.1.179: ICMP echo reply, id 44759, seq 2048, length 8
05:53:14.419872 IP 192.168.1.27 > 192.168.1.179: ICMP echo reply, id 44759, seq 1536, length 8
05:53:14.419882 IP 192.168.1.27 > 192.168.1.179: ICMP echo reply, id 44759, seq 1792, length 8
05:53:14.419882 IP 192.168.1.27 > 192.168.1.179: ICMP echo reply, id 44759, seq 2048, length 8
```

What missing security property enables the attack?

What missing security property enables the attack?

Authentication

of parties

is missing. So anyone can "forge" the IP source/destination !!

The SRC/DST fields of a packet are unauthenticated.
It is possible to mimic any IP on the internet.

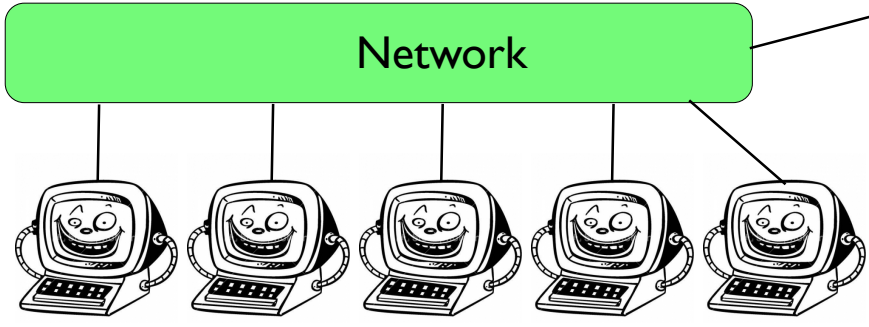
Proper network configuration can limit the attack.

What steps should a network router/gateway/accesspoint take?

- add rules to prevent packet hdr forgery
-

Attacker

SRC: Victim
DES: Broadcast
8 ECHO
0



Network

Patsies

Victim

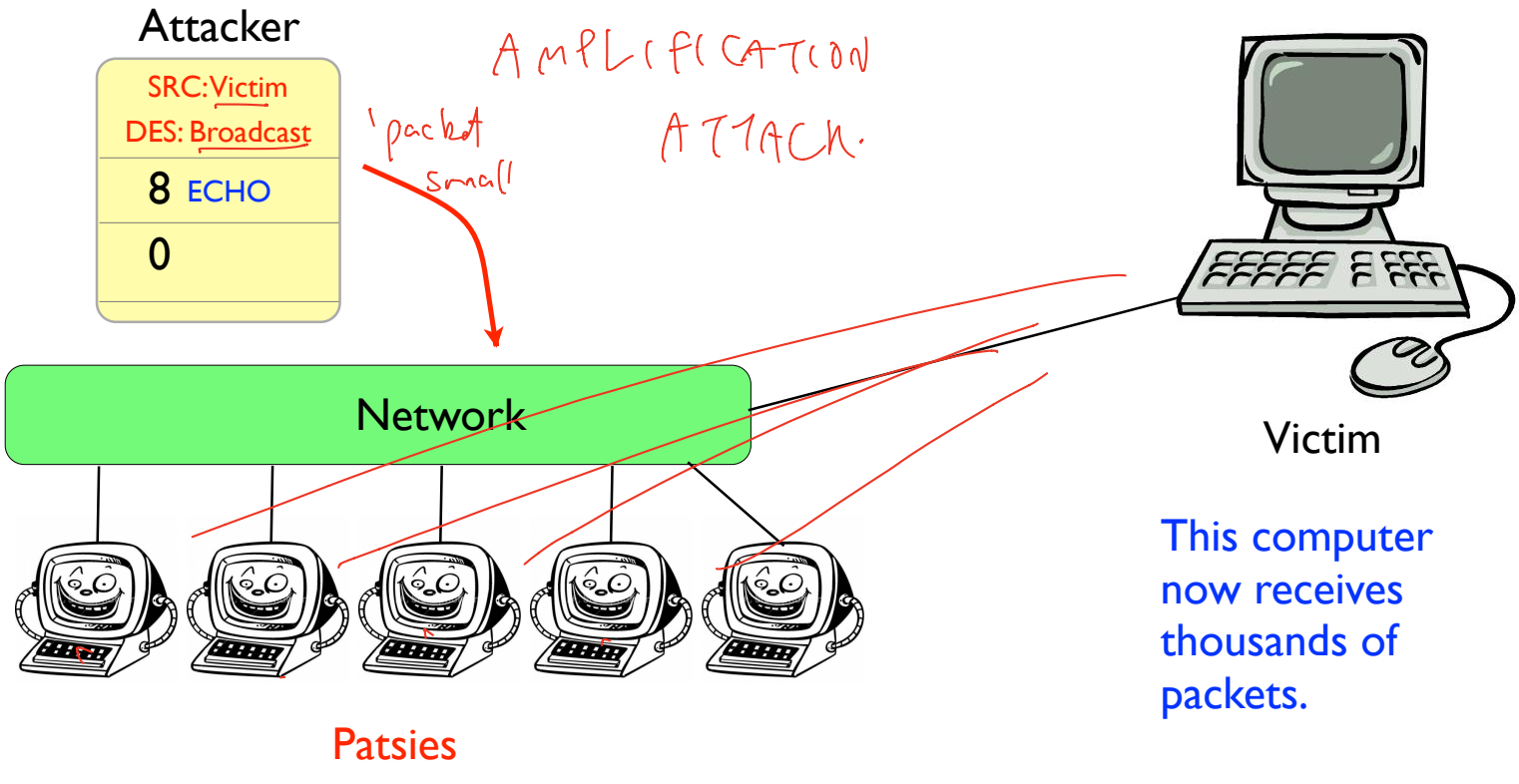
This computer now receives thousands of packets.

http://www.stockphotopro.com/photo_of/cartoon/5809266ZQA/__cartoon__computer_

https://encrypted-tbn3.google.com/images?q=tbn:ANd9GcQGg_2LSF_hJV2xtAzqWY0e_ICU8TIc2fDbZ4n29jZATD4Vzlx8nA

Attacker is able to LEVERAGE its resources.

1 attack packet becomes 1000s.



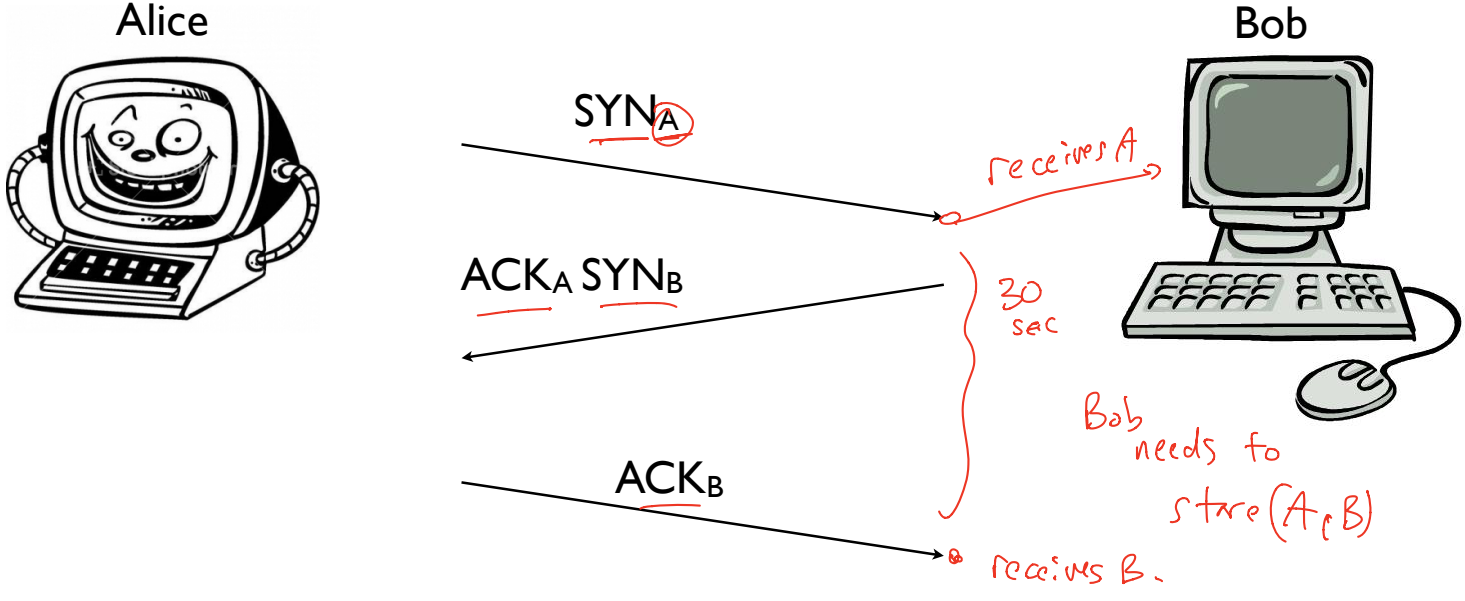
http://www.stockphotopro.com/photo_of/cartoon/5809266ZQA/__cartoon__computer_

https://encrypted-tbn3.google.com/images?q=tbn:ANd9GcQGg_2LSF_hJV2xtAzqWY0e_ICU8TIc2fDbZ4n29jZATD4Vzlx8nA

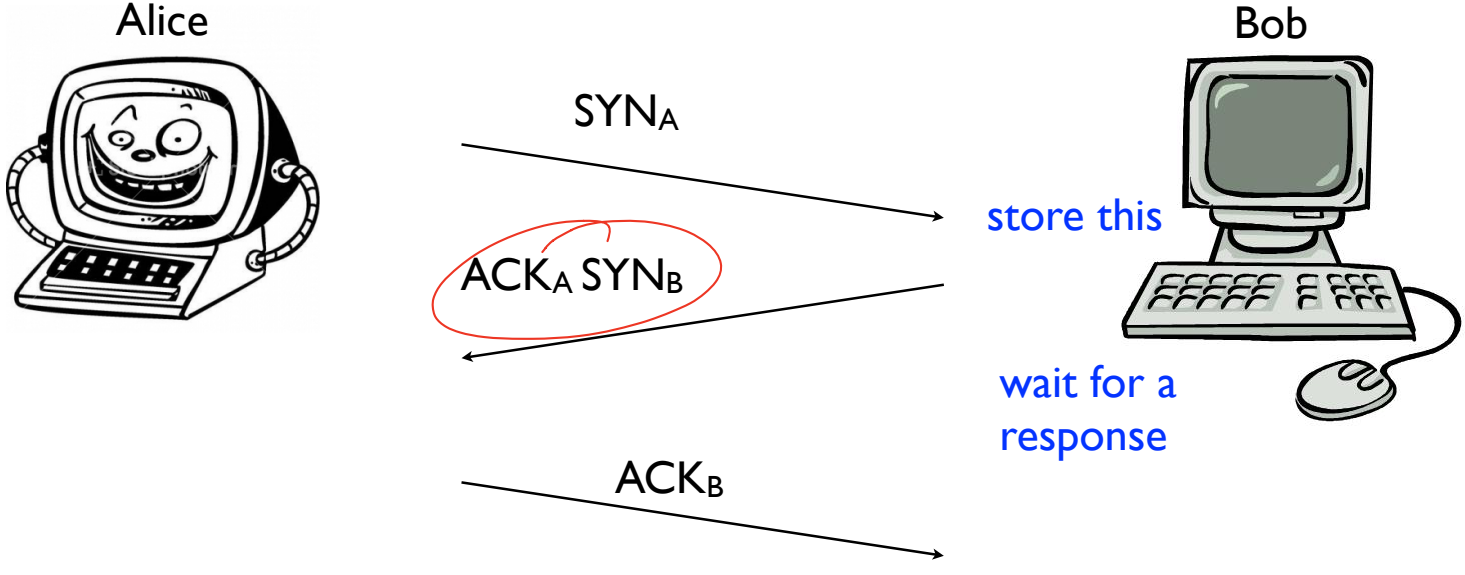
Attacker is able to LEVERAGE its resources.

1 attack packet becomes 1000s.

How a TCP begins



How a TCP begins



How a TCP flood begins

IP

SYN_A

SYN_{A2}

SYN_{A3}

SYN_{A4}

SYN_{A5}

victim stores each of these for timeout (1-2 min)

soon, entire memory is consumed

Amplification

IP1 SYN$_A$

IP2 SYN$_{A2}$

IP3 SYN$_{A3}$

victim stores each of these for timeout (1-2 min)

No storage.

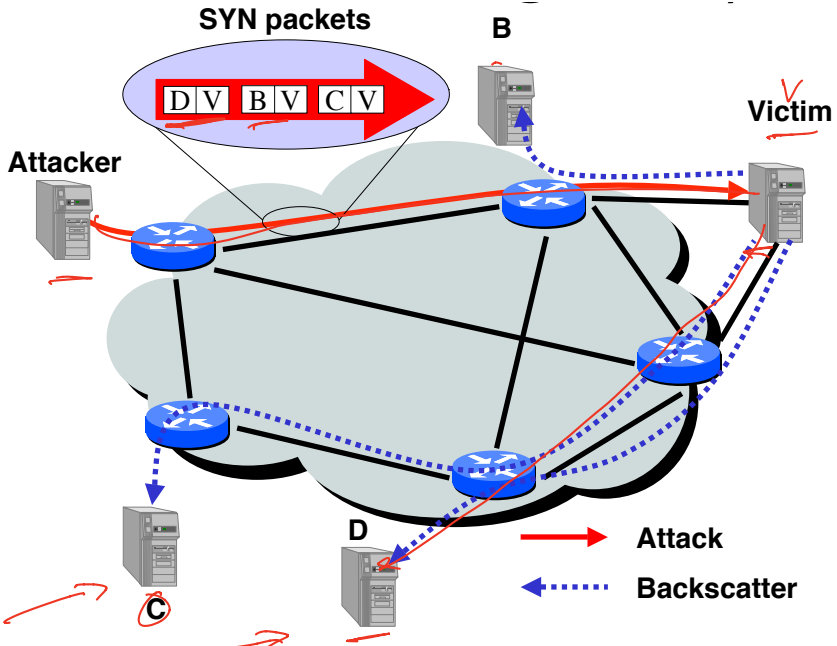
1 32b packet causes **1024b** alloc.

4Kb.

storage on

Denial of Service BACKSCATTER

Detector for SYN flood attacks



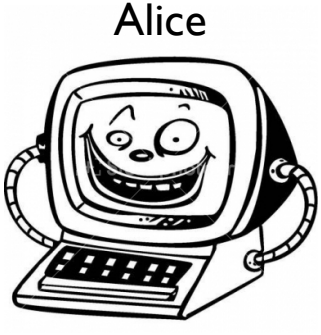
these are the "lenses" of a scope. Listen for "ACK (SYN"

Moore, Voelker, Savage 2001

	Trace-1	Trace-2	Trace-3
Dates (2001)	Feb 01 – 08	Feb 11 – 18	Feb 18 – 25
Duration	7.5 days	6.2 days	7.1 days
Flow-based Attacks:			
Unique victim IPs	1,942	1,821	2,385
Unique victim DNS domains	750	693	876
Unique victim DNS TLDs	60	62	71
Unique victim network prefixes	1,132	1,085	1,281
Unique victim Autonomous Systems	585	575	677
Attacks	4,173	3,878	4,754
Total attack packets	50,827,217	78,234,768	62,233,762
Event-based Attacks:			
Unique victim IPs	3,147	3,034	3,849
Unique victim DNS domains	987	925	1,128
Unique victim DNS TLDs	73	71	81
Unique victim network prefixes	1,577	1,511	1,744
Unique victim Autonomous Systems	752	755	874
Attack Events	112,457	102,204	110,025
Total attack packets	51,119,549	78,655,631	62,394,290

Table 2: Summary of backscatter database.

SYN Cookies



SYN_A

don't store this

$ACK_A\ SYN_B$

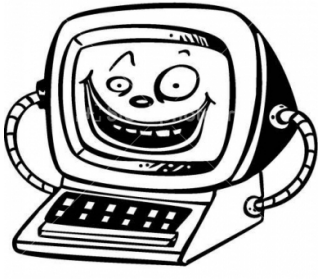
seq# = f(state)

ACK_B seq#

use f(state) to recompute state

SYN Cookies

Alice



Bob

SYN_A

don't store this

$ACK_A\ SYN_B$

seq# = f(state)

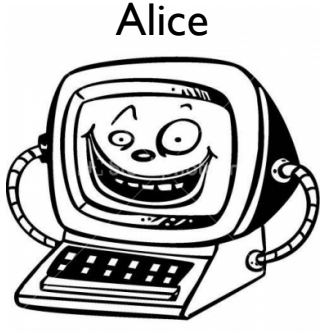
(A, B)

What cryptographic properties does the function f require?

ACK_B seq#

use f(state) + IP addr to recompute/verify state

Cuckoo TCP



SYN_A

$ACK_A\ SYN_B$

ACK_B

if state is full, then randomly evict a "WAITING" TCP Entry

Ping of DEATH

Normal PING requests require 32 bytes.

Attack: send a 65k PING request.

DNS traffic amplification

dig yahoo.com any

;; Query time: 6 msec
;; SERVER: 128.143.2.7#53(128.143.2.7)
;; WHEN: Thu Sep 13 13:44:04 2012
;; MSG SIZE rcvd: 506

~50byte UDP packet leads to a 506b response

10x

d-172-27-45-104: abhi$ dig +bufsize=4096 +dnssec any se @a.ns.se

DNS query with victim AS src IP !!

160x traffic amplification

```
; <<>> DiG 9.8.1-P1 <<>> +bufsize=4096 +dnssec any se @a.ns.se
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29242
;; flags: qr aa rd; QUERY: 1, ANSWER: 20, AUTHORITY: 0, ADDITIONAL: 26
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;se.                            IN      ANY

;; ANSWER SECTION:
se.                     172800  IN      SOA     catcher-in-the-rye.nic.se. registry-default.nic.se. 2012091304 1800 1800 864000 7200
se.                     172800  IN      RRSIG   SOA 5 1 172800 20120925190422 20120913081101 58656 se. DtVv7a9TE2PorcAHozltJ8x8lkkrSJYbUf9zsAUzkZHmadMMcRvm1u1N snzCnURQHILqB7+v0mXySrpl4bW15wVZn6UjcpEEQjq7uqeahK8nOlxJ
XqLvxdz5Ro7WR1+V3dAPm3RH5X7962mZrKdVXF/E01upf96+zxwimOTN lf4=
se.                     172800  IN      NS      e.ns.se.
se.                     172800  IN      NS      b.ns.se.
se.                     172800  IN      NS      c.ns.se.
se.                     172800  IN      NS      a.ns.se.
se.                     172800  IN      NS      i.ns.se.
se.                     172800  IN      NS      g.ns.se.
se.                     172800  IN      NS      d.ns.se.
se.                     172800  IN      NS      f.ns.se.
se.                     172800  IN      NS      j.ns.se.
se.                     172800  IN      RRSIG   NS 5 1 172800 20120924194433 20120911201101 58656 se. M3jZ0lhDkvBfizaxzFgsFWbAEJKN6aj4fn5ZPBlHlwgVTL7jhhsiTd2u HB9Kp0bDSwlBDxnwvGtr8g+Hem9RitYZXxHkbfP9SXhuKsZVtM7Y5WUB
CF7lwRywwnSikjb8su7Ewki7bO5aLTHCWu+1/jPDRNUofHfISqSlJxKm gvI=
se.                     172800  IN      TXT     "SE zone update: 2012-09-13 09:07:13 +0000 (EPOCH 1347527233) (auto)"
se.                     172800  IN      RRSIG   TXT 5 1 172800 20120927095501 20120913081101 58656 se. CKXLjyfqXBYQqYdkUTKPbAwhzQi24DebVrDqrhOo0vMLqCum4AwjrzaV snDHgv1KSMM9ifPYEz5jSrVUsOOyxNgmRKjmIXgjRiaylurvZjlpu2kE
Nd3ppJ5LkP7LuZnbrtVWYmFlYNzlkJDj62TZFdYrFRkGXf6JedU8ldIr zpg=
se.                     7200    IN      NSEC    0-0.se. NS SOA TXT RRSIG NSEC DNSKEY
se.                     7200    IN      RRSIG   NSEC 5 1 7200 20120924215357 20120910221101 58656 se. ZwvY5T0fW84iqsdrQkgIfFhJ6aXYWmLkm+HCiv9/wisTmTj8UJC1dSHm ysZnr0zZ1PS/D+ymVGc/cMiKb3d8Nq2w+/piAHpEqiOtkh38e1ngGX+C
MclBkYV5FiuEC1QSiM+D7H7GSSPrqUBx2M3heWz8MucQvO3MCL81ESsJ WaE=
se.                     3600    IN      DNSKEY  257 3 5 AwEAAZYYG1hpk8XKHNHpdO/EEg+r4YmIEC4Fn3x2DEsygxDuoT9d/QCi X1pz0omFGCaVfCWHvaScVvWd4xP4kNDnSDQxBzPwLEXE3l0cLseMJ2YM QeBPf3hGhLs6VSDnGFKAzNG4fhri9EBTLv9ubL8Kx8cWQKuu3A5HRVD3
li7IZB+0kmUKqGilQdERKt/Ec36BkK93lyGags5RrR2VDdrXCj9Yay90 KCKITk52AbwVoMPm0OYlPbD4ViBPMk5nmh/dPeCoZoVJxgANZ/doVQxR 5vDkMBYxuhrXuQk3CvZBB011NsXxk9yHtHvp/5gjUVJjvhdRvjRB6/xY R03c9owi/aM=
se.                     3600    IN      DNSKEY  256 3 5 AwEAAbTmWA2HUXP60ITEiYuK2E08t4LECz3acvQbzRWScFNl9FWqwcDY mWjZgXYmHWsAqM/Nl3xWR+eQ7/VgLTXMbVlxWMLFlPLGHCe1vI69kNNN N4V/iYt0bjWwvkhys5cYYRocjfYhusGumpqJ2G9OUkjJdk5m6EH/+LIp PJmplg
se.                     3600    IN      DNSKEY  256 3 5 AwEAAe7gh8/AVUjbsQq9PKtoBHOfl/WHTopJCOsEoB7tOaCBov6eN7yO VZT4TOl4idc0R1HGc9bFzQ0U+/4wWBPbVltV8bm1EQm+SNtlONtd6T2d 3wDXhouf1nHCdDKt1mYXuSCaQbgf55xYaPNLEvu5VDtwOIL9C2Gu+XdH aONnbYl
se.                     3600    IN      RRSIG   DNSKEY 5 1 3600 20120924020128 20120910101101 59747 se. GEHtQQL8VOc8FiVCB7SfQ6/WYrzWhA1ftT8v2JElRXF0e6e1TurXepZW QZ1F1jky0lQ31Qt7pbsBA/sOvfWaB4GLMKkgYG2dZgQUwifMi5l5cXyF
EvZzH+jg63Hh1fsorCEcRLNlxRZ4sTkUx/cH7IGp1dpZYpGlRkbQl4Tp zALzkjBulHfMM05hrt6Bh5d/3AfUhlwtN8iu5JX3qPRY+5BVufvTKVpB Dw8zR38sHeqBDL3nPLLje6PhlyyMoM0NuzZh0WfwqFmbJCs+WZiyq1QZ Nm2K3uBMQx7NLaLqFptHb3XB0lhXTWE3PLNij17qg+RHHBPgzwiJY+ja pbNHCg==

;; ADDITIONAL SECTION:
a.ns.se.                172800  IN      A       192.36.144.107
a.ns.se.                172800  IN      AAAA    2a01:3f0:0:301::53
b.ns.se.                172800  IN      A       192.36.133.107
c.ns.se.                172800  IN      A       192.36.135.107
d.ns.se.                172800  IN      A       81.228.8.16
e.ns.se.                172800  IN      A       81.228.10.57
f.ns.se.                172800  IN      A       192.71.53.53
g.ns.se.                172800  IN      A       130.239.5.114
g.ns.se.                172800  IN      AAAA    2001:6b0:e:3::1
i.ns.se.                172800  IN      A       194.146.106.22
i.ns.se.                172800  IN      AAAA    2001:67c:1010:5::53
j.ns.se.                172800  IN      A       199.254.63.1
j.ns.se.                172800  IN      AAAA    2001:500:2c::1
```

j.ns.se. 172800 IN AAAA 2001:500:2c::1
a.ns.se. 172800 IN RRSIG A 5 3 172800 20120926094152 20120912121101 58656 se. cB0VnZRRe7GmP+Ild4rNmQJefMQKx+HOq26gCs+k3q7ZttetdFtqZQa7 hGEkWnALljwqIFgxQucnMRrSVso0uZI21zCe7katSYyK9wJSG1dpsk/G QYcMJc/
EA0deKIVkmA77TWeAi9Atl3cfgDUsibmmCJ08qp34zdoe8wBM fG0=
a.ns.se. 172800 IN RRSIG AAAA 5 3 172800 20120926005130 20120913041101 58656 se. pat/9jqrPpm/AP2czFcNCt477zy9wGgnngeuul+mJsN5l46py+4x0dVS 1dp25ul7BS4nwl/I1yBcvxhPf2bavfLKOqV16p+/yfcBE9Inw8p0O13B
J9Ad87Lb+4rD2NeiFxAoj210pyR4OzsbLwjs1vclqEAzPHh+r66IFuV0 Udg=
b.ns.se. 172800 IN RRSIG A 5 3 172800 20120927063649 20120913021101 58656 se. U8gZpgfj2wCWMrSgnKLyR9VPRyiojP4lGHWlSpeyvu3KTZBSzU7Xw/tu QWORTwjxBkdgTSXNcKJDkQPe8PkMKzPj/aB6w5dU/QXx7fdyGBYHqlC 2nbc5IliG6+/
aV2Eg5T5LiRj2+RWJnQWxyh6TxtccKa5SdZ8aVz+bMGw IlE=
c.ns.se. 172800 IN RRSIG A 5 3 172800 20120925203628 20120913081101 58656 se. oqrUBu72ccG3moTYF8mENrp0d3D/n0Z9GX3tHLpu3+kckgAZEMahYeB3 VhESvysenqXHy9K++STBH/c/BpZJnOnV109mctZX691/NC7A0cUWk8cE
v2PYkSkRATryT2V4soJWbX1kGrc40UMLatqh6gY7tJPLvnkgeXOu1Fy8 Rjo=
d.ns.se. 172800 IN RRSIG A 5 3 172800 20120925050254 20120912181102 58656 se. CqEp4MhqEMzW+Tvg5wTSly/zqMoFBKNvIwr1590yShYfhtLQpXxKquLe IlHtXbY+kSaA8nKw7rhPGI06QRbW8FYYlWyP/3KSoBsVTr+ZZ19A+1wd
dK20GMC6SjAKRU4HE4vVFSZJm5lvtm5RPSzQxIT19tCwNc1Ggj5ZYaAV uj4=
e.ns.se. 172800 IN RRSIG A 5 3 172800 20120926152155 20120913021101 58656 se. qoZASSLoC2MN0bxYc8eTNWjNAlbhSzTyKgBbj4akMDyRQxTeA+YtdURZ lf/5gvDjOOE7yNojuuAzHD8g+dyn5Z7cgmjLIyilo59huDUkSO0bQZsz
PBLouj9+7NMt2Q5tILJG2a9+BRFpsIE+nAxXMQRpldqJ2l+Zde+DNLU/ XTI=
f.ns.se. 172800 IN RRSIG A 5 3 172800 20120926062907 20120913041101 58656 se. kzQMEZB1F5KX06I0TrKgcqKC8Nip3J5/FyTR0O86TdffnIKjQ4Eg83/u yP1kr1LNxCKp8BFHbQKwb50WbxCW0V/BBfWU6L2jeJxz5N1r+zvCzC0v
4AnfNQhJtE3jR6d6RG4DCurkAheFcaPZtmEbYu+jaZi3xLTcw+jEQIE+ d+A=
g.ns.se. 172800 IN RRSIG A 5 3 172800 20120923205729 20120910221101 58656 se. h/pT8oAz0YJI7kN7u1Ez6EGFyco56yFNEOJn0lUuJlaKXoiCWxpa4GoV sWMUQOkffPpfZbOqZf8srgQjKmjhkJwGCn+detbGu9znamKVD1oaYbwG XT3Dn27XEBPVr0dwS5seddbKWCZm1O2v
MTl4cGp1wfuQrkmU9NfJs h0k=
g.ns.se. 172800 IN RRSIG AAAA 5 3 172800 20120924031728 20120910161101 58656 se. EIU7iR+eAlmNWeCGpLxE3998OWAyKOGsDnEgcGF9fyhcxFgw3sDB5kGR /iMGM12RhuK33S3u8te/KQ5DlByeR7Mfj+L7TJR4q1p4rwrxyl6WC45O 9wZRUtBZu/
Zv7UlvVOJDKzGdCaphqj5ey1LI14pyg8QsBPqH2KzbJ8WE VYU=
i.ns.se. 172800 IN RRSIG A 5 3 172800 20120926182411 20120912221101 58656 se. YrdQpeZ1iZKYAos1jw6tRrE6uO/jH/EqkgdW8k8BVJPlTQq66bwelEdn LDYTn7i8QoOJPPlNbiNjAJxXa15pLqIE2PLZdwq9Qzf3ytg04Tctn6FV 3P+fX7al6aZuzAjZnm6/
cBigP2s+Pq96xQbAaqTEqXid5MuKDk2k6NMd QCg=
i.ns.se. 172800 IN RRSIG AAAA 5 3 172800 20120924081359 20120911001101 58656 se. OBy/eN25dUM/kZMsY2oJb6R/VYrQmhPXt3Px401lr1HBv4YJ3HddW5fX ZHgO95CLHDMQX3VQf0zTvHeyKb5rqk/EtZwF6hk/1h6HL7FGytXlzGEb ABr/rU74yk6LU2aDJ5ThE0793dz8ijfj2F/
gu+WDpWP7zp3s+l9naiTM vE0=
j.ns.se. 172800 IN RRSIG A 5 3 172800 20120923152202 20120910141102 58656 se. hFM3pC0tgLGzik7ppcGQrtMDFXTxSKUGqTtbpRtTmEnRHzm3btpdtOg1 lG2YHyFaD/dIKA0wa9qQqjGaifQCc8xY+MkvqFU2MEO83F/tlgmSC+un bWrbytxCXhaKjaU2Zl5/Mk5GsfvB/
fNIBBPIZ5RbrohAbXUQlK6Uz44v yQA=

;; Query time: 126 msec
;; SERVER: 192.36.144.107#53(192.36.144.107)
;; WHEN: Thu Sep 13 06:20:08 2012

;; MSG SIZE rcvd: 4073

Privacy/Tracking Attacks

NMAP

Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

OS fingerprinting

subtle differences in implementations allows an attacker to determine OS and version numbers.

```
MacBook-Pro:p8 abhi$ sudo nmap -O localhost
Password:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-20 05:23 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 993 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
1025/tcp  open  NFS-or-IIS
1080/tcp  open  socks
1110/tcp  open  nfsd-status
3000/tcp  open  ppp
8086/tcp  open  d-s-n
49161/tcp open  unknown
Device type: general purpose
Running: Apple macOS 10.14.X
OS CPE: cpe:/o:apple:mac_os_x:10.14
OS details: Apple macOS 10.14 (Mojave) (Darwin 18.2.0 - 18.6.0)
Network Distance: 0 hops
```

```
MacBook-Pro:p8 abhi$ sudo lsof -i | grep LISTEN
launchd       1            root    7u  IPv6 0x12effbdaed1c4d9f      0t0    TCP *:ssh (LISTEN)
launchd       1            root    8u  IPv4 0x12effbdae8e89237      0t0    TCP *:ssh (LISTEN)
launchd       1            root   10u  IPv6 0x12effbdaed1c4d9f      0t0    TCP *:ssh (LISTEN)
launchd       1            root   11u  IPv4 0x12effbdae8e89237      0t0    TCP *:ssh (LISTEN)
UploadDae   482 panopto_upload    7u  IPv4 0x12effbdb01813e27      0t0    TCP localhost:49220 (LIST
UploadDae   482 panopto_upload    8u  IPv6 0x12effbdaed1c671f      0t0    TCP localhost:49220 (LIST
rapportd    552            abhi    4u  IPv4 0x12effbdaed2c9c3f      0t0    TCP *:64496 (LISTEN)
rapportd    552            abhi    5u  IPv6 0x12effbdb050f873f      0t0    TCP *:64496 (LISTEN)
DashlaneA   660            abhi    7u  IPv4 0x12effbdaf4b42647      0t0    TCP localhost:49161 (LIST
DashlaneP   790            abhi   12u  IPv4 0x12effbdae7a2304f      0t0    TCP localhost:11456 (LIST
BlueJeans  1138            abhi    3u  IPv4 0x12effbdb0269d237      0t0    TCP localhost:18171 (LIST
IPNExtens  1159            abhi   13u  IPv4 0x12effbdaf4b4304f      0t0    TCP localhost:49340 (LIST
Adobe\x20  1231            abhi   14u  IPv4 0x12effbdaed2c882f      0t0    TCP localhost:15292 (LIST
java      28404            abhi   35u  IPv6 0x12effbdaea0cf3df      0t0    TCP *:blackjack (LISTEN)
java      28404            abhi   36u  IPv6 0x12effbdaf6dfba7f      0t0    TCP *:nfsd-status (LISTEN
java      28404            abhi   37u  IPv6 0x12effbdb0322f3df      0t0    TCP *:imyx (LISTEN)
java      28404            abhi   38u  IPv6 0x12effbdaf2fc6d7f      0t0    TCP *:socks (LISTEN)
java      28404            abhi   39u  IPv6 0x12effbdaf2fc40df      0t0    TCP *:iclpv-dm (LISTEN)
com.docke 49813            abhi   89u  IPv6 0x12effbdaf418d3ff      0t0    TCP *:8086 (LISTEN)
com.docke 49813            abhi  120u  IPv6 0x12effbdaed1c60bf      0t0    TCP *:hbci (LISTEN)
com.docke 49847            abhi   24u  IPv4 0x12effbdaf324e647      0t0    TCP *:62762 (LISTEN)
hugo      50331            abhi 1406u  IPv4 0x12effbdaf6f49c3f      0t0    TCP localhost:bmc_patrolc
```

Network Anonymity

My browser essentially determines my identity.

http://panopticlick.eff.org/index.php

Your browser fingerprint **appears to be unique** among the 2,407,421 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 21.2 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in **this article**.

Help us increase our sample size:

SYSTEM FONTS. 1 in 2407421 have this set of fonts.

Adobe Caslon Bold Alternate, Adobe Caslon Bold Italic Alternate, Adobe Caslon Italic Alternate, Adobe Caslon Regular Alternate, Adobe Caslon Semibold Alternate, Adobe Caslon Semibold Italic Alternate, Adobe Caslon Bold, Adobe Caslon Bold Italic, Adobe Caslon Bold Oldstyle Figures, Adobe Caslon Bold Oldstyle Figures, Adobe Caslon Italic, Adobe Caslon Italic Oldstyle Figures, Adobe Caslon Ornaments, Adobe Caslon Regular, Adobe Caslon Regular Small Caps & Oldstyle Figures, Adobe Caslon Semibold, Adobe Caslon Semibold Italic, Adobe Caslon Semibold Italic Oldstyle Figures, Adobe Caslon Semibold Small Caps & Oldstyle Figures, Adobe Caslon Bold Italic Swash, Adobe Caslon Italic Swash, Adobe Caslon Semibold Italic Swash, Adobe Caslon Bold Expert, Adobe Caslon Bold Italic Expert, Adobe Caslon Italic Expert, Adobe Caslon Regular Expert, Adobe Caslon Semibold Expert, Adobe Caslon Semibold Italic Expert, Adobe Caslon Pro TNY, Adobe Caslon Pro TNY Italic, Adobe Caslon Pro TNY Bold, Adobe Caslon Pro TNY Bold Italic, Adobe Garamond Bold, Adobe Garamond Bold Italic, Adobe Garamond Bold Italic Oldstyle Figures, Adobe Garamond Bold Oldstyle Figures, Adobe Garamond Italic, Adobe Garamond Regular, Adobe Garamond Small Caps & Oldstyle Figures, Adobe Garamond Semibold, Adobe Garamond Semibold Italic, Adobe Garamond Semibold Italic Oldstyle Figures, Adobe Garamond Semibold Small Caps & Oldstyle Figures, Adobe Garamond Titling Capitals, Adobe Garamond Bold Expert, Adobe Garamond Bold Italic Expert, Adobe Garamond Italic Expert, Adobe Garamond Regular Expert, Adobe Garamond Semibold Expert, Adobe Garamond Semibold Italic Expert, Abadi MT Condensed Extra Bold, Abadi MT Condensed Light, Al Bayan Plain, Al Bayan Bold, American Typewriter, American Typewriter Bold, American Typewriter Condensed, American Typewriter Condensed Bold, American Typewriter Condensed Light, American Typewriter Light, Amputa, Andale Mono, Apple Chancery, Apple Braille, Apple Braille Outline 6 Dot, Apple Braille Outline 8 Dot, Apple Braille Pinpoint 6 Dot, Apple Braille Pinpoint 8 Dot, Apple Color Emoji, AppleGothic Regular, AppleMyungjo Regular, Apple SD Gothic Neo Bold, Apple SD GothicNeo ExtraBold, Apple SD Gothic Neo Heavy, Apple SD Gothic Neo Light, Apple SD Gothic Neo Medium, Apple SD Gothic Neo Regular, Apple SD Gothic Neo SemiBold, Apple SD Gothic Neo Thin, Apple SD Gothic Neo UltraLight, Apple Symbols, Arial Black, Arial Bold Italic, Arial Bold, Arial Italic, Arial Hebrew, Arial Hebrew Bold, Arial, Arial Narrow, Arial Narrow Bold, Arial Narrow Bold Italic, Arial Narrow Italic, Arial Rounded MT Bold, Arial Unicode MS, Avenir Black, Avenir Black Oblique, Avenir Book, Avenir Book Oblique, Avenir Heavy, Avenir Heavy Oblique, Avenir Light, Avenir Light Oblique, Avenir Medium, Avenir Medium Oblique, Avenir Oblique, Avenir Roman, Avenir Next Bold, Avenir Next Bold Italic, Avenir Next Demi Bold, Avenir Next Demi Bold Italic, Avenir Next Heavy, Avenir Next Heavy Italic, Avenir Next Italic, Avenir Next Medium, Avenir Next Medium Italic, Avenir Next Regular, Avenir Next Ultra Light, Avenir Next Ultra Light Italic, Avenir Next Condensed Bold, Avenir Next Condensed Bold Italic, Avenir Next Condensed Demi Bold, Avenir Next Condensed Demi Bold Italic, Avenir Next Condensed Heavy, Avenir Next Condensed Heavy Italic, Avenir Next Condensed Italic, Avenir Next Condensed Medium, Avenir Next Condensed Medium Italic, Avenir Next Condensed Regular, Avenir Next Condensed Ultra Light, Avenir Next Condensed Ultra Light Italic, Ayuthaya, Baghdad, Bangla MN, Bangla MN Bold, Bangla Sangam MN, Bangla Sangam MN Bold, Baskerville Old Face, Baskerville, Baskerville Bold, Baskerville Bold Italic, Baskerville Italic, Baskerville SemiBold, Baskerville SemiBold Italic, Batang, Bauhaus 93, Bell MT, Bell MT Bold, Bell MT Italic, Bernard MT Condensed, Big Caslon Medium, Blackout Midnight, Book Antiqua, Book Antiqua Bold, Book Antiqua Bold Italic, Book Antiqua Italic, Bookman Old Style, Bookman Old Style Bold, Bookman Old Style Bold Italic, Bookman Old Style Italic, Bookshelf Symbol 7, Braggadocio, Britannic Bold, Brush Script MT Italic, Calibri, Calibri Bold, Calibri Bold Italic, Calibri Italic, Calisto MT Bold, Calisto MT, Calisto MT Bold Italic, Calisto MT Italic, Cambria, Cambria Bold, Cambria Bold Italic, Cambria Italic, Cambria Math, Candara, Candara Bold, Candara Bold Italic, Candara Italic, Century, Century Gothic, Century Gothic Bold, Century Gothic Bold Italic, Century Gothic Italic, Century Schoolbook, Century Schoolbook Bold, Century Schoolbook Bold Italic, Century Schoolbook Italic, Chalkboard, Chalkboard Bold, Chalkboard SE Bold, Chalkboard SE Light, Chalkboard SE Regular, Chalkduster, Charcoal CY, Cochin, Cochin Bold, Cochin Bold Italic, Cochin Italic, Colonna MT, Comic Sans MS, Comic Sans MS Bold, Consolas, Consolas Bold, Consolas Bold Italic, Consolas Italic, Constantia, Constantia Bold, Constantia Bold Italic, Constantia Italic, Cooper Black, CopperanAChoco, CopperanCreamAI, Copperplate, Copperplate Bold, Copperplate Light, Copperplate Gothic Bold, Copperplate Gothic Light, Corbel, Corbel Bold, Corbel Bold Italic, Corbel Italic, Corsiva Hebrew, Corsiva Hebrew Bold, Courier, Courier Bold, Courier Bold Oblique, Courier Oblique, Courier New Bold Italic, Courier New Bold, Courier New Italic, Curlz MT, BiauKai, Damascus, Damascus Bold, DecoType Naskh, Delicious-Bold, Delicious-BoldItalic, Delicious-Heavy, Delicious-Italic, Delicious-Roman, Delicious-SmallCaps, Desdemona, Devanagari MT, Devanagari MT Bold, Devanagari Sangam MN, Devanagari Sangam MN Bold, Didot, Didot Bold, Didot Italic, Digital-7, District Thin, Dubtronic Solid, Dubtronic Inline, Edwardian Script ITC, Engravers MT, Engravers MT Bold, Euphemia UCAS, Euphemia UCAS Bold, Euphemia UCAS Italic, Eurostile Bold, Eurostile, Fontin Bold, Fontin Italic, Fontin Regular, Fontin SmallCaps, Footlight MT Light, Franklin Gothic Book, Franklin Gothic Book Italic, Franklin Gothic Medium, Franklin Gothic Medium Italic, Futura Book, Futura Condensed ExtraBold, Futura Condensed Medium, Futura Medium, Futura Medium Italic, GB18030 Bitmap, Gabriola, Garamond, Garamond Bold, Garamond Italic, Geeza Pro, Geeza Pro Bold, Geneva, Geneva CY, Georgia, Georgia Bold, Georgia Bold Italic, Georgia Italic, Gill Sans, Gill Sans Bold, Gill Sans Bold Italic, Gill Sans Italic, Gill Sans Light, Gill Sans Light Italic, Gill Sans Ultra Bold, Gill Sans MT, Gill Sans MT Bold, Gill Sans MT Bold Italic, Gill Sans MT Italic, Gloucester MT Extra Condensed, Goudy Old Style Bold, Goudy Old Style Italic, Goudy Old Style, Gujarati MT, Gujarati MT Bold, Gujarati Sangam MN, Gujarati Sangam MN Bold, Gulim, Gurmukhi MN, Gurmukhi MN Bold, Gurmukhi Sangam MN, Gurmukhi Sangam MN Bold, Haettenschweiler, Harrington, Helvetica, Helvetica Bold, Helvetica Bold Oblique, Helvetica Light, Helvetica Light Oblique, Helvetica Oblique, Helvetica CY Bold, Helvetica CY Bold Oblique, Helvetica CY Oblique, Helvetica CY Plain, Helvetica Neue, Helvetica Neue Bold, Helvetica Neue Bold Italic, Helvetica Neue Condensed Black, Helvetica Neue Condensed Bold, Helvetica Neue Italic, Helvetica Neue Light, Helvetica Neue Light Italic, Helvetica Neue Medium, Helvetica Neue UltraLight, Helvetica Neue UltraLight Italic, Herculanum, Hiragino Kaku Gothic Pro W3, Hiragino Kaku Gothic Pro W6, Hiragino Kaku Gothic ProN W3, Hiragino Kaku Gothic ProN W6, Hiragino Kaku Gothic Std W8, Hiragino Kaku Gothic StdN W8, Hiragino Maru Gothic Pro W4, Hiragino Maru Gothic ProN W4, Hiragino Mincho Pro W3, Hiragino Mincho Pro W6, Hiragino Mincho ProN W3, Hiragino Mincho ProN W6, Hiragino Sans GB W3, Hiragino Sans GB W6, Hoefler Text Black, Hoefler Text Black Italic, Hoefler Text Italic, Hoefler Text Ornaments, Hoefler Text, Hydroplane Regular, Impact, Imprint MT Shadow, InaiMathi, HeadLineA Regular, PilGi Regular, GungSeo Regular, PCMyungjo Regular, Kailasa Regular, Kannada MN, Kannada MN Bold, Kannada Sangam MN, Kannada Sangam MN Bold, Kefa Bold, Kefa Regular, Khmer MN, Khmer MN Bold, Khmer Sangam MN, Kino MT, Kokonor Regular, Krungthep, KufiStandardGK, Latin Modern Mono 10 Italic, Latin Modern Mono 10 Regular, Latin Modern Mono 12 Regular, Latin Modern Mono 8 Regular, Latin Modern Mono 9 Regular, Latin Modern Mono Caps 10 Oblique, Latin Modern Mono Caps 10 Regular, Latin Modern Mono Light 10 Bold, Latin Modern Mono Light 10 Bold Oblique, Latin Modern Mono Light 10 Oblique, Latin Modern Mono Light 10 Regular, Latin Modern Mono Light Cond 10 Oblique, Latin Modern Mono Light Cond 10 Regular, Latin Modern Mono Prop 10 Oblique, Latin Modern Mono Prop 10 Regular, Latin Modern Mono Prop Light 10 Bold, Latin Modern Mono Prop Light 10 BoldOblique, Latin Modern Mono Prop Light 10 Oblique, Latin Modern Mono Prop Light 10 Regular, Latin Modern Mono Slanted 10 Regular, Latin Modern Roman 10 Bold, Latin Modern Roman 10 Bold Italic, Latin Modern Roman 10 Italic, Latin Modern Roman 10 Regular, Latin Modern Roman 12 Bold, Latin Modern Roman 12 Italic, Latin Modern Roman 12 Regular, Latin Modern Roman 17 Regular, Latin Modern Roman 5 Bold, Latin Modern Roman 5 Regular, Latin Modern Roman 6 Bold, Latin Modern Roman 6 Regular, Latin Modern Roman 7 Bold, Latin Modern Roman 7 Italic, Latin Modern Roman 7 Regular, Latin Modern Roman 8 Bold, Latin Modern Roman 8 Italic, Latin Modern Roman 8 Regular, Latin Modern Roman 9 Bold, Latin Modern Roman 9 Italic, Latin Modern Roman 9 Regular, Latin Modern Roman Caps 10 Oblique, Latin Modern Roman Caps 10 Regular, Latin Modern Roman Demi 10 Oblique, Latin Modern Roman Demi 10 Regular, Latin Modern Roman Dunhill 10 Oblique, Latin Modern Roman Dunhill 10 Regular, Latin Modern Roman Slanted 10 Bold, Latin Modern Roman Slanted 10 Regular, Latin Modern Roman Slanted 12 Regular, Latin Modern Roman Slanted 17 Regular, Latin Modern Roman Slanted 8 Regular, Latin Modern Roman Slanted 9 Regular, Latin Modern Roman Unslanted 10 Regular, Latin Modern Sans 10 Bold, Latin Modern Sans 10 Bold Oblique, Latin Modern Sans 10 Oblique, Latin Modern Sans 10 Regular, Latin Modern Sans 12 Oblique, Latin Modern Sans 12 Regular, Latin Modern Sans 17 Oblique, Latin Modern Sans 17 Regular, Latin Modern Sans 8 Oblique, Latin Modern Sans 8 Regular, Latin Modern Sans 9 Oblique, Latin Modern Sans 9 Regular, Latin Modern Sans Demi Cond 10 Oblique, Latin Modern Sans Demi Cond 10 Regular, Latin Modern Sans Quotation 8 Bold, Latin Modern Sans Quotation 8 Bold Oblique, Latin Modern Sans Quotation 8 Oblique, Latin Modern Sans Quotation 8 Regular, Lao MN, Lao MN Bold, Lao Sangam MN, Wide Latin, League Gothic, Apple LiGothic Medium, LiHei Pro, LiSong Pro, Apple LiSung Light, Lot, Lucida Blackletter, Lucida Bright, Lucida Bright Demibold, Lucida Bright Demibold Italic, Lucida Bright Italic, Lucida Calligraphy Italic, Lucida Console, Lucida Fax Regular, Lucida Fax Demibold, Lucida Fax Demibold Italic, Lucida Fax Italic, Lucida Grande, Lucida Grande Bold, Lucida Handwriting Italic, Lucida Sans Regular, Lucida Sans Demibold Roman, Lucida Sans Demibold Italic, Lucida Sans Italic, Lucida Sans Typewriter Regular, Lucida Sans Typewriter Bold, Lucida Sans Typewriter Bold Oblique, Lucida Sans Typewriter Oblique, Lucida Sans Unicode, MS Gothic, MS Mincho, MS PGothic, MS PMincho, MS Reference Sans Serif, MS Reference Specialty, MT Extra, Malayalam MN, Malayalam MN Bold, Malayalam Sangam MN, Malayalam Sangam MN Bold, Marion Bold, Marion Italic, Marion Regular, Marker Felt Thin, Marker Felt Wide, Marlett, MathJax_Math-Italic, Matura MT Script Capitals, Meiryo, Meiryo Bold, Meiryo Bold Italic, Meiryo Italic, Menlo Bold, Menlo Bold Italic, Menlo Italic, Menlo Regular, Microsoft Yi Baiti, Microsoft Himalaya, Microsoft Sans Serif, Microsoft Tai Le, Microsoft Tai Le Bold, MingLiU_HKSCS-ExtB, MingLiU_HKSCS, MingLiU, MingLiU-ExtB, Minion Black, Minion Bold, Minion Bold Italic, Minion Italic Display, Minion Regular Display, Minion Italic, Minion Regular, Minion Semibold, Minion Semibold Italic, Mistral, Modern No. 20, Molot, Monaco, Mongolian Baiti, Monotype Corsiva, Gurmukhi MT, Monotype Sorts, Mshtakan, Mshtakan Bold, Mshtakan BoldOblique, Mshtakan Oblique, Myanmar MN, Myanmar MN Bold, Myanmar Sangam MN, Myriad MM, Myriad MM Italic, NYIrvinEMAC, Nadeem, Nanum Brush Script, NanumGothic Bold, NanumGothic ExtraBold, NanumMyeongjo, NanumMyeongjo Bold, NanumMyeongjo ExtraBold, Nanum Pen Script, New Peninim MT, New Peninim MT Bold, New Peninim MT Bold Inclined, New Peninim MT Inclined, News Gothic MT, News Gothic MT Bold, News Gothic MT Italic, Noteworthy Bold, Noteworthy Light, Omnes Black, Omnes Black Italic, Omnes Bold, Omnes Bold Italic, Omnes ExtraLight, Omnes ExtraLight Italic, Omnes Hairline, Omnes Hairline Italic, Omnes Light, Omnes Light Italic, Omnes Medium, Omnes Medium Italic, Omnes Regular, Omnes Regular Italic, Omnes Semibold, Omnes Semibold Italic, Omnes Thin, Omnes Thin Italic, Onyx, Optima Bold, Optima Bold Italic, Optima ExtraBlack, Optima Italic, Optima Regular, Orbitron Black, Orbitron Bold, Orbitron Light, Orbitron Medium, Oriya MN, Oriya MN Bold, Oriya Sangam MN, Oriya Sangam MN Bold, Osaka, Osaka-Mono, PMingLiU, PMingLiU-ExtB, PT Sans Bold, PT Sans Bold Italic, PT Sans Caption, PT Sans Caption Bold, PT Sans Italic, PT Sans Narrow, PT Sans Narrow Bold, PT Sans, Palatino Bold, Palatino Bold Italic, Palatino Italic, Palatino, Palatino Linotype Bold, Palatino Linotype Bold Italic, Palatino Linotype Italic, Palatino Linotype, Papyrus, Papyrus Condensed, Pasion, Perpetua, Perpetua Bold, Perpetua Bold Italic, Perpetua Italic, Perpetua Titling MT Bold, Perpetua Titling MT Light, PicoSuperUltraBold, Pincoyablack Black, Plantagenet Cherokee, Playbill, Raanana, Raanana Bold, Rockwell, Rockwell Bold, Rockwell Bold Italic, Rockwell Extra Bold, Rockwell Italic, Hei Regular, Kai Regular, STFangsong, STHeiti, Heiti SC Light, Heiti SC Medium, Heiti TC Light, Heiti TC Medium, STXIGeneral-Bold, STXIGeneral-BoldItalic, STXIGeneral-Italic, STXIGeneral-Regular, STIXIntegralsD-Bold, STIXIntegralsD-Regular, STIXIntegralsSm-Bold, STIXIntegralsSm-Regular, STIXIntegralsUp-Bold, STIXIntegralsUp-Regular, STIXIntegralsUpD-Bold, STIXIntegralsUpD-Regular, STIXIntegralsUpSm-Bold, STIXIntegralsUpSm-Regular, STIXNonUnicode-Bold, STIXNonUnicode-BoldItalic, STIXNonUnicode-Italic, STIXNonUnicode-Regular, STIXSizeFiveSym-Regular, STIXSizeFourSym-Bold, STIXSizeFourSym-Regular, STIXSizeOneSym-Bold, STIXSizeOneSym-Regular, STIXSizeThreeSym-Bold, STIXSizeThreeSym-Regular, STIXSizeTwoSym-Bold, STIXSizeTwoSym-Regular, STIXVariants-Bold, STIXVariants-Regular, STKaiti, Kaiti SC Black, Kaiti SC Bold, Kaiti SC Regular, STSong, Songti SC Black, Songti SC Bold, Songti SC Light, Songti SC Regular, STXihei, Sabon LT Std Bold, Sabon LT Std Bold Italic, Sabon LT Std Italic, Sabon LT Std Roman, Sathu, Silom, SimHei, SimSun, SimSun-ExtB, Sinhala MN, Sinhala MN Bold, Sinhala Sangam MN, Sinhala Sangam MN Bold, Skia Regular, Skia Regular Black, Skia Regular Bold, Skia Regular Condensed, Skia Regular Extended, Skia Regular Light, Skia Regular Light Condensed, Skia Regular Light Extended, Skia Regular Medium, Skia Regular Medium Condensed, Skia Regular Medium Extended, Skia Regular Outline, Skia Regular Outline Condensed, Skia Regular Outline Extended, Skia Regular Raised, Skia Regular Raised Condensed, Skia Regular Raised Extended, Skia Regular Shadow, Skia Regular Shadow Condensed, Skia Regular Shadow Extended, Skia Regular Black Condensed, Skia Regular Black Extended, Skia Regular Bold Condensed, Skia Regular Bold Extended, Sliced AB , Stencil, Symbol, Tahoma, Tahoma Negreta, Tamil MN, Tamil MN Bold, Tamil Sangam MN, Tamil Sangam MN Bold, Telugu MN, Telugu MN Bold, Telugu Sangam MN, Telugu Sangam MN Bold, Thonburi, Thonburi Bold, Times Bold, Times Bold Italic, Times Italic, Times Roman, Times New Roman Bold Italic, Times New Roman Bold, Times New Roman Italic, Times New Roman, Trebuchet MS Bold Italic, Trebuchet MS, Trebuchet MS Bold, Trebuchet MS Italic, Tw Cen MT Bold, Tw Cen MT Bold Italic, Tw Cen MT Italic, Tw Cen MT, Verdana, Verdana Bold, Verdana Bold Italic, Verdana Italic, Webdings, Wingdings, Wingdings 2, Wingdings 3, Yanone Kaffeesatz Bold, Yanone Kaffeesatz Light, Yanone Kaffeesatz Regular, Yanone Kaffeesatz Thin, YoshiRule-Regular, Yuppy SC Regular, Yuppy TC Regular, Zag Bold, Zag Regular, Zapf Dingbats, Zapfino, advent Bd2, bubbleboddy Fat, bubbleboddy light Light (via Flash)

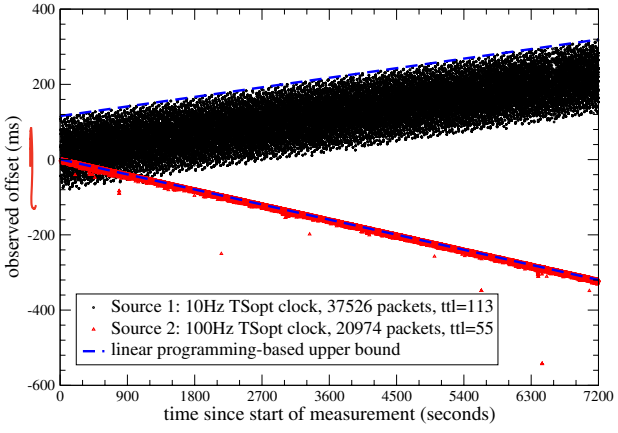


Figure 1. TSopt clock offset-sets for two sources in BB_N. Trace recorded on an OC-48 link of a U.S. Tier 1 ISP, 2004-04-28 19:30–21:30PDT. The source with the wide band has a 10 Hz TSopt clock, the source with the narrow band has a 100 Hz TSopt clock. A source with no clock skew would have a horizontal band.

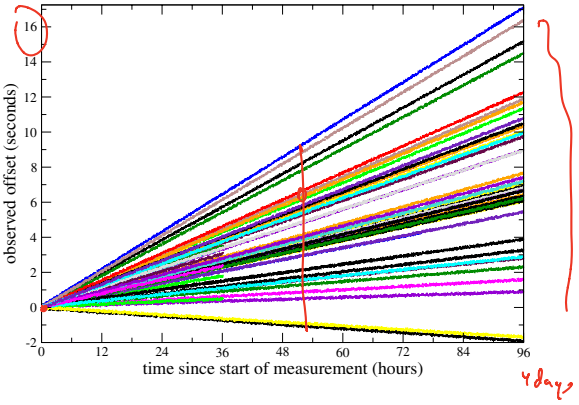
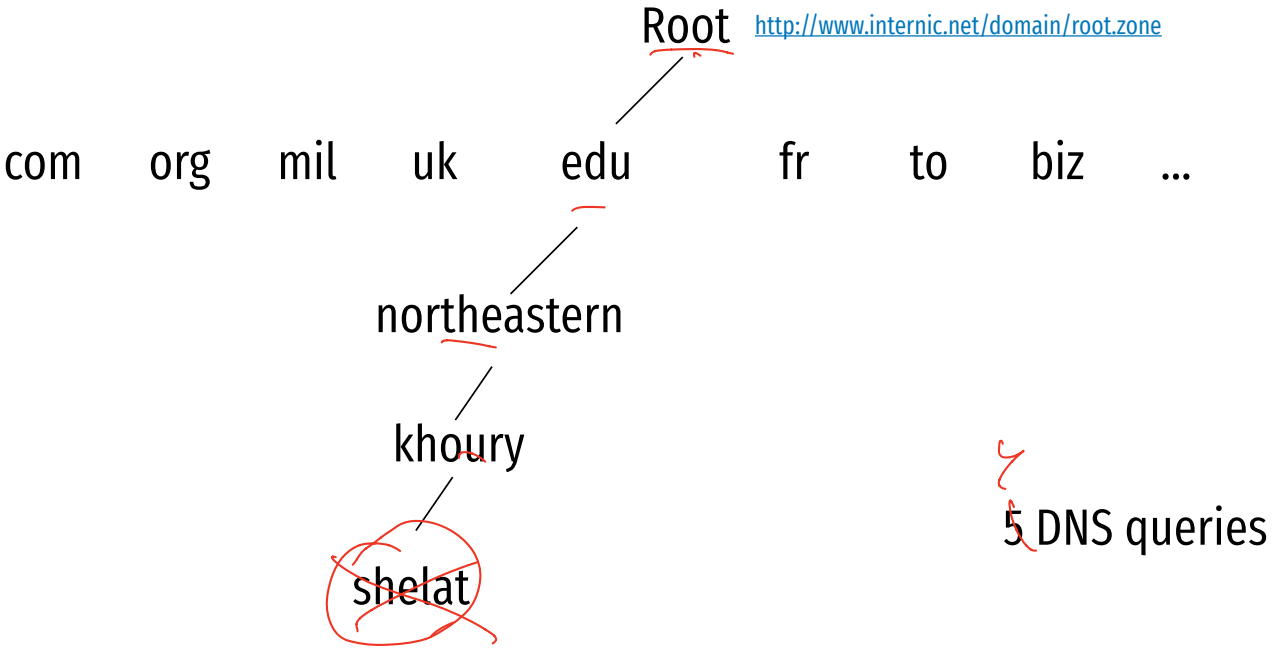


Figure 3. TSopt clock offset-sets for 69 Micron 448MHz Pentium II machines running Windows XP Professional SP1. Trace recorded on `host2`, three hops away, 2004-09-10 08:30PDT to 2004-09-14 08:30PDT.

Remote Physical Device Finterprinting [KBC05]

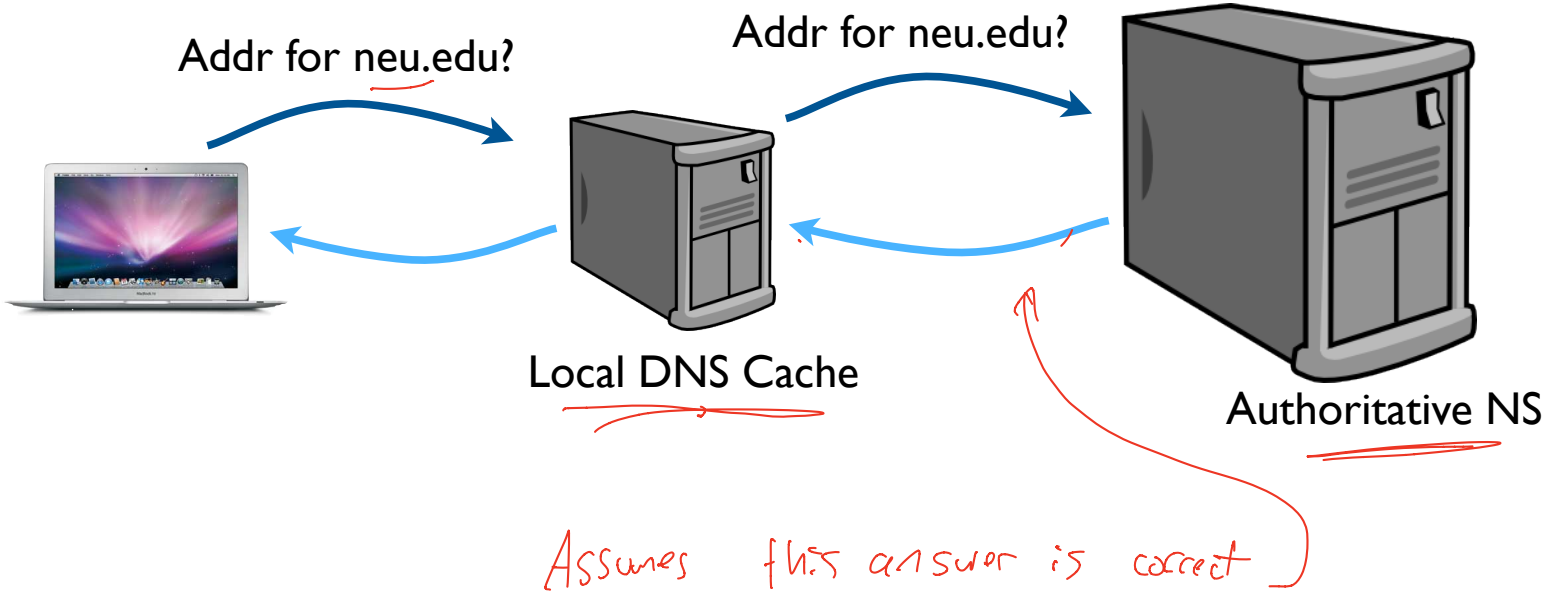
Remember DNS Query?



Cannot run DNS Query for EVERY URL!

Solution: cache it

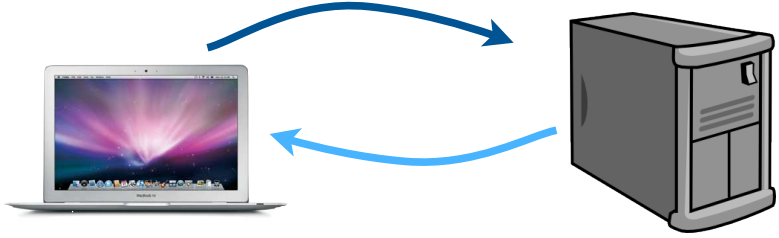
First time



http://www.clker.com/clipart-1826.html

Second time

Addr for neu.edu?



"I just looked that up.
The answer is 23.38.112.27"

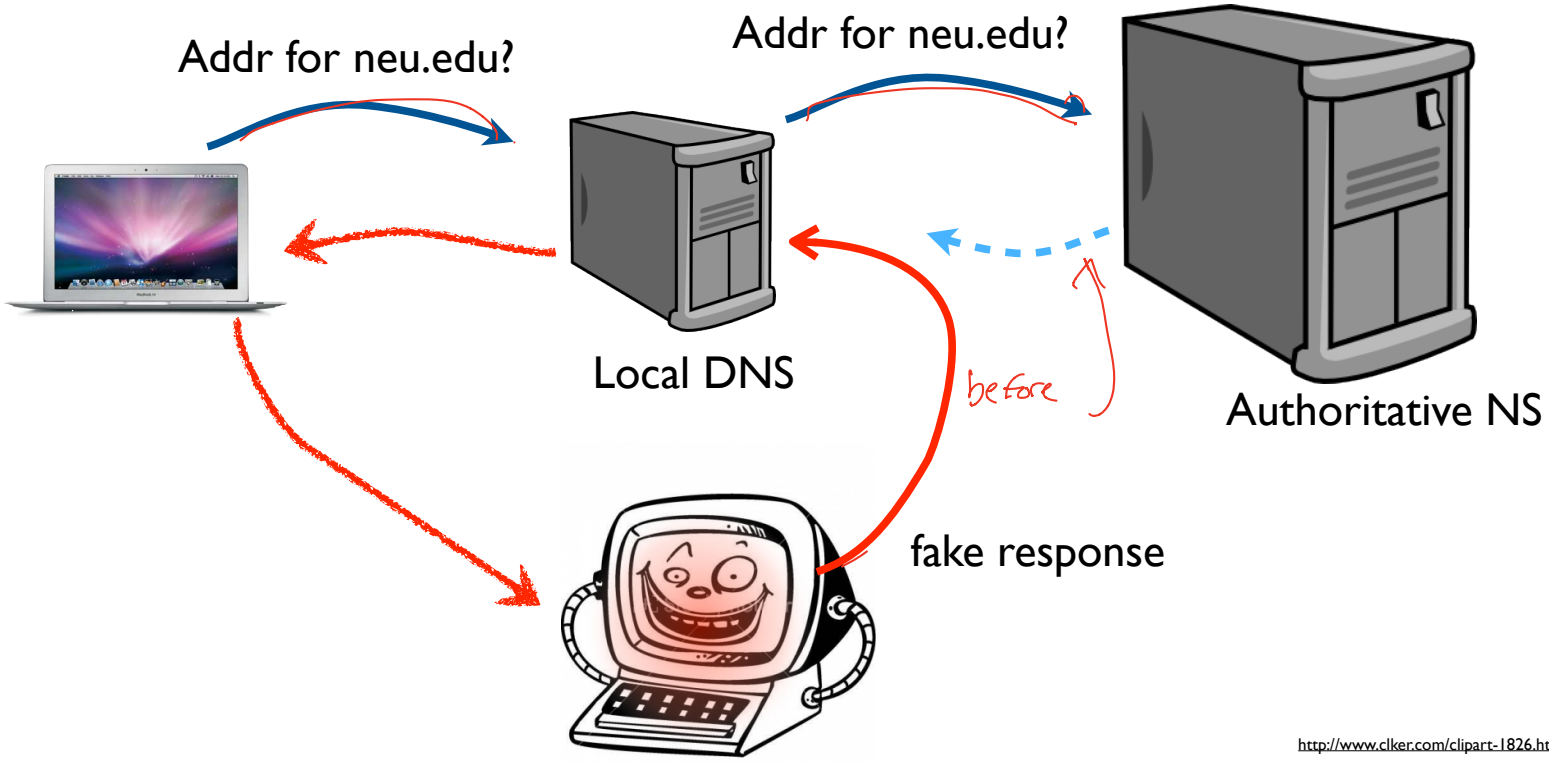
Local DNS Cache

http://www.clker.com/clipart-1826.html

Solution: cache it

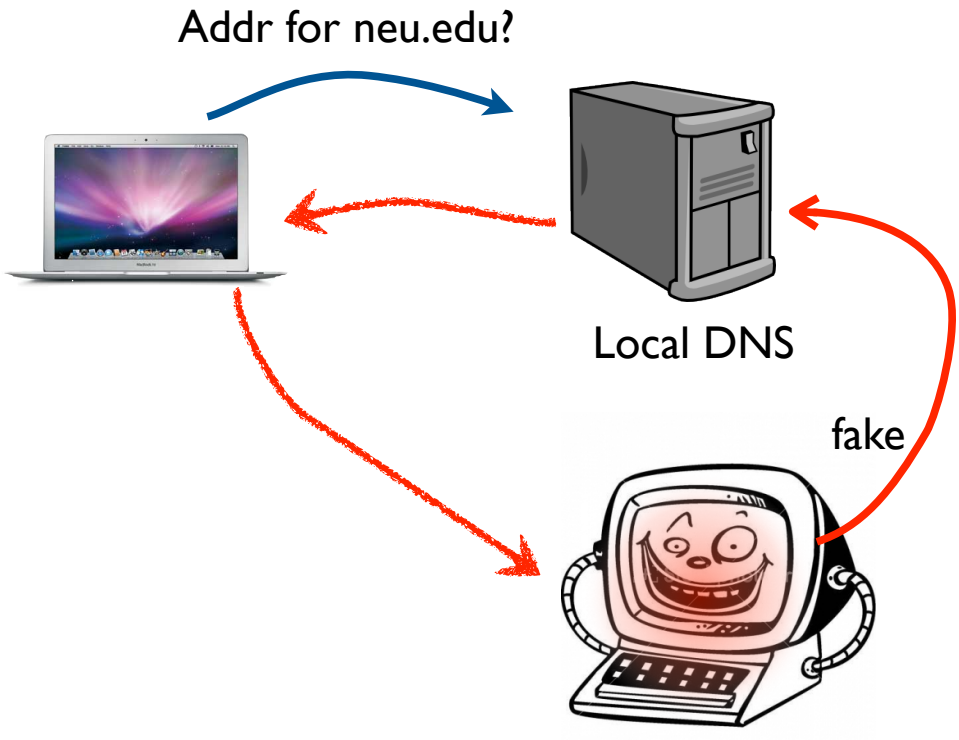
two small problems: AUTHENTICITY
AVAILABILITY

DNS Cache POISON



http://www.clker.com/clipart-1826.html

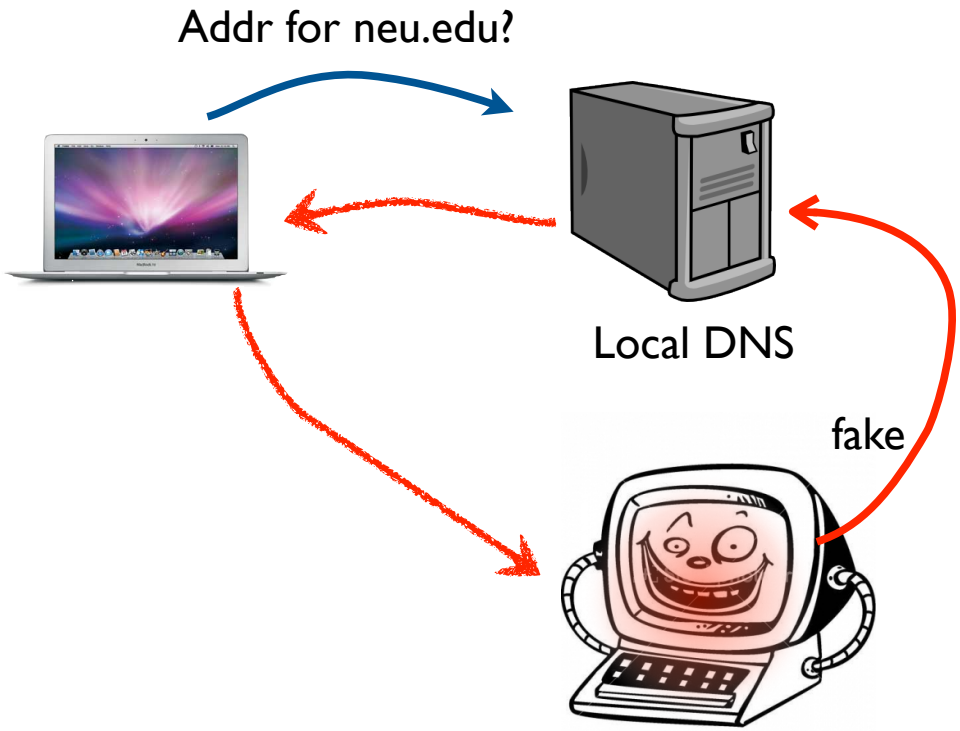
FAKE RESPONSE can:



provide the wrong answer for neu.edu

provide the wrong answer for other domains!

FAKE RESPONSE can:



provide the wrong answer for neu.edu

provide the wrong answer for other domains!

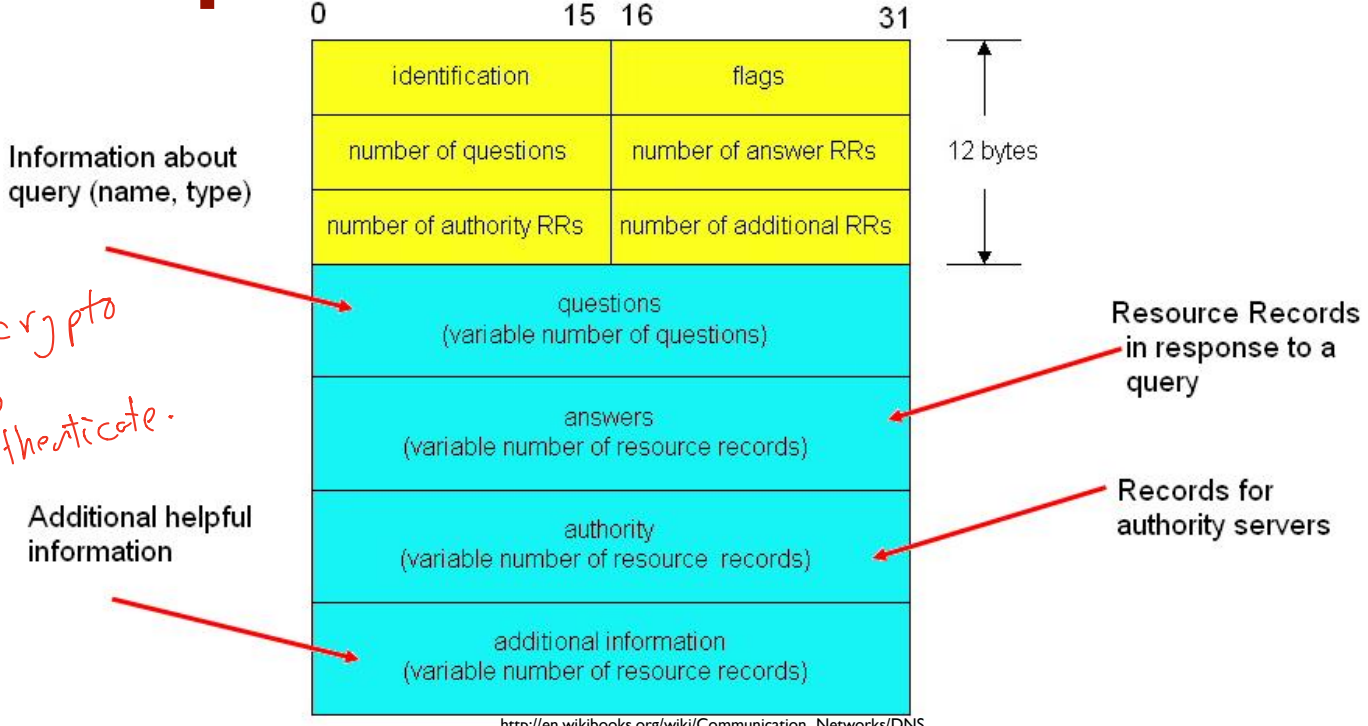
these responses can be cached for days!

they affect everyone else using that local DNS!

Attacker's fake response needs to APPEAR as a legitimate RESPONSE.

DNS packet UDP

2 fixes: DNSSec
DNS-over-https.



http://en.wikibooks.org/wiki/Communication_Networks/DNS

No crypto to authenticate.

Attacker's fake response needs to APPEAR as a legitimate RESPONSE and arrive FIRST.

Needs to GUESS: Query ID

UDP Port

Attacker makes one bogus website

<img src="http://bogus1.yahoo.com">

<img src="http://bogus2.yahoo.com">

<img src="http://bogus1000.yahoo.com">

A Network is a public resource.

If you are on the same network (WIFI), then sniffing makes DNS cache poison easy.

Guess is not necessary.

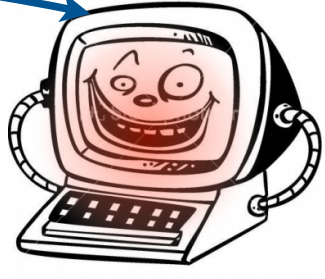
You can answer first.

Not on same network

webserver for freeipads.com

Not on same network

1. GET index.html



webserver for freeipads.com

2. Reply with page that has <img src=apple.com/...>

3. Reply with DNS entry for apple.com

so very quickly, and 100,000 times

Implementation detail of DNS

DNS ID has 65,536 possibilities.
Suppose the DNS lookup agent uses SEQUENTIALLY chosen ids.

Implementation detail of DNS

0. DNS lookup on freeipads.com

1. GET index.html

record the ID used in this request and respond with n+1 here

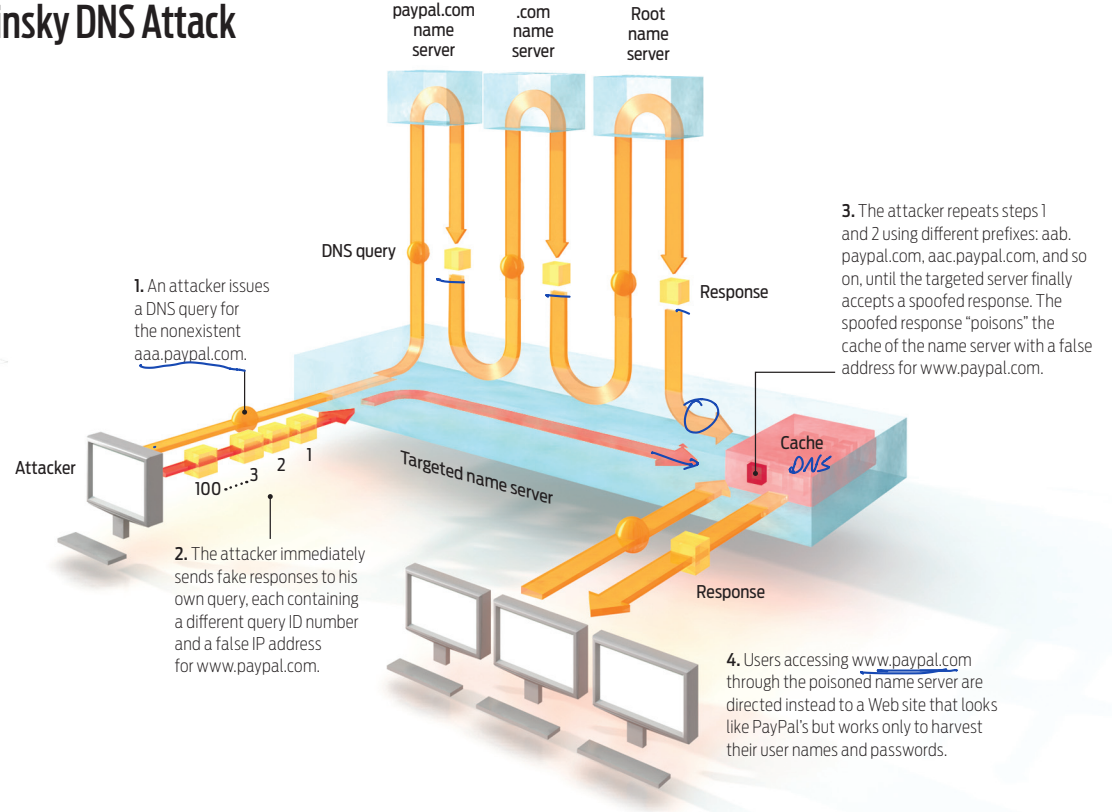
webserver/DNS for freeipads.com

2. Reply with page that has <img src=apple.com/...>

3. Reply with DNS entry for apple.com

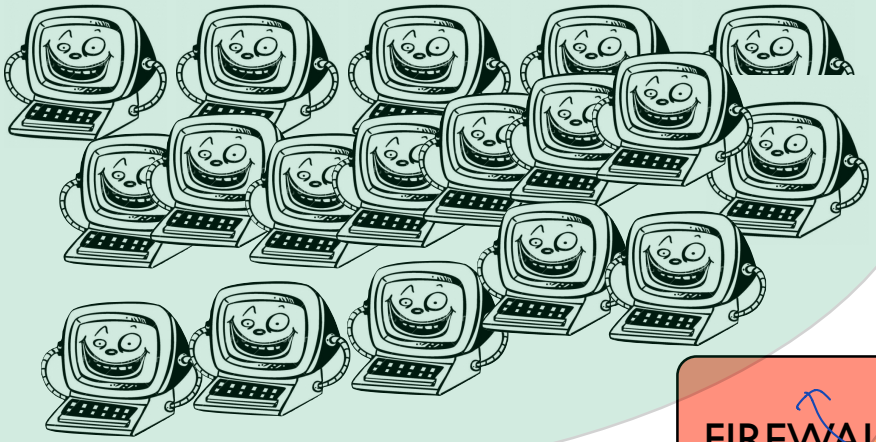
so very quickly, and 100,000 times

Kaminsky DNS Attack



http://spectrum.ieee.org/images/oct08/images/phish03.pdf

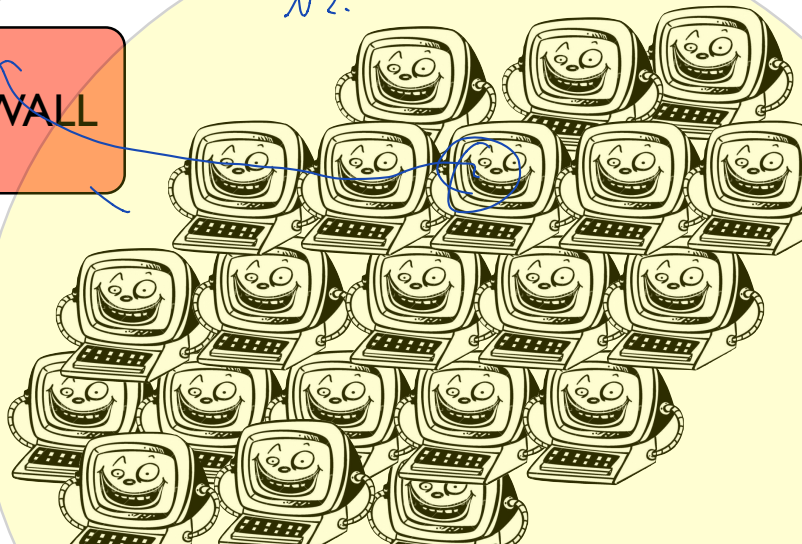
How to mitigate network attacks?



N1

FIREWALL

N2.



filter traffic between networks.

① DROP poorly formed packets

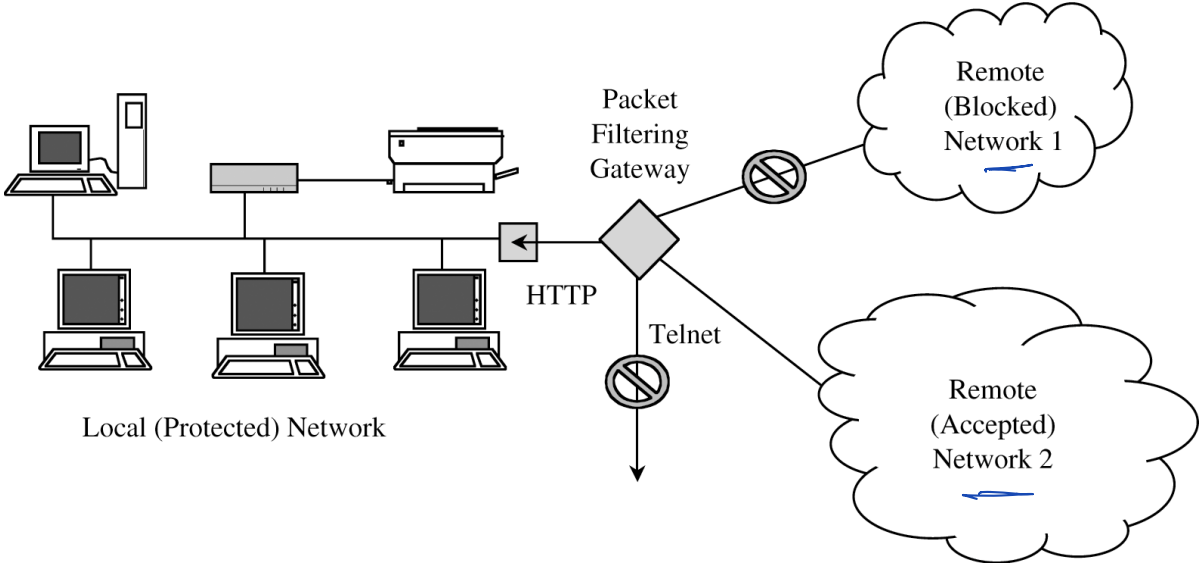
Firewalls

Stateless Packet Filter	Rules based on addr/port + header info
Statefull Packet Filter	above + state between each packet
Statefull Packet Inspection	above + can inspect the data of the package

StateLESS Packet Filter

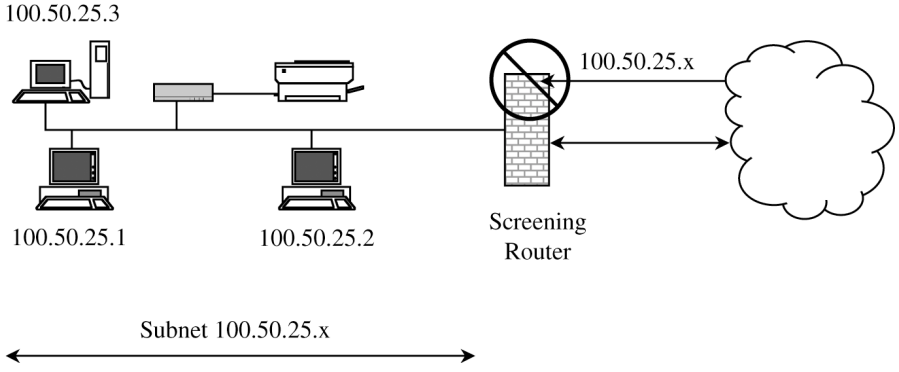
Rules based on addr/port + header info

Look at the packet and decide immediately whether to drop or forward.



•Local subnet has all traffic from remote network 1 blocks (say, network with IP address 253.128.x.x)

• Allow some traffic from Remote Network 2 (say, 253.127.x.x), but only if it is destined for port 80 (web-traffic), Drop all other ports



prevent external traffic from “spoofing” internal addresses.

StateFULL Packet Filter

Rules based on addr/port + header info

networks scans can be detected and stopped

detect invalid tcp packets

Statefull Packet Inspection

can filter for known attacks/shellcode