4. Network Attacks and Their Detection

Covert Channels, MitM, Poisoning, L7 threats

Simona Buchovecká, Tomáš Čejka

Faculty of Information Technology, CTU in Prague

simona.buchovecka@fit.cvut.cz, tomas.cejka@fit.cvut.cz

March 7, 2021

Section 1

Covert Channels, Tunneling

Covert Channels

Some definitions of a covert channel:

- a transmission channel that may be used to transfer data in a manner that violates security policy (Van Horenbeeck)
- a means of communication not normally intended to be used for communication (Zander, Armitage & Branch, 2007)
- a mechanism for sending and receiving information data between machines without alerting any firewalls and IDSs on the network (Buetler, 2008)

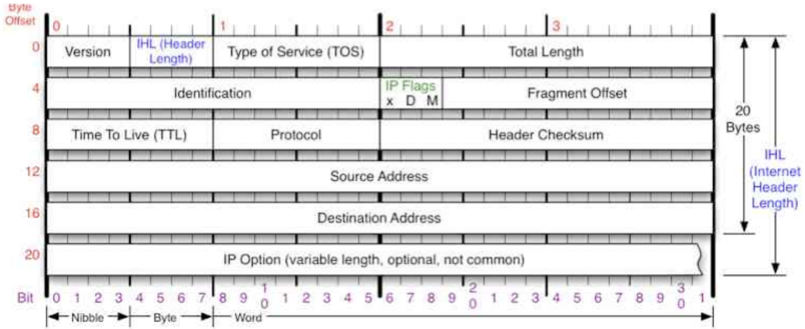
https://www.sans.org/reading-room/whitepapers/detection/covert-channels-33413

Motivation

- Exfiltrate data from an otherwise secure system
- Avoid detection of unauthorized access
- Malware communication — C&C channel hiding
- Circumvent filters which may be in place limiting their freedom of speech
- Bypass firewalls for unrestricted access to the web

Methods of Covert Data Encoding

- Header bit modulation
- Header bit crafting
- Optional header extension
- Temporal channels



Section 2

ICMP

ICMP Packet

IP Datagram

	Bits 0–7	**Bits 8–15**	**Bits 16–23**	**Bits 24–31**
IP Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Header (8 bytes)	Type of message	Code	Checksum	
	Header Data			
ICMP Payload (*optional*)	Payload Data			

ICMP Tunnelling I

No.	Time	Source	Destination	Protocol	Info	Packet Size
19	11:19:37.039393	10.2.240.197	10.2.240.195	ICMP	Echo (ping) request	770
20	11:19:37.039473	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	770
30	11:19:37.071352	10.2.240.197	10.2.240.195	ICMP	Echo (ping) request	770
31	11:19:37.071399	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	770
39	11:19:37.652033	[redacted].244.0.3	10.2.240.195	DNS	Standard query response CNAME www.l.google.com	192
43	11:19:37.653062	10.2.240.195	[redacted].85.227.147	HTTP	GET / HTTP/1.1	738
54	11:19:40.733100	[redacted].85.227.147	10.2.240.195	TCP	[TCP segment of a reassembled PDU]	1516
56	11:19:40.733240	[redacted].85.227.147	10.2.240.195	TCP	[TCP segment of a reassembled PDU]	1516
58	11:19:40.733870	[redacted].85.227.147	10.2.240.195	TCP	[TCP segment of a reassembled PDU]	1516
60	11:19:40.733941	[redacted].85.227.147	10.2.240.195	HTTP	HTTP/1.1 200 OK (text/html)	283
66	11:19:40.735795	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	1096
67	11:19:40.735906	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	1096
68	11:19:40.735983	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	1096
69	11:19:40.736059	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	1096
70	11:19:40.736134	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	1096
71	11:19:40.736209	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	1096
72	11:19:40.736306	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	1096
73	11:19:40.736381	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	1096
74	11:19:40.736479	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	1096
75	11:19:40.736552	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	1096
76	11:19:40.736633	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	1052
77	11:19:40.757953	10.2.240.197	10.2.240.195	ICMP	Echo (ping) request	850
78	11:19:40.758020	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	850
92	11:19:40.778930	10.2.240.197	10.2.240.195	ICMP	Echo (ping) request	964
93	11:19:40.778952	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	964
94	11:19:40.779003	10.2.240.197	10.2.240.195	ICMP	Echo (ping) request	850
95	11:19:40.779024	10.2.240.195	10.2.240.197	ICMP	Echo (ping) reply	850

ICMP Tunnelling II

```
0000  00 00 00 01 00 06 00 50  56 32 74 1c 00 00 08 00   ........P V2t.....
0010  45 00 02 f2 00 00 40 00  40 01 42 7e 0a 02 f0 c5   E.....@. @.B~....
0020  0a 02 f0 c3 08 00 59 f0  e5 ec 00 2e d5 20 08 80   ......Y. ..... ..
0030  00 00 00 00 00 00 00 00  40 00 00 02 00 00 00 35   ........ @......5
0040  00 00 02 b9 00 2e e5 ec  47 45 54 20 68 74 74 70   ........ GET http
0050  3a 2f 2f 77 77 77 2e 67  6f 6f 67 6c 65 2e 63 6f   ://www.g oogle.co
0060  6d 2f 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   m/ HTTP/ 1.1..Hos
0070  74 3a 20 77 77 77 2e 67  6f 6f 67 6c 65 2e 63 6f   t: www.g oogle.co
0080  6d 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   m..User- Agent: M
0090  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 58 31 31 3b   ozilla/5 .0 (X11;
00a0  20 55 3b 20 4c 69 6e 75  78 20 69 36 38 36 3b 20    U; Linu x i686;
00b0  65 6e 2d 55 53 3b 20 72  76 3a 31 2e 39 2e 31 2e   en-US; r v:1.9.1.
00c0  38 29 20 47 65 63 6b 6f  2f 32 30 31 30 30 32 31   8) Gecko /2010021
00d0  34 20 4c 69 6e 75 78 20  4d 69 6e 74 2f 38 20 28   4 Linux  Mint/8 (
00e0  48 65 6c 65 6e 61 29 20  46 69 72 65 66 6f 78 2f   Helena)  Firefox/
00f0  33 2e 35 2e 38 0d 0a 41  63 63 65 70 74 3a 20 74   3.5.8..A ccept: t
0100  65 78 74 2f 68 74 6d 6c  2c 61 70 70 6c 69 63 61   ext/html ,applica
0110  74 69 6f 6e 2f 78 68 74  6d 6c 2b 78 6d 6c 2c 61   tion/xht ml+xml,a
0120  70 70 6c 69 63 61 74 69  6f 6e 2f 78 6d 6c 3b 71   pplicati on/xml;q
0130  3d 30 2e 39 2c 2a 2f 2a  3b 71 3d 30 2e 38 0d 0a   =0.9,*/* ;q=0.8..
0140  41 63 63 65 70 74 2d 4c  61 6e 67 75 61 67 65 3a   Accept-L anguage:
0150  20 65 6e 2d 75 73 2c 65  6e 3b 71 3d 30 2e 35 0d    en-us,e n;q=0.5.
0160  0a 41 63 63 65 70 74 2d  45 6e 63 6f 64 69 6e 67   .Accept- Encoding
0170  3a 20 67 7a 69 70 2c 64  65 66 6c 61 74 65 0d 0a   : gzip,d eflate..
0180  41 63 63 65 70 74 2d 43  68 61 72 73 65 74 3a 20   Accept-C harset:
0190  49 53 4f 2d 38 38 35 39  2d 31 2c 75 74 66 2d 38   ISO-8859 -1,utf-8
01a0  3b 71 3d 30 2e 37 2c 2a  3b 71 3d 30 2e 37 0d 0a   ;q=0.7,* ;q=0.7..
01b0                                                     Keep-Ali ve: 300.
```

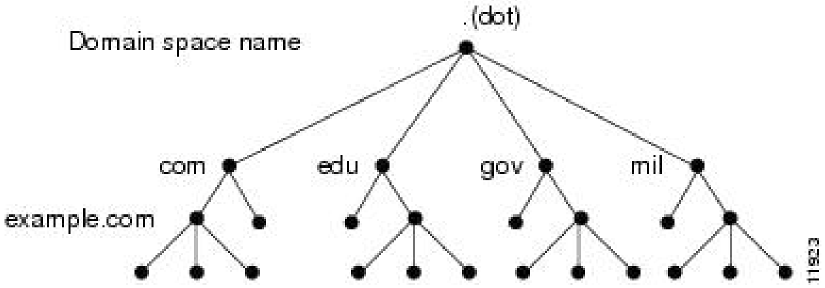
Section 3

Domain Name System (DNS)

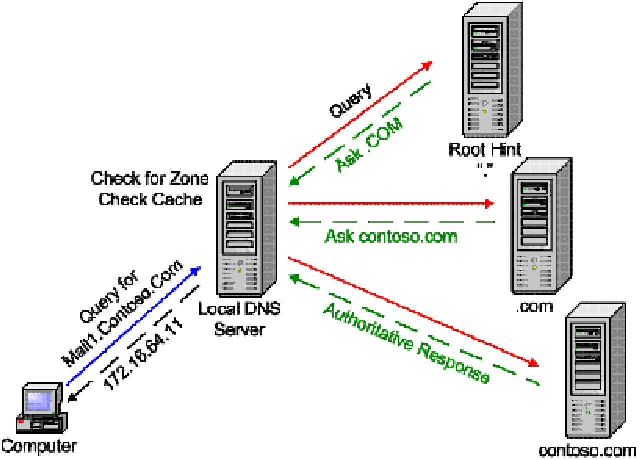
Recap: How does DNS work?

```
1252:~# dig fit.cvut.cz

; <<>> DiG 9.11.4-P1-RedHat-9.11.4-5.P1.fc28 <<>> fit.cvut.cz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61156
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
    ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 8192
;; QUESTION SECTION:
;fit.cvut.cz.      IN   A

;; ANSWER SECTION:
fit.cvut.cz.    3327   IN   A 147.32.232.248

;; Query time: 1 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Sun Oct 21 12:52:22 CEST 2018
;; MSG SIZE  rcvd: 56
```

DNS I

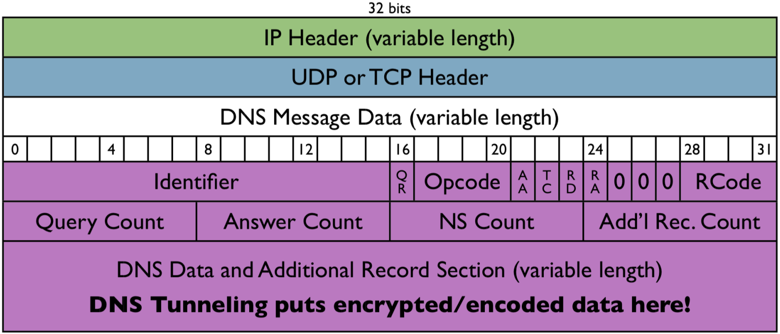


DNS II



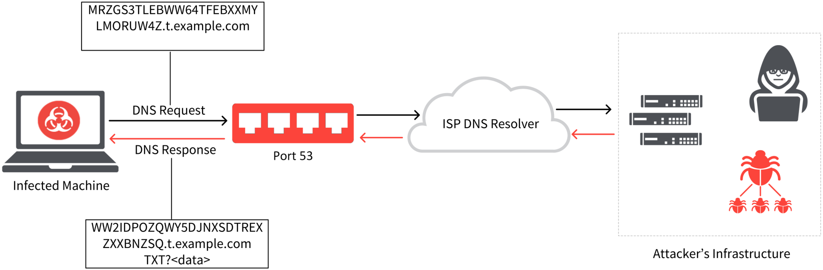
Query
Ask .COM
Root Hint
"."
Check for Zone
Check Cache
Ask contoso.com
.com
Query for
Mail1.Contoso.Com
172.16.64.11
Local DNS
Server
Authoritative Response
Computer
contoso.com

DNS Message

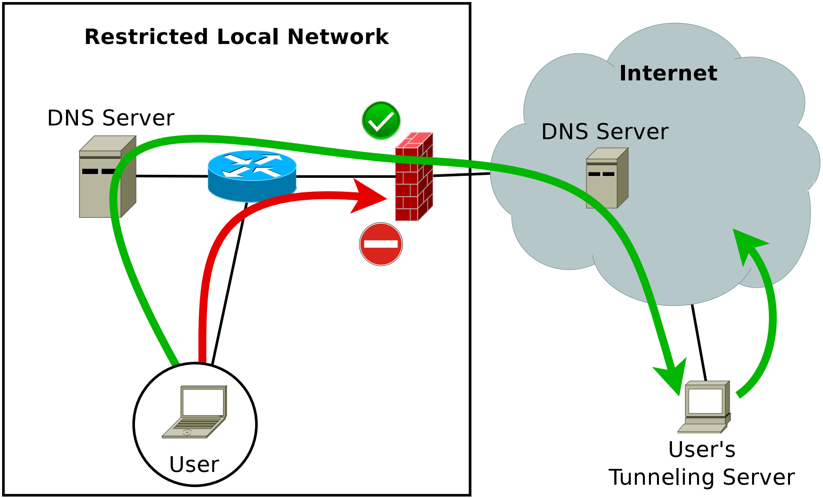


QR	...	Query / Response	RD	...	Recursion Desired
AA	...	Authoritative Response	RA	...	Recursion Available
TC	...	Truncation Flag (UDP<512B)	RCode	...	Response Code (0-10)

DNS Tunnel (malware communication)



DNS Tunnel (escape from restricted network)



DNS Tunnelling: HowTo

Transmit "Greetings!" ...

- Client: base32 encode "Greetings!" and make a DNS query: I5ZGKZLUNFXGO4ZB.sshdns.mydomain.com
- Local DNS response: "I do not know I5ZGKZLUNFXGO4ZB. sshdns.mydomain.com, ask the DNS server of mydomain.com at IP address: w.x.y.z."
- w.x.y.z DNS response: "Ask DNS for sshdns.example.com at IP: a.b.c.d". This is attackers server with the proxy software.
- The proxy server base32 decodes I5ZGKZLUNFXGO4ZB as "Greetings!"

... and receive a reply "Hello..."

- The proxy server base64 encodes "Hello..." to get "SGVsbG8uLi4=" and returns that in a TXT record.
- The client receives "SGVsbG8uLi4=" and b64decode's it to get "Hello..."

Example of Tunneled Data I

DNS Request

```
Daaapiaicab.FV++++++++9-J8C8FR3bL+P3L+ZLPb2XZCvg7LYN
qwo-BvjMjODlt4U91.sv7KFx672PumRw8Zkz2gZWUaFhuNaK0fQ2
IsVKRZMh5I3vp5U1aq05qQV.o8ht+jU2qSNm5rqNbdXdDPTnaf8a
39lUYGOfFV2JE8lO6JaJOXDdDoSkg.DAC-GMaj7klra4TVy3+bnT
O9jl4lhIk+AkavZiqgKy3fjakMjSzIDgKvg.abc.ab
```

= 255 characters of domain name

Example of Tunneled Data II

DNS Request

```
Paaapiamci1gq.abc.ab
Paaapiamei1ia.abc.ab
Paaapiaici1lq.abc.ab
Paaapiaiei1mq.abc.ab
```

= many packets with short domain names lookups

DNS Response

```
fp4suaacaakjngaaaeaaaagsaqaabhh6ovo2cp3kedmpt7ieaeaa
aaa3aaaabsm.wvxuacaaiaaaqbuikomje3t7uab3vmf55ydjxg47
jlyphl7y.v3.url.abc.ab
```

data stored in TXT field

Detection

- Unencrypted tunnel:
  Search for specific signatures, e.g., SSH connection contains identification string
  (`SSH-protoversion-softwareversion SP comments CR LF`).
- Anomaly detection
  - abnormally big packets — ICMP, DNS
  - high packet rate of ICMP, DNS
- Entropy of DNS data?

Detection

T. Cejka, Z. Rosa, and H. Kubatova: *Stream-wise detection of surreptitious traffic over DNS*. In 2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Athens, Greece, 2014, pp. 300–304.

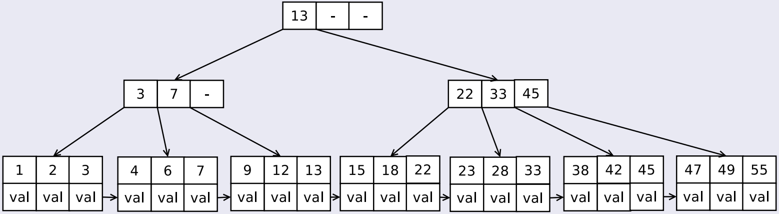
What the Detection Module Analyzes?

Many characteristics are observed or computed:

1. Mean value and variance of sizes of DNS requests & responses
2. Number of letters/digits in domain names
3. Fraction of common part of domain names
4. Repeating domain names

Data Structures

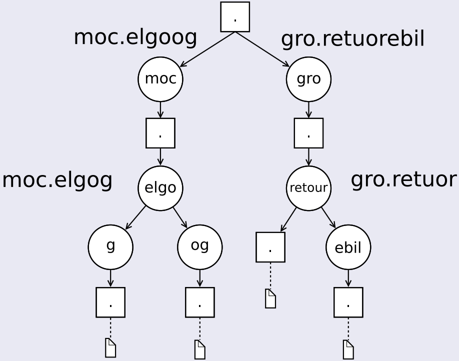
B+ tree



- network (IPv4 / IPv6) addresses used as keys
- stored values contain information about DNS traffic of an address

Data Structure in the memory

"Prefix" tree



- used for domain names storage (from right to left)
- analysis of different and common parts of domain names
- extended with metadata (statistics about domain names)

Countermeasures?

- Rate limiting
- Implicit output blocking & Permitted local proxy (with analysis)
- ???

Section 4

DNS over HTTPS

DNS over HTTPS (DoH)

- Encrypted communication of DNS requests&responses using HTTPS
- Motivation: “privacy” of the users
- Based on GET / POST methods
- wireformat — binary DNS data encoded to HTTPS data
- DoH providers, e.g., Cloudflare, Google
- Supported by modern web browsers, OS

DoH: Potential Security Threats

- Covert channel
- CC communication
- Serving malware files
- Serving hidden links

DoH: Research in Detection

- DoH traffic differs in some characteristics
- Firefox / Chrome / cloudflared differs
- Beware of traffic context

D. Vekshin, K. Hynek, and T. Cejka: *DoH Insight: Detecting DNS over HTTPS by Machine Learning*. In Proceedings of the 15th International Conference on Availability, Reliability and Security, New York, NY, USA, 2020.

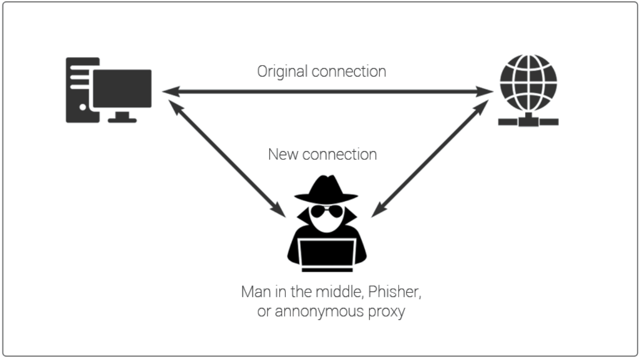
K. Hynek and T. Čejka: *Privacy Illusion: Beware of Unpadded DoH*. Proceedings of the 11th Annual IEEE Information Technology, Electronics and Mobile Communication Conference (IEMCON2020), 2020.

Section 5

Man in the Middle (MitM)

MitM Introduction

- Goal: to allow the intruder or the unauthorized party to eavesdrop and/or modify the transmitted data
- 1^{st} step: getting the access to the network traffic



- Mr.Robot series: "femtocell": bogus AP
- DHCP – rogue DHCP server
- ARP cache poisoning
- DNS cache poisoning
- DNS hijacking (https://en.wikipedia.org/wiki/Domain_hijacking)
- BGP hijacking (https://en.wikipedia.org/wiki/BGP_hijacking)
- Session hijacking (https://en.wikipedia.org/wiki/Session_hijacking)
- NTP MitM (Delorean https://github.com/PentesterES/Delorean), affecting HSTS?

  Selvi, Jose. Bypassing HTTP strict transport security. Black Hat Europe (2014).

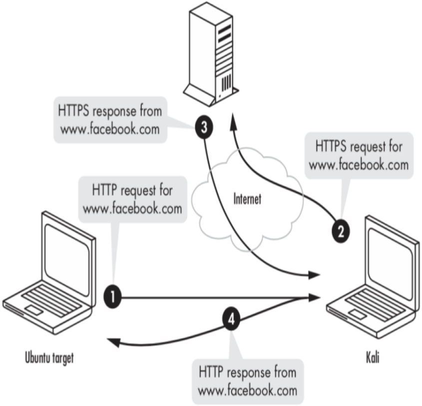
MitM and Encryption

How to intercept the encrypted data?

- SSL Stripping
- Host Certificate Hijacking / Certificate pinning
- TLS Protocol Downgrade

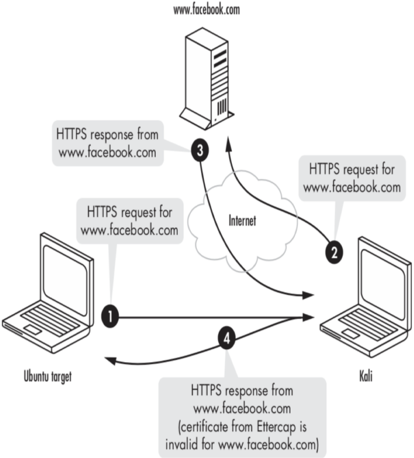
SSL Stripping

- SSLstrip tool
- In SSL MitM users have to click on SSL certificate warning
- Connection to the user is SSL stripped in plain HTTP
- Connection to the webserver from the attacker via HTTPS



Host Certificate Hijacking / Certificate Pinning

If the attacker is able to inject malicious root certificate into the trusted root certificate authority store of the victim device, user will receive no warning messages for certificates being not valid.



TLS Protocol Downgrade

Manipulate the negotiated connection to downgrade the negotiated protocol or cipher suites — various known attacks

- BEAST (CVE-2011-3389)
- BREACH (CVE-2013-3587)
- CRIME (CVE-2012-4929)
- Heartbleed (CVE-2014-0160)
- POODLE (CVE-2014-3566)

Section 6

DNS Attacks

DNS

- To increase performance – server caches resolved translation for a certain amount of time
- No cryptographic protection, no authentication, no integrity checks by default
- DNS accepts only responses to pending queries... However, first good answer wins
- Cache poisoning attacks possible

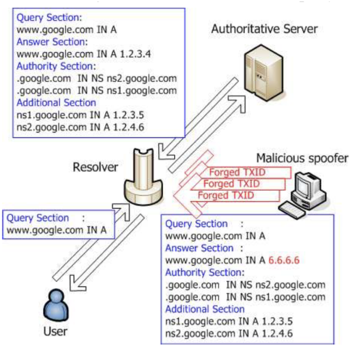
  Sooel Son and Vitaly Shmatikov: *The Hitchhiker's Guide to DNS Cache Poisoning*

Blind response forgery using birthday attack

By default, DNS only checks are:

- 16-bit transaction ID (TXID) must match: query and response
- *srcip* and *dstport* of response ? = *dstip* and *srcport* of the query
- First arriving UDP packet satisfying the condition is treated as valid

TXID has only N bits of entropy (theoretically N=16);
Much less in practice: TXID not randomized properly (just incrementing)



Cache Poisoning without Response Forgery

Bailiwick rule

(example from http://www.linuxjournal.com/content/understanding-kaminskys-dns-bug)

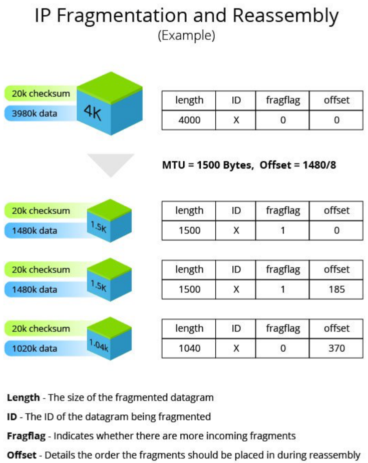
- Adopted by BIND in 1993
- Before adopted, the owner of any DNS authoritative server could compromise records corresponding to any domain name
- Kaminsky's exploit presented on BlackHat conference allows to even bypass the bailiwick check

```
# dig doesnotexist.example.com
;; ANSWER SECTION:
doesnotexist.example.com.  120     IN  A     10.10.10.10

;; AUTHORITY SECTION:
example.com.              86400    IN  NS    www.example.com.

;; ADDITIONAL SECTION:
www.example.com.         604800    IN  A     10.10.10.20
```

Fragmentation Attack

https://www.incapsula.com/ddos/attack-glossary/ip-fragmentation-attack-teardrop.html

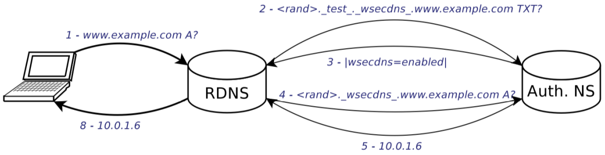
https://ripe67.ripe.net/presentations/240-ipfragattack.pdf



Response forgery using eavesdropping

Different proposed countermeasures:

- Source port randomization
- 0x20-bit encoding — randomize the case of question name — ask for wWw.xyz.com, WWW.XyZ.com instead of www.xyz.com etc.
- Extended Query ID (XQID) - A domain name label consisting of 24 to 63 random characters (0-9, a-z). Not case sensitive
- WSEC-DNS (`http://ieeexplore.ieee.org/document/5270363/`):
  - Does not add confidentiality nor provides authentication
  - Protects against "blind" brute forcing
  - DNS is still vulnerable to trivial attacks such as network eavesdroppers & packet forging



Section 7

Brief information about DNSSEC

DNSSEC

https://www.nanog.org/meetings/nanog51/presentations/Sunday/DNSSEC-tutorial-for-NANOG51-2011-01.pdf

- DNSSEC provides no confidentiality = all DNS data are public
- DNSSEC provides data origin authentication & data integrity
- Each zone has a public/private key pair
- Public key is stored in DNSKEY record
- Private key needs to be keep safe — HSM (Hardware Security Module)

DNSKEY record

256/257 — 16bit flag field — DNSSEC zone key/key-signing key (used for signing zone keys) 3 protocol octet for DNSSEC 5 algorithm number (RSA with SHA-1) The public key itself

```
example.com.   2849 IN  DNSKEY 257 3 8 (
          AwEAAZ0aqu1rJ6orJynrRfNpPmayJZoAx9Ic2/Rl9VQW
          LMHyjxxem3VUSoNUIFXERQbj0A9Ogp0zDM9YIccKLRd6
          LmWiDCt7UJQxVdD+heb5Ec4qlqGmyX9MDabkvX2NvMws
          UecbYBq8oXeTT9LRmCUt9KUt/WOi6DKECxoG/bWTykrX
          yBR8elD+SQY43OAVjlWrVltHxgp4/rhBCvRbmdflunaP
          Igu27eE2U4myDSLT8a4A0rB5uHG4PkOa9dIRs9y00M2m
          Wf4lyPee7vi5few2dbayHXmieGcaAHrx76NGAABeY393
          xjlmDNcUkF1gpNWUla4fWZbbaYQzA93mLdrng+M=
          ) ; KSK; alg = RSASHA256 ; key id = 45620
example.com.   2849 IN  DNSKEY 256 3 8 (
          AwEAAd3ls8XH4tS6n576cFPy9ZbtQlf8ivP29WA41Kes
          7KRQvU+jATlR68mBW2AaIMxfdYaV9ddg0zz6jAt8o3zT
          foylcr8UpmgD0C1qZ/OQYQ/gAOATMDCT6lz8cz+eYB+R
          k2b/Ptuhkx2HRkZJKJyirRyHyg7vYQ0gMIdNJ8D9munn
          ) ; ZSK; alg = RSASHA256 ; key id = 63855
```

RRSIG Record

- Each resource record set (RRSET) in a zone is signed by zone's private key
- RRSET – records with same owner, class and type
- Digital signature is stored in RRSIG record

A type of records signed 5 digital algorithm used (RSA with SHA1) 3 number of lables in the signed name 86400 original TTL When the signature expires When the record were signed 41148 the key ID/tag/footprint Test.com signer's name Digital signature itself

```
;; ANSWER SECTION:
example.com.      16484 IN A 93.184.216.34
example.com.      16484 IN RRSIG A 8 2 86400 (
            20181029053351 20181007181129 63855 example.com.
            XRKd78dE8RDam/6g2gSRM3GRy8PvpAoNFMZRPJSSMjRn
            lftP9aNZHGuKldks/2R6f7hY/iZpzuwsI3LEv8T7e1DV
            TlQesVe5S0StdkD+ssFq9iG+Rdbe7cjQDQ0aWAkzgAPE
            bFmh/2wZ4NT1CQKoshprVqcpMeasCxlJvXCyB7c= )
```

Issues with DNSSEC

- Large response (packet-amplifier)
- Complexity of key management – prevents broad deployment
- Subdomain Injection
  causes resolvers to accept, cache and provide to clients a mapping for a non-existing (child) domain, of a DNSSEC- protected parent domain
- Attacker can create fake sub-domains – this can lead to XSS, phishing, cookie stealing
- Name Server Hijacking
  causes resolvers to cache and use incorrect name servers for a DNSSEC-protected domain point them to name servers belonging to the attacker

Section 8

Some Other L7 Threats

VoIP — SIP

- Deregistering
- INVITE of Death (malformed or otherwise malicious `SIP INVITE`, `https://en.wikipedia.org/wiki/INVITE_of_Death`)
- Password guessing
- User account (extension) scanning
- Dial scheme guessing (exploit of weak configuration)
- SCAM (similar to SPAM known from e-mails) → leads to DoS

Additional Reading:

- T. Jánský, et al.: *Hunting SIP Authentication Attacks Efficiently*. AIMS 2017, Zurich.
- T. Cejka, et al.: *Using Application-Aware Flow Monitoring for SIP Fraud Detection*. AIMS 2015, Ghent.

Shellshock / Bashdoor

- Vulnerability in Bash, disclosed in 2014
- Arbitrary code execution
- Specific exploitation vectors:
  - CGI-based web server
  - OpenSSH server, *ForceCommand* feature
  - DHCP clients, can pass commands to Bash, additional options
  - Qmail server, processing mails by Bash
  - IBM HMC, gain access to Bash from the restricted shell of the IBM Hardware Management Console

HTTP

- SlowLoris (https://en.wikipedia.org/wiki/Slowloris_(computer_security)) / Slowdroid (https://en.wikipedia.org/wiki/Slowdroid)
- RUDY (R-U-Dead-Yet? https://sourceforge.net/projects/r-u-dead-yet/)
- Exploit known vulnerabilities (CMS, ...)
- Password guessing (there was a "bug" in WordPress: different delays during authentication)
- SQL injection over HTTP(s)

SMTP

- Sending SPAM is one of the typical activies of malware.
- Spoofed addresses make a SMTP server to produce lots of bounces.
- Spreading of malware, worms
- There are many blacklists (`http://valli.org`) and best practices as a "defense".

Section 9

Closing Words

References

- http://cs.uccs.edu/~jkalita/papers/2014/HoqueNetworkAttacksJCNA2014.pdf
- https://www.eecis.udel.edu/~sunshine/publications/ccr.pdf
- https://www.eecis.udel.edu/~mills/teaching/eleg867b/dos/p38-paxson.pdf
- http://www.cs.uccs.edu/~jkalita/papers/2013/BhuyanMonowarComputerJournal2013.pdf
- http://www.cs.uccs.edu/~jkalita/papers/2015/RupDekaJNCA2015.pdf
- http://ce.sharif.edu/courses/83-84/1/ce534/resources/root/Papers/attackstaxonomy.pdf
- https://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history
- and other links inside this presentation

Questions?