Prof. Sukumar Nandi
Department of Computer Science and Engineering
Indian Institute of Technology Guwahati
Email: sukumar@iitg.ernet.in

2018 Cyber Security Trends

The Latest and the Greatest Changes to the Computer and Networks Security Paradigm

Table of Contents

Introduction

System Security

Network Security

Application Security

Transport Layer Security

References

Introduction

Why do we need to stay up-to-date with cyber-security trends?

- Cyber-attacks evolve: ransomware are MITM are very common today.
- Numerous exploits are found every minute.
- Discovered exploits are also fixed over time.
- New paradigms like IoT, smart home, vehicular networks, etc. increase attack surface.
- We need to build secure systems to minimize cyber attacks.
- We need to counter censorship and cyber-espionage by oppressive nation states.

Attacks on System Software

System software like firmware, bootloader, operating system and system utilities can be attacked in numerous ways.

- Malware due to running untrusted code: viruses, spyware, trojan horses, worms, ransomware etc.
- Operating system, bootloader and firmware exploits.
- Backdoors in applications, OS, bootloader and firmware.
- Insufficient or poor OS security models.
- Poor end-user awareness.

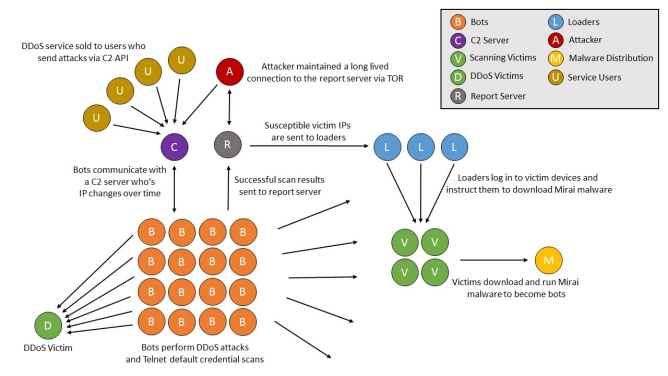
Malware

Malware are softwares which are specifically designed to disrupt, damage, or gain authorized access to a computer system.

- Malware usually infect the system either automatically by exploits or due to end-user action caused by poor judgement.
- Antivirus and malware suites are no longer effective against these. In fact there are known cases, where increase the number of security holes [1, 2]. On Windows, the default Defender is sufficient.
- Malware also affect non-PC and non-server platforms such as mobile devices and IoT devices like phones (RedDrop, Pegasus) and webcams (Mirai).

Malware

Mirai malware botnet structure


B Bots
C C2 Server
V Scanning Victims
D DDoS Victims
R Report Server
L Loaders
A Attacker
M Malware Distribution
U Service Users
DDoS service sold to users who send attacks via C2 API
U
U
U
U
A
Attacker maintained a long lived connection to the report server via TOR
C
R
Susceptible victim IPs are sent to loaders
L
L
L
Bots communicate with a C2 server who's IP changes over time
Successful scan results sent to report server
Loaders log in to victim devices and instruct them to download Mirai malware
B
V
V
V
V
M
Victims download and run Mirai malware to become bots
D
DDoS Victim
Bots perform DDoS attacks and Telnet default credential scans

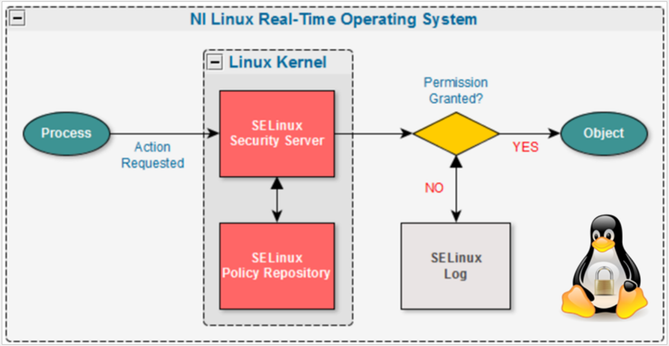
Malware

Malware can be mitigated by following the given steps:

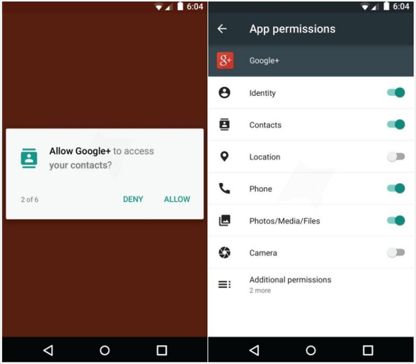
- Updating OS, applications and firmware regularly.
- If a product no longer receives software updates, limit usage and people accessing it to the bare minimum.
- Using kernel level security measures like SELinux, AppArmor, grsecurity, OpenBSM, etc.
- Avoid installing apps from unknown and untrusted sources.
- Observing the permissions requested by an app before installing.
- If using an untrusted app is needed, run it on a virtual machine (KVM, VMWare) or a container (Docker, LXC, BSD jails) to isolate it.

Malware

SELinux workflow[3]



Android permissions[4]



Allow Google+ to access your contacts?

2 of 6

DENY ALLOW

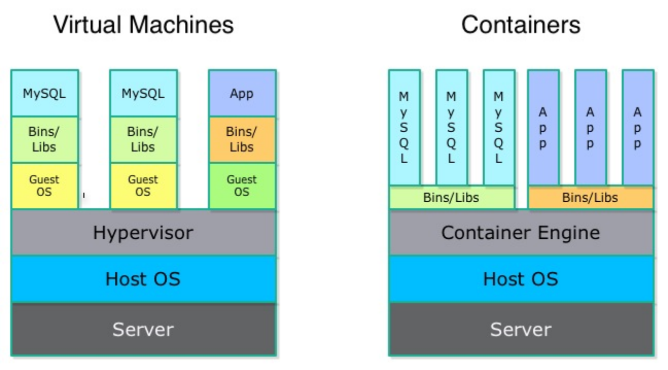
App permissions

Google+

- Identity ☑
- Contacts ☑
- Location ☐
- Phone ☑
- Photos/Media/Files ☑
- Camera ☐
- Additional permissions
  2 more

Malware

Virtual Machines and Containers[5]



Exploits

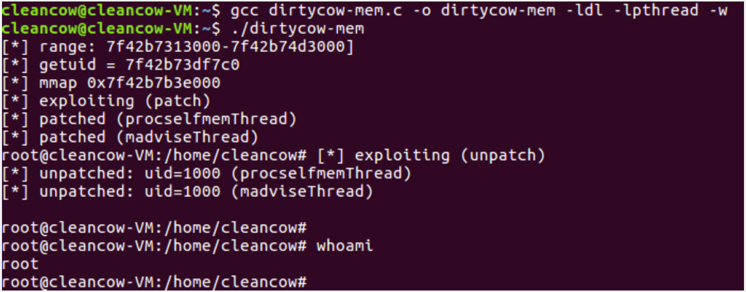
An exploit is a vulnerability in a computer system which allows an attacker to reduce its information assurance, security, control and performance.

Exploits arise due to:

- Complexity of software code that leaves unintended access points.
- Familiarity and reuse of software that allows an attacker to make an intelligent guess.
- Fundamental operating system design flaws that grants full system access to a program.
- Bugs left by the programmer in a software application.
- Not sanitizing/validating user input and mishandling buffer overflow cases.
- Not learning from past mistakes.

Exploits

Dirtycow local root exploit[6]

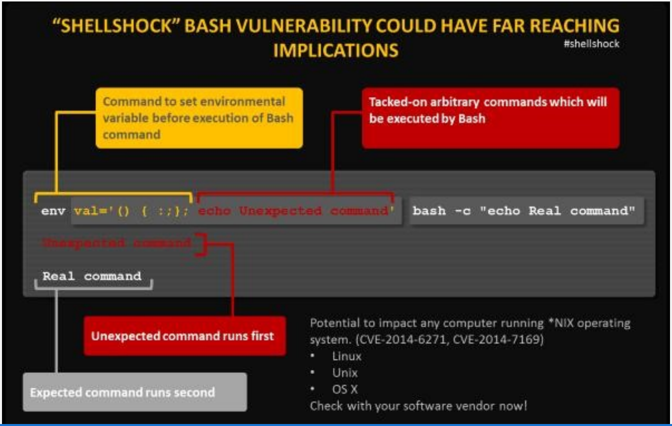


```
cleancow@cleancow-VM:~$ gcc dirtycow-mem.c -o dirtycow-mem -ldl -lpthread -w
cleancow@cleancow-VM:~$ ./dirtycow-mem
[*] range: 7f42b7313000-7f42b74d3000]
[*] getuid = 7f42b73df7c0
[*] mmap 0x7f42b7b3e000
[*] exploiting (patch)
[*] patched (procselfmemThread)
[*] patched (madviseThread)
root@cleancow-VM:/home/cleancow# [*] exploiting (unpatch)
[*] unpatched: uid=1000 (procselfmemThread)
[*] unpatched: uid=1000 (madviseThread)

root@cleancow-VM:/home/cleancow#
root@cleancow-VM:/home/cleancow# whoami
root
root@cleancow-VM:/home/cleancow#
```

Exploits

BASH Shellshock exploit[7]



“SHELLSHOCK” BASH VULNERABILITY COULD HAVE FAR REACHING IMPLICATIONS

#shellshock

Command to set environmental variable before execution of Bash command

Tacked-on arbitrary commands which will be executed by Bash

```
env val='() { :;}; echo Unexpected command' bash -c "echo Real command"
Unexpected command
Real command
```

Unexpected command runs first

Expected command runs second

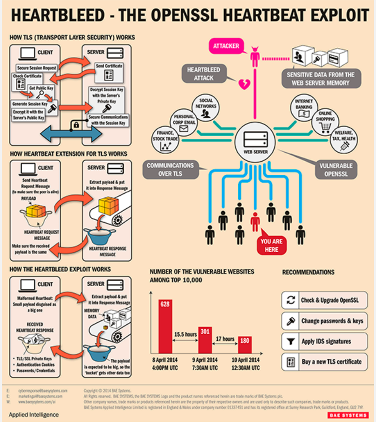
Potential to impact any computer running *NIX operating system. (CVE-2014-6271, CVE-2014-7169)

- Linux
- Unix
- OS X

Check with your software vendor now!

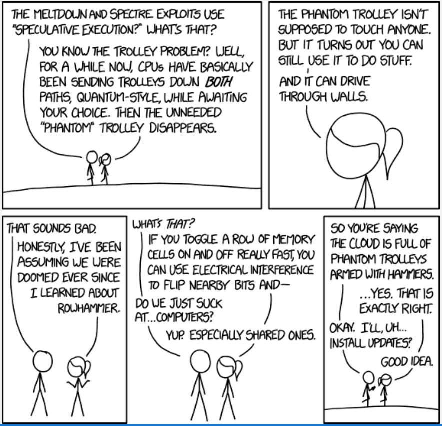
Exploits

OpenSSL Heartbleed exploit[8]


HEARTBLEED - THE OPENSSL HEARTBEAT EXPLOIT
HOW TLS (TRANSPORT LAYER SECURITY) WORKS
CLIENT
SERVER
Secure Session Request
Send Certificate
Check Certificate
Get Public Key
Decrypt Session Key with the Server's Private Key
Generate Session Key
Encrypt it with the Server's Public Key
Secure Communications with the Session Key
HOW HEARTBEAT EXTENSION FOR TLS WORKS
CLIENT
SERVER
Send Heartbeat Request Message (to make sure the peer is alive)
PAYLOAD
Extract payload & put it into Response Message
HEARTBEAT REQUEST MESSAGE
Make sure the received payload is the same
HEARTBEAT RESPONSE MESSAGE
HOW THE HEARTBLEED EXPLOIT WORKS
CLIENT
SERVER
Malformed Heartbeat: Small payload disguised as a big one
Extract payload & put it into Response Message
MEMORY DATA
RECEIVED HEARTBEAT RESPONSE
• TLS/SSL Private Keys
• Authentication Cookies
• Passwords/Credentials
The payload is expected to be big, so the "bucket" gets other data too
ATTACKER
HEARTBLEED ATTACK
SENSITIVE DATA FROM THE WEB SERVER MEMORY
SOCIAL NETWORKS
PERSONAL, CORP EMAIL
FINANCE, STOCK TRADE
INTERNET BANKING
ONLINE SHOPPING
WELFARE, TAX, HEALTH
WEB SERVER
COMMUNICATIONS OVER TLS
VULNERABLE OPENSSL
YOU ARE HERE
NUMBER OF THE VULNERABLE WEBSITES AMONG TOP 10,000
628
15.5 hours
301
17 hours
180
8 April 2014 4:00PM UTC
9 April 2014 7:30AM UTC
10 April 2014 12:30AM UTC
RECOMMENDATIONS
Check & Upgrade OpenSSL
Change passwords & keys
Apply IDS signatures
Buy a new TLS certificate
E: cyberresponse@baesystems.com
E: marketingai@baesystems.com
W: www.baesystems.com/ai
Applied Intelligence
Copyright © 2014 BAE Systems.
All Rights reserved. BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trade marks of BAE Systems plc.
Other company names, trade marks or products referenced herein are the property of their respective owners and are used only to describe such companies, trade marks or products.
BAE Systems Applied Intelligence Limited is registered in England & Wales under company number 01337451 and has its registered office at Surrey Research Park, Guildford, England, GU2 7YP.
BAE SYSTEMS

Exploits

Meltdown and Spectre exploits[9]


THE MELTDOWN AND SPECTRE EXPLOITS USE "SPECULATIVE EXECUTION?" WHAT'S THAT?
YOU KNOW THE TROLLEY PROBLEM? WELL, FOR A WHILE NOW, CPUs HAVE BASICALLY BEEN SENDING TROLLEYS DOWN *BOTH* PATHS, QUANTUM-STYLE, WHILE AWAITING YOUR CHOICE. THEN THE UNNEEDED "PHANTOM" TROLLEY DISAPPEARS.
THE PHANTOM TROLLEY ISN'T SUPPOSED TO TOUCH ANYONE. BUT IT TURNS OUT YOU CAN STILL USE IT TO DO STUFF.
AND IT CAN DRIVE THROUGH WALLS.
THAT SOUNDS BAD.
HONESTLY, I'VE BEEN ASSUMING WE WERE DOOMED EVER SINCE I LEARNED ABOUT ROWHAMMER.
WHAT'S *THAT?*
IF YOU TOGGLE A ROW OF MEMORY CELLS ON AND OFF REALLY FAST, YOU CAN USE ELECTRICAL INTERFERENCE TO FLIP NEARBY BITS AND—
DO WE JUST SUCK AT...COMPUTERS?
YUP. ESPECIALLY SHARED ONES.
SO YOU'RE SAYING THE CLOUD IS FULL OF PHANTOM TROLLEYS ARMED WITH HAMMERS.
...YES. THAT IS EXACTLY RIGHT.
OKAY. I'LL, UH... INSTALL UPDATES?
GOOD IDEA.

Exploits

Exploits can be mitigated by:

- Keeping OS, software and firmware up-to-date with latest patches.
- Following best practices for software development.
- Handling user input with caution.
- Use past experience as a guiding light.

Backdoors

A backdoor is a hidden path left by the creators of a computer system that allows complete access to it by bypassing the normal authentication mechanisms used to limit access control.

Some notable newest backdoors are:

- Samsung Galaxy devices running proprietary Android versions come with a back door[10] that provides remote access to the data stored on the device.
- Siri, Alexa, and all the other voice-control systems can be hijacked by programs that play commands in ultrasound[11] that humans can't hear.
- Many appliances (like webcams) are sold with spyware sending lots of data to China.
- All Verizon Wireless Android phones now come with app that allows OEMs backdoor access to install other apps without permission[12].
- OnePlus found to be collecting personally identifiable analytics data[13] from phone owners.
- Intel AMT backdoor allows hackers to gain control of PCs in under a minute[14].

Backdoors

Backdoors can be mitigated by:

- Only buying products that respect privacy.
- Avoiding unbranded electronics.
- Using Free and Open Source Software (FOSS) and Hardware (FOSH) as much as possible.
- Raising voices against (esp. Chinese and US) manufacturers that indulge in illegal and unethical practices.

End-user awareness

“A computer is only as smart as the person using it.”

- One must have basic awareness about the computer system we use.
- Always observe the system for any anomalies, like slowness, freezing, creation of unknown files, unknown app installations and similar unexpected behaviour.
- Never install apps from unknown sources and do not accept toolbars or other adware bundled in installers.
- Never install apps without looking at the permissions being requested.
- Never click on scammy ads that require you to install something on the internet.
- Always update your OS and apps.
- Remember to back up your computer at regular intervals. Backups are the best solution to system software attacks.
- If you do not plan to use your computer for a long time, it is better to keep it powered off.
- Last but not the least, always prefer to use free and open source software because they can be easily audited for security issues.

Attacks using the Network Stack

Various attacks are possible using the network stack, especially using network layer (IP), transport layer (TCP/UDP) and application layer (HTTP/DNS/NTP) in conjunction. Some newest trending attacks are:

- Reflection and amplification attacks aided with application layer protocols like DNS and NTP.
- Man-in-the-middle attacks.
- Censorship (as in China, Iran and Cuba).
- Cyber-espionage (as done by NSA and various companies).

Reflection and amplification attacks

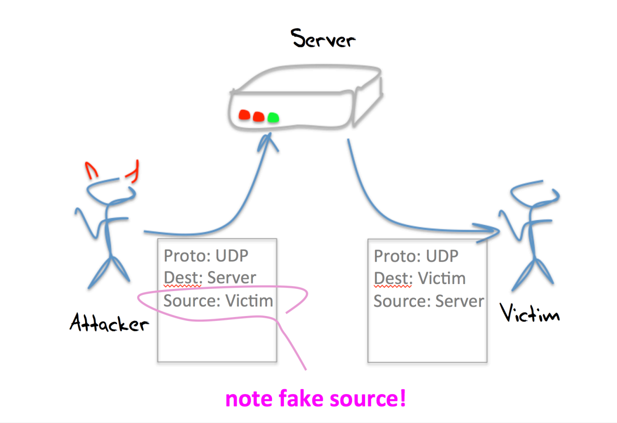
A reflection attack is a type of Distributed Denial of Service (DDoS) attack uses openly accessible servers of the aiding protocol (i.e. DNS or NTP) to attack a target from multiple locations. The attacker sends a request to these open servers spoofing or pretending to be the target. All the servers then send the response to the target at the same time, bringing it down.

An amplification attack is a type of Distributed Denial of Service (DDoS) attack in which the attacker exploits vulnerabilities in the aiding protocol (i.e. DNS or NTP) servers to turn initially small queries into much larger payloads, which are used to bring down the victim's servers.

Reflection and amplification combined can generate attacks with a huge size and volume, often exceeding 300 Gbps.

Reflection and amplification attacks

Reflection attack[15]



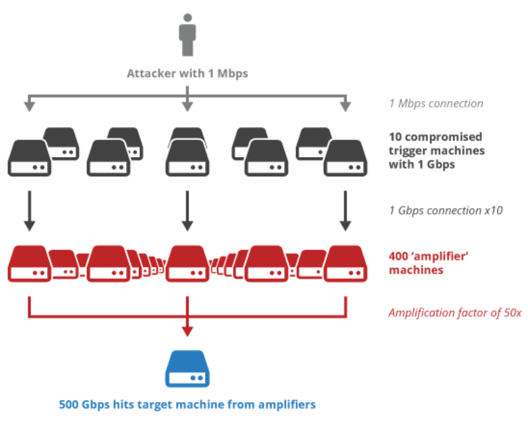
Proto: UDP
Dest: Server
Source: Victim

Proto: UDP
Dest: Victim
Source: Server

note fake source!

Reflection and amplification attacks

Amplification attack[16]


Attacker with 1 Mbps
1 Mbps connection
10 compromised trigger machines with 1 Gbps
1 Gbps connection x10
400 'amplifier' machines
Amplification factor of 50x
500 Gbps hits target machine from amplifiers

Reflection and amplification attacks

Reflection and amplification attacks can be reduced by configuring open servers/resolvers in the following manner:

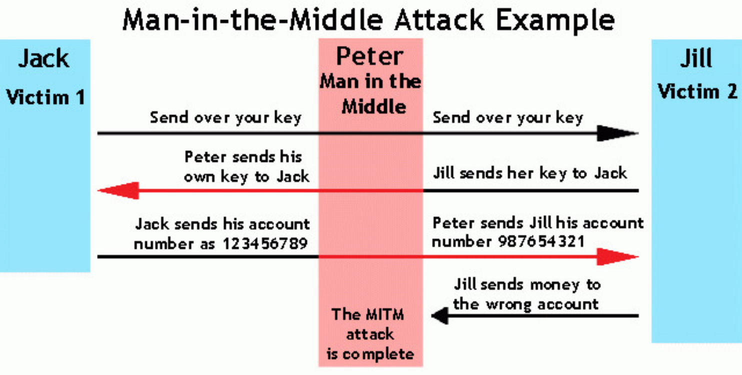
- Disabling recursive/open access if not needed.
- Limiting the number of services offered.
- Limiting the people or resources that can access.
- Employing rate limits on queries.
- Filtering or not responding to unnecessary or anomalous requests.

Man-in-the-middle attacks

A man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Man-in-the-middle attacks

How is an MITM attack[17] performed?


Man-in-the-Middle Attack Example
Jack
Victim 1
Peter
Man in the Middle
Jill
Victim 2
Send over your key
Send over your key
Peter sends his own key to Jack
Jill sends her key to Jack
Jack sends his account number as 123456789
Peter sends Jill his account number 987654321
Jill sends money to the wrong account
The MITM attack is complete

Man-in-the-middle attacks

The chances of MITM attack can be reduced by:

- Verifying the hostname or address in the address bar while connecting to a website or service.
- Using TLS (SSL) everywhere and as much as possible.
- Ensuring that your computer's OS supports DNSSEC.

Censorship

Internet censorship is the control or suppression of what can be accessed, published, or viewed on the Internet enacted by regulators, or on their own initiative.

Censorship

- restricts free and fair access to the Internet and creates inequality.
- violates right to life by restricting access to emergency/help in oppressive regions.
- violates right to free speech.
- violates right to information.

Censorship

Internet censorship is practiced extensively in oppressive regions such as China, Cuba and Iran in order to

- avoid citizens from getting information about the horrible actions of their regimes.
- to prevent citizens from dissent and organizing uprisings.
- to prevent citizens from sending information about the regime abroad.
- to prevent access to art and literature not approved of by the regime.

Even liberal nations practice censorship in response to copyright strikes, reducing access to P2P or to prohibit activities forbidden by the law.

Censorship

“The Net interprets censorship as damage and routes around it.”
– John Gilmore, Electronic Frontier Foundation

Censorship can be defeated with the following steps:

- Setting up your phone or computer to use non-ISP DNS like Google DNS or OpenDNS.
- Browsing in HTTPS and using TLS (SSL) everywhere.
- Using censorship circumvention tools.

Censorship

Censorship circumvention tools

- VPNs like OpenConnect/AnyConnect, OpenSSH, OpenVPN and WireGuard can defeat censorship in Turkey and Iran.
- ShadowSocks and ShadowSocksR socks proxy servers can defeat censorship in China.
- Streisand is a wizard that can help set up the above mentioned tools in a few minutes.

Cyber-espionage

Cyber espionage, is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of proxy servers, cracking techniques and malicious software including trojan horses and spyware.

For example, the National Security Agency has been spying on billions of individuals around the world with the PRISM and Fairview.

Cyber-espionage

Cyber-espionage can be avoided by:

- Avoiding using Microsoft Windows and preferring to use a free-and-open-source OS like GNU/Linux distros or FreeBSD.
- Using HTTPS and TLS (SSL) everywhere.
- Avoiding products with known backdoors.
- Switching to secure email services like Protomail and Tutanota.
- Using VPNs in public wifi hotspots.

Attacks on applications today

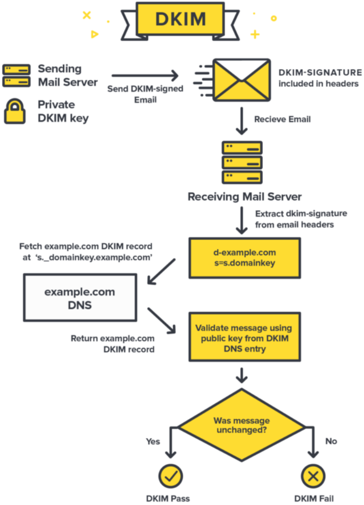
The most common attacks on applications today are:

- Malicious email: spam and phishing attacks
- DNS poisoning
- Browser based attacks

Spam and phishing emails

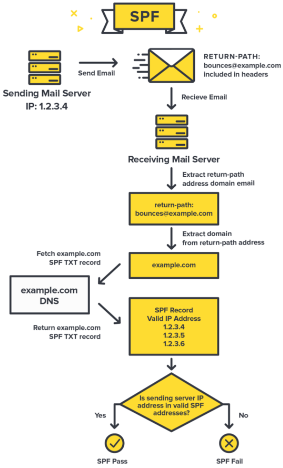
- Email spam, also known as junk email, is a type of electronic spam where unsolicited messages are sent by email.
- Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an email.
- Most spam and phishing emails are sent using botnets.
- Since spam filters are heuristic-based, they cannot catch all possible spam and phishing email.
- We need some way to validate the sender: DKIM and SPF.
- We need a policy to handle spam: DMARC

DKIM [18]

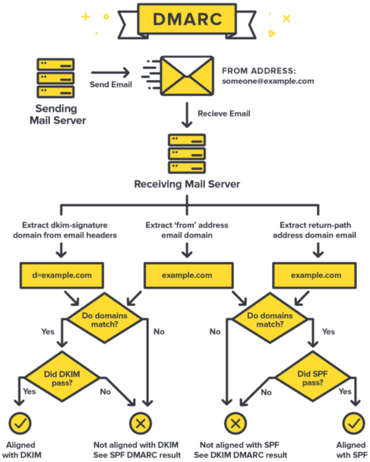


DKIM
Sending Mail Server
Private DKIM key
Send DKIM-signed Email
DKIM-SIGNATURE included in headers
Recieve Email
Receiving Mail Server
Extract dkim-signature from email headers
d-example.com s=s.domainkey
Fetch example.com DKIM record at 's._domainkey.example.com'
example.com DNS
Return example.com DKIM record
Validate message using public key from DKIM DNS entry
Was message unchanged?
Yes
No
DKIM Pass
DKIM Fail

SPF [19]


SPF
Sending Mail Server
IP: 1.2.3.4
Send Email
RETURN-PATH:
bounces@example.com
included in headers
Recieve Email
Receiving Mail Server
Extract return-path address domain email
return-path: bounces@example.com
Extract domain from return-path address
example.com
Fetch example.com SPF TXT record
example.com DNS
Return example.com SPF TXT record
SPF Record
Valid IP Address
1.2.3.4
1.2.3.5
1.2.3.6
Is sending server IP address in valid SPF addresses?
Yes
No
SPF Pass
SPF Fail

DMARC [20]



DMARC

Sending Mail Server

Send Email

FROM ADDRESS:
someone@example.com

Recieve Email

Receiving Mail Server

Extract dkim-signature domain from email headers

Extract 'from' address email domain

Extract return-path address domain email

d=example.com

example.com

example.com

Do domains match?

Yes

No

Did DKIM pass?

Yes

No

Aligned with DKIM

Not aligned with DKIM
See SPF DMARC result

Do domains match?

No

Yes

Did SPF pass?

No

Yes

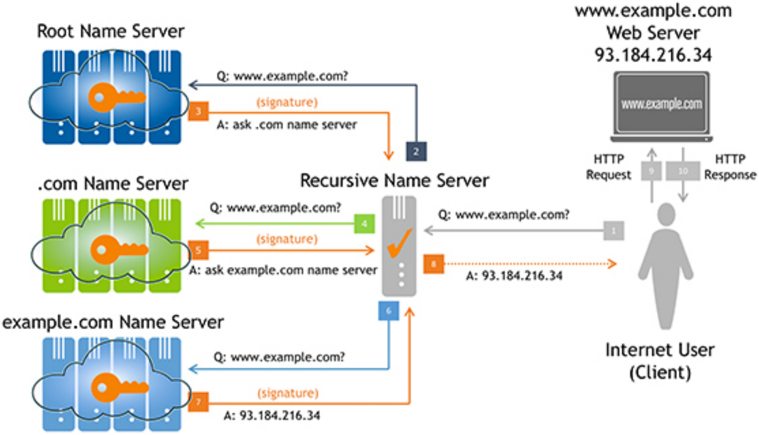
Not aligned with SPF
See DKIM DMARC result

Aligned wth SPF

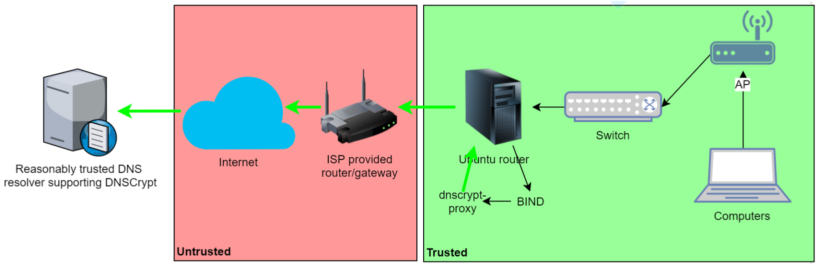
DNS poisoning

- DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect IP address. This results in traffic being diverted to the attacker's computer (or any other computer).
- We need to figure out a way to ensure that the answer to the DNS query is valid: DNSSEC.
- We need to ensure that the DNS communication between our computer and a resolver is safe and secure: DNSCrypt, DNS-over-TLS.

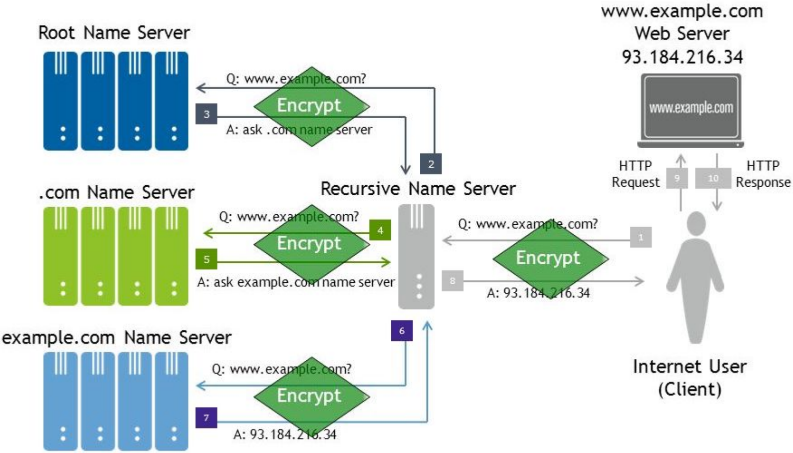
DNSSEC [21]


Root Name Server
Q: www.example.com?
(signature)
3
A: ask .com name server
2
.com Name Server
Q: www.example.com?
4
(signature)
5
A: ask example.com name server
Recursive Name Server
Q: www.example.com?
1
8
A: 93.184.216.34
6
example.com Name Server
Q: www.example.com?
(signature)
7
A: 93.184.216.34
www.example.com
Web Server
93.184.216.34
www.example.com
HTTP Request
9
10
HTTP Response
Internet User
(Client)

DNSCrypt [22]


Reasonably trusted DNS resolver supporting DNSCrypt
Internet
ISP provided router/gateway
Untrusted
Ubuntu router
dnscrypt-proxy
BIND
Switch
AP
Computers
Trusted

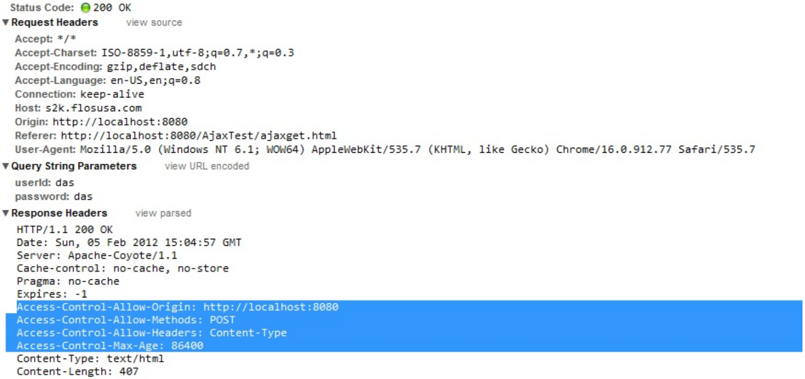
DNS-over-TLS [23]



Browser attacks

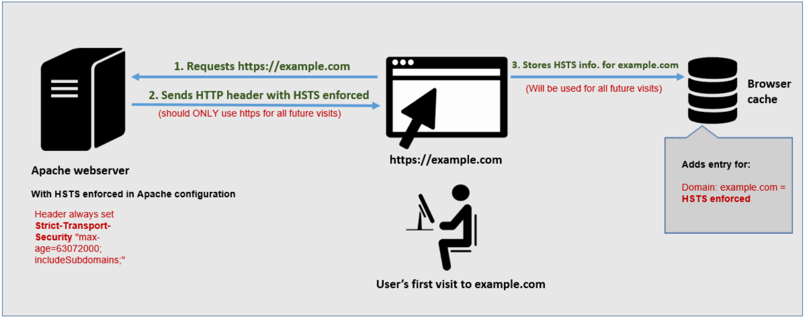
- Browsers can be exploited in numerous ways: cross-site scripting (XSS), Cross-Site Request Forgery (CSRF) and Clickjacking.
- Many of these attacks can be mitigated simply by browsing over HTTPS instead of plain HTTP.
- Many of the XSS and CSRF attacks can be mitigated by using the CORS and Access-Control-Allow-Headers headers.
- HTTPS to HTTP downgrade attacks can be prevented by using the HSTS header.

Access-control-allow headers [24]



```
Status Code: ● 200 OK
▼Request Headers        view source
  Accept: */*
  Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
  Accept-Encoding: gzip,deflate,sdch
  Accept-Language: en-US,en;q=0.8
  Connection: keep-alive
  Host: s2k.flosusa.com
  Origin: http://localhost:8080
  Referer: http://localhost:8080/AjaxTest/ajaxget.html
  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.7 (KHTML, like Gecko) Chrome/16.0.912.77 Safari/535.7
▼Query String Parameters        view URL encoded
  userId: das
  password: das
▼Response Headers        view parsed
  HTTP/1.1 200 OK
  Date: Sun, 05 Feb 2012 15:04:57 GMT
  Server: Apache-Coyote/1.1
  Cache-control: no-cache, no-store
  Pragma: no-cache
  Expires: -1
  Access-Control-Allow-Origin: http://localhost:8080
  Access-Control-Allow-Methods: POST
  Access-Control-Allow-Headers: Content-Type
  Access-Control-Max-Age: 86400
  Content-Type: text/html
  Content-Length: 407
```

HSTS header [25]


1. Requests https://example.com
2. Sends HTTP header with HSTS enforced
(should ONLY use https for all future visits)
3. Stores HSTS info. for example.com
(Will be used for all future visits)
Browser cache
Apache webserver
https://example.com
Adds entry for:
Domain: example.com = HSTS enforced
User's first visit to example.com

With HSTS enforced in Apache configuration

```
Header always set
Strict-Transport-
Security "max-
age=63072000;
includeSubdomains;"
```

Web server with HTTP Strict Transport Security (HSTS) enforced

TLS is no longer hard or expensive to implement

- Contrary to popular belief, TLS (SSL) is not expensive anymore to implement.
- The most CPU intensive part of TLS is the key exchange handshake that uses asymmetric-key RSA cryptography. It has long been replaced by lot less intensive ECC.
- ECC is not only cheaper to implement, but also provides better security at low key sizes. E.g. 384-bit ECC is equivalent to 7680-bit RSA.
- TLS connections now negotiate a one-time use session key using Elliptic-Curve Diffie-Hellman Ephemeral key exchange for forward secrecy in case the private key is compromised. Static RSA key exchange is no longer used.
- Symmetric key encryption mechanisms now use AEAD like AES-GCM, AES-CCM and ChaCha20-Poly1305 which are faster and face less pipeline blocks compared to CBC ciphers.
- The other cost associated with TLS, i.e., acquiring SSL certificates, is now gone. Let’s Encrypt issues TLS certificates free of cost.

TLS 1.3

The upcoming version of TLS, i.e., TLS 1.3 brings about massive overhauls to the protocol.

Features removed[26]:

- Static RSA handshake
- CBC MAC-then-Encrypt (MtE) modes
- RC4
- SHA1, MD5
- Compression
- Renegotiation

TLS 1.3

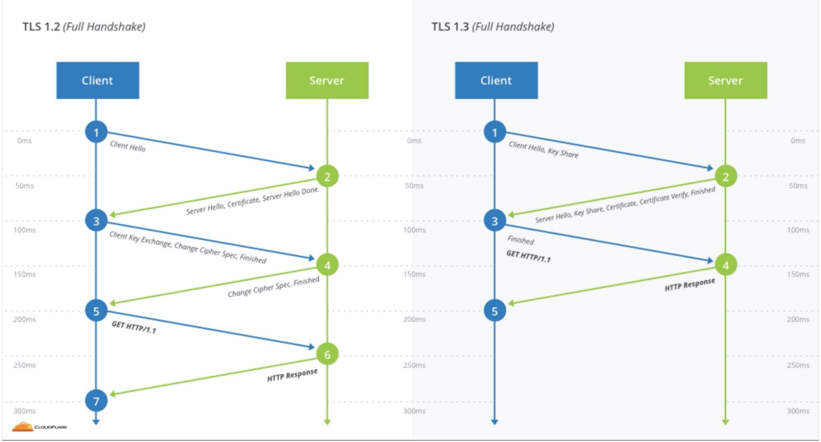
Features improved[26]:

- Fixed DHE groups
- RSA-Probabilistic Signature Scheme (RSASSA-PSS)
- AEAD Nonce
- Session IDs and Tickets

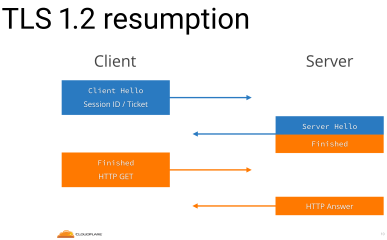
Features added[26]:

- Full handshake signature
- Downgrade protection
- Abbreviated resumption with optional (EC)DHE
- Elliptic Curve 25519 and 448

TLS 1.2 2-RTT vs TLS 1.3 1-RTT handshake [27]



TLS 1.2 1-RTT vs TLS 1.3 0-RTT session resumption [26]



TLS 1.2 resumption

Client

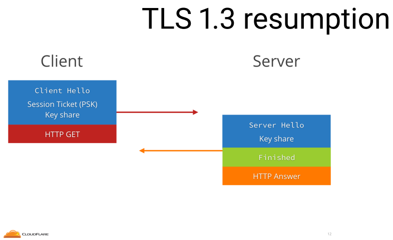
Server

Client Hello
Session ID / Ticket

Server Hello
Finished

Finished
HTTP GET

HTTP Answer



TLS 1.3 resumption

Client

Server

Client Hello
Session Ticket (PSK)
Key share
HTTP GET

Server Hello
Key share
Finished
HTTP Answer

References I

[1] S. Anthony, “It might be time to stop using antivirus,” Jan 2017. [Online]. Available: https://arstechnica.com/information-technology/2017/01/antivirus-is-bad/

[2] D. Mahal, “Antivirus software is bad for you and your computer,” Aug 2016. [Online]. Available: https://www.mahal.org/antivirus-software-is-bad-for-you-and-your-computer

[3] “Selinux – addressing access control security in labview rio devices.” [Online]. Available: http://www.ni.com/white-paper/52729/en/

[4] “Android m permissions and what they mean to you.” [Online]. Available: https://www.androidpit.com/android-m-permissions-explained

[5] L. Cobb, “Containers don’t contain the whole future: Vms are still app-ropos,” Aug 2016. [Online]. Available: https://yourdailytech.com/storage-architecture/containers-dont-contain-the-whole-future/

[6] “Analysis of ”dirtycow” kernel exploit,” Oct 2016. [Online]. Available: https://www.flashpoint-intel.com/blog/cybercrime/analysis-dirtycow-kernel-exploit/

References II

[7] “Exploiting and verifying shellshock: Cve-2014-6271,” Feb 2015. [Online]. Available: http://resources.infosecinstitute.com/bash-bug-cve-2014-6271-critical-vulnerability-scaring-internet/

[8] “‘heartbleed’ openssl vulnerability: A slow-motion train wreck.” [Online]. Available: http://searchsecurity.techtarget.com/news/2240217969/Heartbleed-OpenSSL-vulnerability-A-slow-motion-train-wreck

[9] [Online]. Available: https://xkcd.com/1938/

[10] “Replicant developers find and close samsung galaxy backdoor.” [Online]. Available: https://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-galaxy-backdoor

[11] J. Vincent, “Inaudible ultrasound commands can be used to secretly control siri, alexa, and google now,” Sep 2017. [Online]. Available: https://www.theverge.com/2017/9/7/16265906/ultrasound-hack-siri-alexa-google

[12] “All verizon android phones now come with app that allows oems backdoor access to install other apps without permission • r/android.” [Online]. Available: https://www.reddit.com/r/Android/comments/2nw54f/all_verizon_android_phones_now_come_with_app_that/

References III

[13] "[never settle] oneplus found to be collecting personally identifiable analytics data from phone owners," Oct 2017. [Online]. Available: https://www.androidpolice.com/2017/10/10/never-settle-oneplus-found-collecting-personally-identifiable-analytics-data-phone-owner

[14] A. Verma, "Backdoor in 30 seconds: New major amt security flaw is here to haunt intel laptops," Jan 2018. [Online]. Available: https://fossbytes.com/new-intel-amt-flaw-security/

[15] [Online]. Available: http://www.potaroo.net/ispcol/2014-03/ntpddos.html

[16] S. Khandelwal, "Largest ever 400gbps ddos attack hits europe uses ntp amplification," Feb 2014. [Online]. Available: https://thehackernews.com/2014/02/NTP-Distributed-Denial-of-Service-DDoS-attack.html

[17] "Man in the middle (mitm) attack," Aug 2017. [Online]. Available: https://www.veracode.com/security/man-middle-attack

[18] "Dkim: Protect your domain from email forging." [Online]. Available: https://postmarkapp.com/guides/dkim

[19] "How does spf protect your domain from email spoofing?" [Online]. Available: https://postmarkapp.com/guides/spf

References IV

[20] “Dmarc: Monitor & secure your email delivery.” [Online]. Available: https://postmarkapp.com/guides/dmarc

[21] “Increasing the strength of the zone signing key for the root zone,” Feb 2017. [Online]. Available: https://blog.verisign.com/security/increasing-the-strength-of-the-zone-signing-key-for-the-root-zone/

[22] Dan. [Online]. Available: https://www.makethenmakeinstall.com/2017/12/dnscrypt-proxy-as-a-forwarder-for-bind/

[23] “Dns privacy overview allison mankin & shumon huque, verisign labs dns-oarc fall workshop october 3, 2015.” [Online]. Available: http://slideplayer.com/slide/8356847/

[24] betterThanZero, “Java servlet to solve origin not allowed by access-control-allow-origin issue.” [Online]. Available: http://www.mysamplecode.com/2012/02/access-control-origin-not-allowed.html

[25] “How to delete hsts setting from chrome for a domain.” [Online]. Available: https://techglimpse.com/chrome-https-website-hsts-failed/

[26] F. Valsorda, “An overview of tls 1.3 and q&a,” Oct 2017. [Online]. Available: https://blog.cloudflare.com/tls-1-3-overview-and-q-and-a/

References V

[27] N. Sullivan, “Introducing tls 1.3,” Apr 2017. [Online]. Available: https://blog.cloudflare.com/introducing-tls-1-3/

Thank You