# 2550 Intro to cybersecurity L27: Wifi security \& Review 

abhi shelat

Attacker is able to $L E V E R A G E$ its resources.

I attack packet becomes 1000s.


Attacker is able to $\angle E V E R A G E$ its resources.

I attack packet becomes 1000s.

## How a TCP begins



## How a TCP begins



## SyN <br> How a TCP flood begins


victim stores each of these for timeout ( $\mathrm{I}-2 \mathrm{~min}$ )

Soon, entire
memory is consumed

## Amplification


victim stores
each of these for timeout ( $1-2 \mathrm{~min}$ )
No storage.


## $4 k b$



132 b packet causes 1024 b alloc. .

## Denial of Service BACKSCATTER



## a scope. Listen for "ACK/Syo"

Moore,Voelker, Savage 200I

|  | 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



use f(state) to<br>recompute state

## SYN Cookies



What cryptographic properties does the function $f$ require?


## Cuckoo TCP



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
d-172-27-45-104: abhi\$ dig +bufsize=4096 +dnssec any se @a.ns.se
; <<> DiG 9.8.1-P1 <<> +bufsize=4096 +dnssec any se @a.ns.se ;; global options: +cm
;; 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

$$
\text { DNS every with viction AS sac } 10 \text { !! }
$$

;" OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;, QUESTION SECTION:
L60x traffic amplifeietion


```
llllll
```



```
a.ns.se. }172800\mathrm{ IN RRSIG AAAA 5 3 172800 20120926005130 20120913041101 58656 se. pat/9jqrPpm/AP2czFcNCt477zy9wGgnngeuul+mJsN5I46py+4x0dVS 1dp25ul7BS4nwl/14yBcvxhPf2baviLKOqV16p+/yfcBE9Inw8p0013B
J9Ad87Lb+4rD2NeiFxAoj210pyR4OzsbLwjs1vclqEAzPHh+r661FuV0 Udg=
```



```
aV2Eg5T5LiRj2+RWJnQWxyh6TxtccKa5SdZ8aVz+bMGw IIE=
c.ns.se. IT2800 IN RRSIG A 5 3 17280020120925203628 2012091308110158656 se. ogrUBu72ccG3moTYF8mENrpOd3D/n0Z9GX3tHLpu3+kckgAZEMahYeB3 VhESvysenqXHy9K++STBH/c/BpZJnOnV109mctZX691/NC7AOcUWk8cE
2PYkSkRATryT2V4soJWbX1kGrc40UMLatgh6gY7.JPLvnkgeXOu1Fy8 Rjo=
ns.Se. _172800 IN RRSIG A S 3 172800 201209250502542012091218110258656 se. CqEp4MhqEMzW+Tvg5wTSIy/zqMoFBKNvlwr1590yShYfhtLQpXxKquLe IIHtXbY+kSaA8nKw7rhPGIO6QRbW8FYYIWyP/3KSoBsVTr+ZZ19A+1wd
e.ns.se. 172800 IN RRSIG A 5 3 172800 20120926152155 2012091302110158656 se. qoZASSLoC2MNObxYc8eTNWjNAlbhSzTyKgBbj4akMDyRQxTeA+YtdURZ If/5gvDjOOE7yNojuuAzHD8g+dyn5Z7cgmjLlyilo59huDUkSOObQZsz
PBLouj9+7NMt2Q5tLLJG2a9+BRFpsIE+nAxXMQRpldqJ2l+Zde+DNLU/ XTI=
M,
```





```
Zv7UlvVOJDKzGdCaphqj5ey1LI14pyg8QsBPqH2KzbJ8WE VYU=
```



```
cBigP2s+Pq96xQbAaqTEqXid5MuKDk2k6NMd QCg=
```




```
j.n.se. 172800 IN \
```

Query time: 126 msec
SERVER: 192.36.144.107\#53(192.36.144.107)
;; 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 -0 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
```



## 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.








 , It Italic, Futura Book, Futura Condensed ExtraBold, Futura Condensed Medium, Futura Medium, Futura Medium Italic, GB18030 Bitmap, Gabriola, Garamond, Garamond Bold, Garamond Itaic, Geeza Pro, Sans Bold Italic, Gill Sans Italic, Gill Sans Light, Gill Sans Light Italic, Gill Sans Ulitra 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, GIa















Figure 1. TSopt clock offset-sets for two sources in $\mathrm{BB}_{\mathrm{N}}$. Trace recorded on an OC48 link of a U.S. Tier 1 ISP, 2004-04-28 19:3021:30PDT. 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



## Second time

Addr for neu.edu?

"I just looked that up. The answer is 23.38 . 1 I 2.27 "

Local DNS Cache

# Solution: cache it 

two small problems: AUTHENTICITY
AVAILABILITY $\leftharpoonup$

## DNS Cache POISON



## FAKE RESPONSE can:

Addr for neu.edu?

provide the wrong answer for neu.edu
provide the wrong answer for other domains!

## FAKE RESPONSE can:

Addr for neu.edu?

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.

# packet UDP 

$$
2 f i x e s
$$

DNSSeC DNS - over-https.


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

## Needs to GUESS: Query ID




Attacker makes one bogus website <img src="http://bogusl.yahoo.com"> <img src="http://bogus2.yahoo.com">
<img src="http://bogus 1000.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


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


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


How to mitigate network attacks?


Statefull Packet Filter

Statefull Packet Inspection

Rules based on addr/port + header info above + state between each packet 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 I 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

UBI QuITIDUs. converient


DANGEROUSM insecure tio-

WPA2

WPA2 uses a passphrase to generate a PSK, which is used to generate a PMK and PTK.



Wifi 4-way handshake passphrase ssin.

[calculate PMK]
passphrase

[calculate PMK]

## Wifi 4-way handshake

 passphrase
[calculate PMK]
NonceA
passphrase

[calculate PMK]
[compute PTK]

## Wifi 4-way handshake

 passphrase[calculate PMK] NonceA
[calculate PMK]
[compute PTK]
NonceC + MsgIntCode
The KCK is used to compute MIC.

## Wifi 4-way handshake

 passphrase(1)

[calculate PMK]
NonceA
[compute PTK]
NonceC + MsgIntCode
The KCK is used to compute MIC.
KeyInstall + MsgIntCode
KeyInstalled + MsgIntCode

## How to attack a WPA2 session

 passphrase NonceA (a)NonceC + MsgIntCode
The KCK is used to compute MIC.

Listen for the NonceA, NonceC, MIC value, AP MAC, client MAC, SSID. $\rightarrow$ For each passphrase in the dictionary:

Use passphrase to compute PMK, PTK.
Use PTK to compute a MIC and test whether it is equal to captured one.

## Demo



Pixel phone sharing wifi

Attacker using packet capture over wifi

## Why does this attack succeed?

Most people use bad passwords for wifi.

Review

## Our main topics

Authentication, passwords -
Cryptography
Authorization
Social engineering
Systems security
Exploits: System, Web, Network

## Passwords and Authentication

What is authentication?

Classes of secrets?

Methods and attacks against passwords?

Passwords in the real (distributed) world, Oauth, 2fa.

Cryptography
keys - Privacy: Encryption.
Authenticity: Signatures \& MAC.

Hashing:

$$
\text { SHA. 250, SMA. } 512 \text { etc- }
$$

## Authorization

Access Control Check

## Basics of an access control check

- Given an access request from a subject, on behalf of a principal, for an object, return an access control decision based on the policy



## Authorization

Access Control Check

## Basics of an access control check

Two types
Access Control Models

- Discretionary Access Control (DAC)
- The kind of access control you are familiar with
- Access rights propagate and may be changed at subject's discretion
- Implemented in Windows and Linux
- Main issues:

Ambient authority (subjects inherit all permissions of principals)

- Confused deputies (subject doesn't know which principal it serves): setuid
- Mandatory Access Control (MAC)
- Access of subjects to objects is based on a system-wide policy managed by admin
- Bell-LaPadula: MAC for confidentiality (uses Multi Level Security)

Biba: MAC for integrity

- Main issues:

Inflexible and complicated to manage
Do not prevent side channel attack

- Given an access request from a subject, on behalf of a principal, for an object, return an access control decision based on the policy



## Social Engineering

1. Cognitive vulnerabilities

- Subconscious decisions may be made before you are consciously aware
- Behavioral, social, memory biases

2. Social engineering tactics

- Weaponizing cognitive vulnerabilities
- Pretexting and framing
- Elicitation and persuasion

3. Social engineering attacks

- Baiting, Tailgating
- Phishing, spear phishing
- CEO fraud
- Scareware


## System Security: Attack Surfaces

- Steal the device and use it
- Social Engineering
- Trick the user into installing malicious software
- Spear phishing
- OS-level attacks
- Backdoor the OS
- Direct connection via USB
- Exploit vulnerabilities in the OS or apps (e.g. email clients, web browsers)
- Network-level attacks
- Passive eavesdropping on the network
- Active network attacks (e.g. man-in-the-middle)


## Modern defense: Isolation

Most modern CPUs support protected mode
x86 CPUs support three rings with different privileges

- Ring 0: Operating System
- Code in this ring may directly access any device
- Ring 1,2 : device drivers
- Code in these rings may directly access some devices
- May not change the protection level of the CPU
- Ring 3: userland
- Code in this ring may not directly access devices
- All device access must be via OS APIs
- May not change the protection level of the CPU


## Modern defense: Isolation

Most modern CPUs support protected mode
x86 CPUs support three rings with different privileges

- Ring 0: Operating System
- Code in this ring may directly access any device
- Ring 1,2 : device drivers
- Code in these rings may directly access some devices
- May not change the protection level of the CPU
- Ring 3: userland
- Code in this ring may not directly access devices
- All device access must be via OS APIs
- May not change the protection level of the CPU


Physical Memory

Virtual Memory:


## Basis for tools

## Security Technologies

## Authentication

- Physical and remote access is restricted


## Access control

- Processes cannot read/write any file
- Users may not read/write each other's files arbitrarily
- Modifying the OS and installing software requires elevated privileges


Firewall

- Unsolicited communications from the internet are blocked
- Only authorized processes may send/receive messages from the internet

Anti-virus

- All files are scanned to identify and quarantine known malicious code

Logging

- All changes to the system are recorded
- Sensitive applications may also log their activity in the secure system log

Exploits

## Anatomy of an exploit



## Mitigations

- Stack canaries
- Compiler adds special sentinel values onto the stack before each saved IP
- Canary is set to a random value in each frame
- At function exit, canary is checked
- If expected number isn't found, program closes with an error
- Non-executable stacks
- Modern CPUs set stack memory as read/write, but no eXecute
- Prevents shellcode from being placed on the stack
- Address space layout randomization
- Operating system feature
- Randomizes the location of program and data memory each time a program executes

SQL Injection
dater interpreted as coke. bis flaw
'SELECT * FROM user_tbl WHERE user="\%s' AND pw="\%s";'


## Systems Security Principles



1. Fail-safe Defaults
2. Separation of Privilege
3. Least Privilege
4. Open Design
5. Economy of Mechanism
6. Complete Mediation
7. Compromise Recording
8. Work Factor


## Cybersecurity and Ethics

- Many laws govern cybersecurity
- Designed to help prosecute criminals
- Discourage destructive or fraudulent activities
- However, these laws are broad and often vague
- Easy to violate these laws accidentally
- Security professionals must be cautious and protect themselves
- Cybersecurity raises complex ethical questions
- When and how to disclose vulnerabilities
- How to handle leaked data
- Line between observing and enabling crime
- Balancing security vs. autonomy
- Ethical norms must be respected
- Rights and expectations of individuals and companies
- Community best-practices


## 5 Lessons

## mit

Lesson 1:
Never trust input from the user

Lesson 2:
Never mix code and data

## Lesson 3:

Use the best tools at your disposal

Lesson 4:


Vigilance

Lesson 5:
Patch!

## Topics we did not cover

- Crimeware Botnets
- Post-quantum cryptography
- Crypto currencies and smart contracts
- Protocol Security (TLS, wireless, SDN)
- Side channel attacks
- Secure Hardware Technologies (TPM, TXT)
- Distributed System Security and Resilience
- Privacy and regulations
- Fuzzing and software testing
- Formal verification
- Mobile and IoT security
- Machine Learning for Security
- Adversarial Machine Learning

Failures
Operation

- mplementation

D ESIGN
A bStraction

## TAs deserve thanks!

Kieran Croucher, Noelle Floyd, Byron Kress, Sarah Lackey, Nathan Pedowitz, Donald Sea, Riddhi Adhiya, Martin Petrauskas

Please submit a TRACE course review

