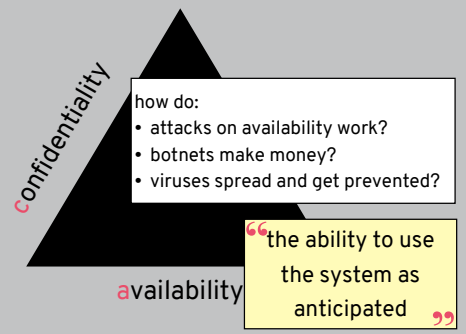
SECURITY (COMP0141): AVAILABILITY

UCL

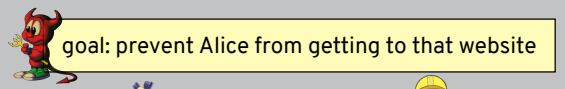
AVAILABILITY



how do:
- attacks on availability work?
- botnets make money?
- viruses spread and get prevented?

"the ability to use the system as anticipated"

WHY IS AVAILABILITY IMPORTANT?



http://me.bob.com/hi.html

can't get stuff done

can't run business (make $)

Availability is important both for users and for services

THREATS TO AVAILABILITY

Hardware failures

Denial of service (DoS)

Malware

Hardware failures are not adversarial so we won't be talking about them

THREATS TO AVAILABILITY

Hardware failures

Denial of service (DoS)

Malware

THREAT MODEL FOR DOS

goal: take down a service

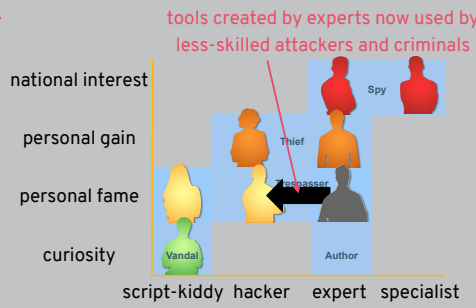
simple: have one machine
distributed: have many machines

$: small amount of computational power
$$$: large amount of computational power

clueless: little technical ability
savvy: strong technical ability

The goal (motivation) of the attacker is to prevent availability, they might have different capabilities. Here the threat model is a little different than we've seen since it's more risk management and less binary

THREAT LANDSCAPE



(David Aucsmith, Microsoft)

Important to remember that people can do this with far fewer capabilities than were previously required

---

ANONYMOUS

politically motivated attacks
targets advertised on social media
join by downloading Loic program
famous targets: PayPal, Scientology, Sony, Visa

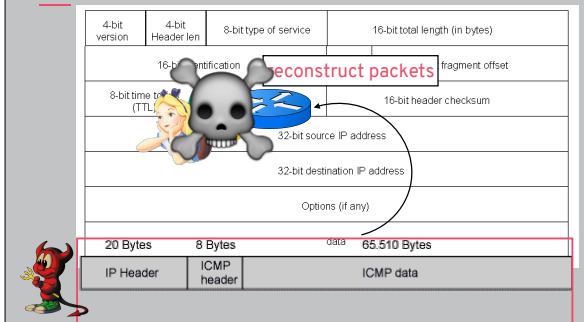
It can also be even easier to carry out attacks by just joining a large group (requires no technical sophistication at all)

HOW DOES DOS WORK?

“Ping of death”

Let’s start with a very simple DoS attack: the ping of death

PING OF DEATH



We don’t need to worry about the technical details, but basically the attacker can construct a packet that’s too big and causes a machine to die when it tries to reconstruct

PING OF DEATH

vulnerability?

reconstruction fails on packets that are too big

threat?

simple: have one machine

$: small amount of computational power

clueless(-ish): little technical ability

protection?

easy: filter out these packets before reconstruction

This is very simple but luckily easy to prevent

HOW DOES DOS WORK?

"Ping of death"

Unintentional

This is not an attack but it is very common

UNINTENTIONAL

Maybe festival tickets go on sale and the site crashes, or a meme goes viral

UNINTENTIONAL

vulnerability?

inability to predict spikes in popularity

threat?

distributed: have many machines

$$$: large amount of computational power

clueless: little technical ability (not even an attack!)

protection?

hard: no real way to know

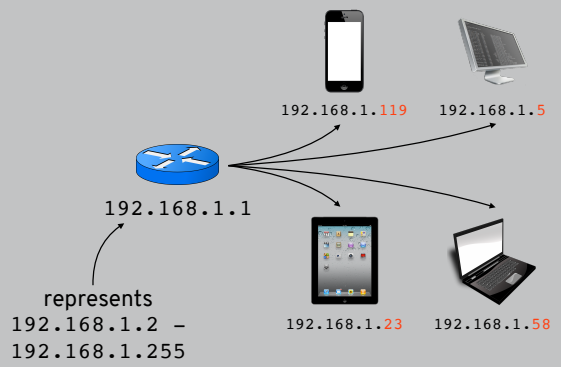
This is hard to prevent since we don't really know what will go viral and what won't

HOW DOES DOS WORK?

"Ping of death"
Unintentional
Smurf attack

15

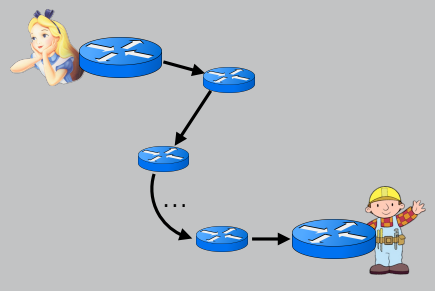
BROADCAST ADDRESSES



16

A smurf attack exploits the fact that user devices are not connected to the main Internet, but go through a router. Broadcast allows us to reach them all at the same time

IP SPOOFING



17

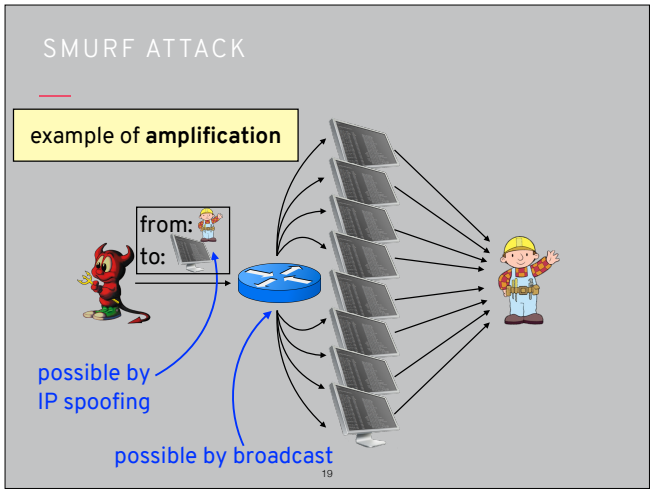
IP SPOOFING

4-bit version	4-bit Header len	8-bit type of service	16-bit total length (in bytes)
16-bit identification		3-bit flags	13-bit fragment offset
8-bit time to live (TTL)	8-bit protocol	16-bit header checksum	
Professor Evil's ~~Alice's~~ IP address			
Bob's IP address			
Options (if any)			
"I want the content at `hi.html`"			

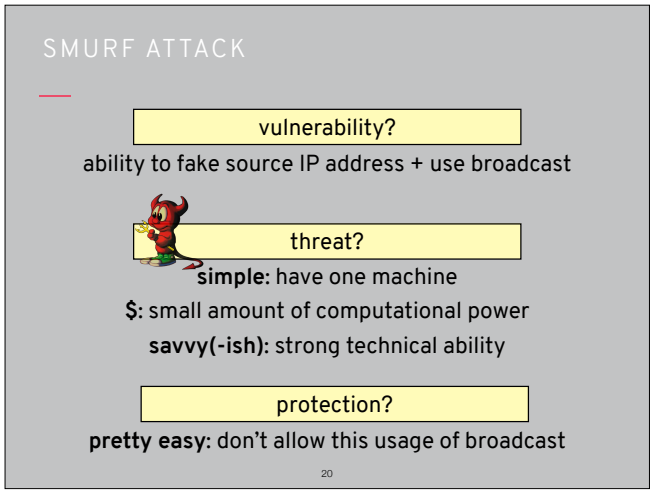
the Internet was not designed for security!

18

Remember, there is no authentication on the Internet so it is easy to spoof IP addresses (i.e., pretend something came from a place even if it didn't)



Combining these two things allows for the full attack: the attacker broadcasts to a lot of devices a message that looks like it came from Bob, and when they all go to respond to Bob he gets overwhelmed



If we don't allow broadcast then we can prevent this attack

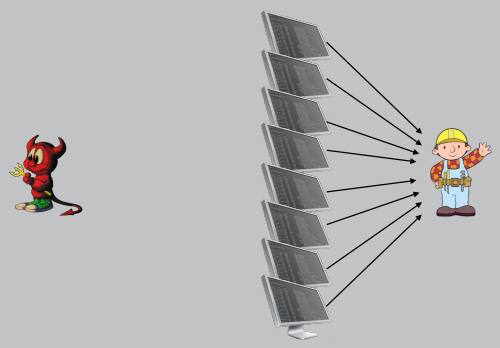
HOW DOES DOS WORK?

"Ping of death"
Unintentional
Smurf attack
DDoS

21

DDoS is very serious

DISTRIBUTED DOS (DDOS)



22

Basically it's like a smurf attack, except the machines are all just controlled by the attacker

DDOS

vulnerability?

none, really!

threat?

distributed: have many machines

$$$: large amount of computational power

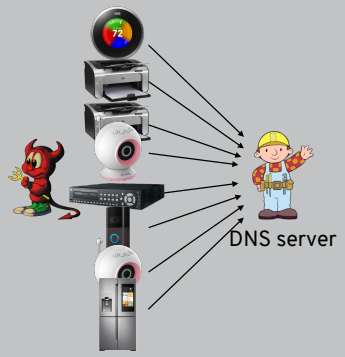
savvy: strong technical ability

protection?

very difficult!

23

EXAMPLE: MIRAI (2016)

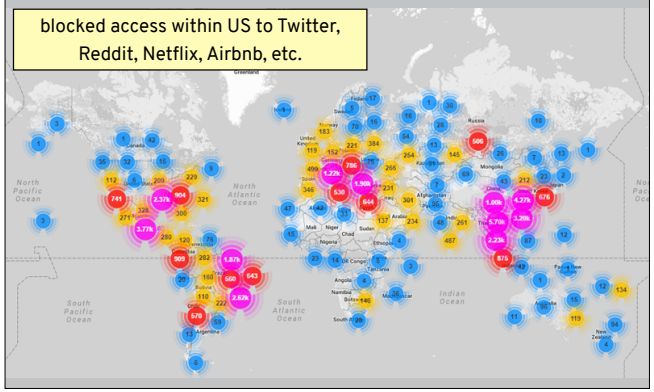


24

One example: Mirai worked by compromising IoT devices and forming a botnet, then attacking DNS resolvers rather than a single site or service

EXAMPLE: MIRAI (2016)

blocked access within US to Twitter, Reddit, Netflix, Airbnb, etc.



It was quite a devastating attack!

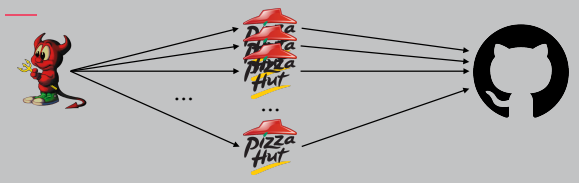
EXAMPLE: GITHUB ATTACK (2018)

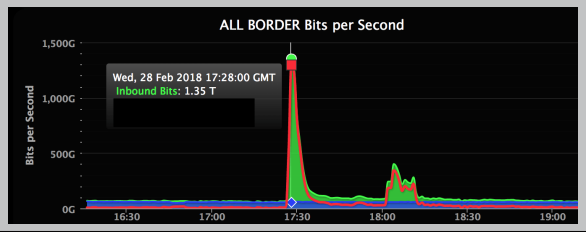
You can achieve amplification without broadcast

This is the intuition behind a **memcached** attack – no botnets needed!

Memcached attacks are the modern version of a smurf attack, use spoofing combined with amplification

EXAMPLE: GITHUB ATTACK (2018)





Peak of the attack saw 1.35 terabytes per second directed at Github's servers (126.9 million packets per second). At the time this was the biggest DDoS attack ever recorded

---

EXAMPLE: GITHUB ATTACK (2018)

You can achieve amplification without broadcast

This is the intuition behind a **memcached** attack – no botnets needed!

Actually though, Github survived this attack!

How did Github survive an attack of this size?

DDOS PROTECTION

risk management

attack

defence

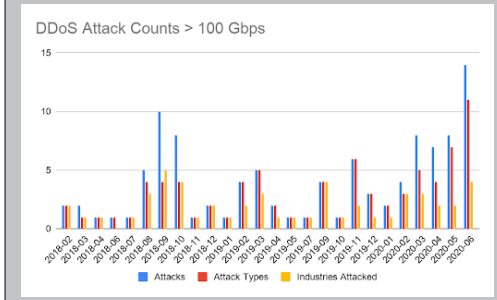
CLOUDFLARE

Akamai

29

Protection here is very much an arms race, there are companies that offer it as a service but there's no silver bullet.

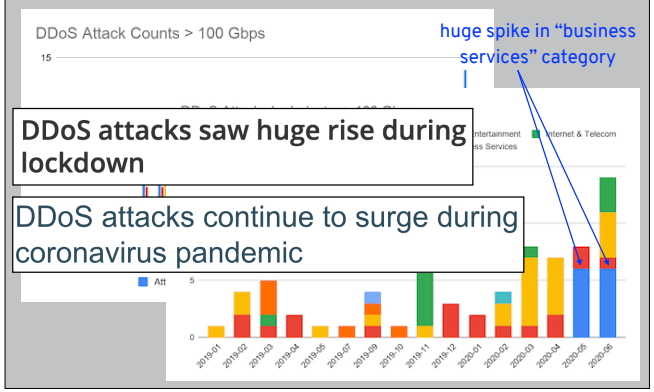
DDOS IS INCREASINGLY POPULAR



30

DDoS is very much on the rise

DDOS IS INCREASINGLY POPULAR



This is especially true with so many people working from home around the world – can have an especially high impact

---

DDOS AS A SERVICE

threat?

distributed: have many machines

$$$: large amount of ~~computational power~~ money

savvy: strong technical ability

booter (**stresser**) service will do attack for you, hosted with **bulletproof** providers who don't care about content and don't comply with law enforcement

The attacker doesn't really need the things we said, just needs money. DDoS is a service today so they can hire a booter service (can often pay with bitcoins). These services are themselves hosted on bulletproof providers that don't care about content

DDOS *NOT* AS A SERVICE

q: but how do booter services work? how to do it myself?
a: use a **botnet**.

But how do the people you pay carry out the attack?