

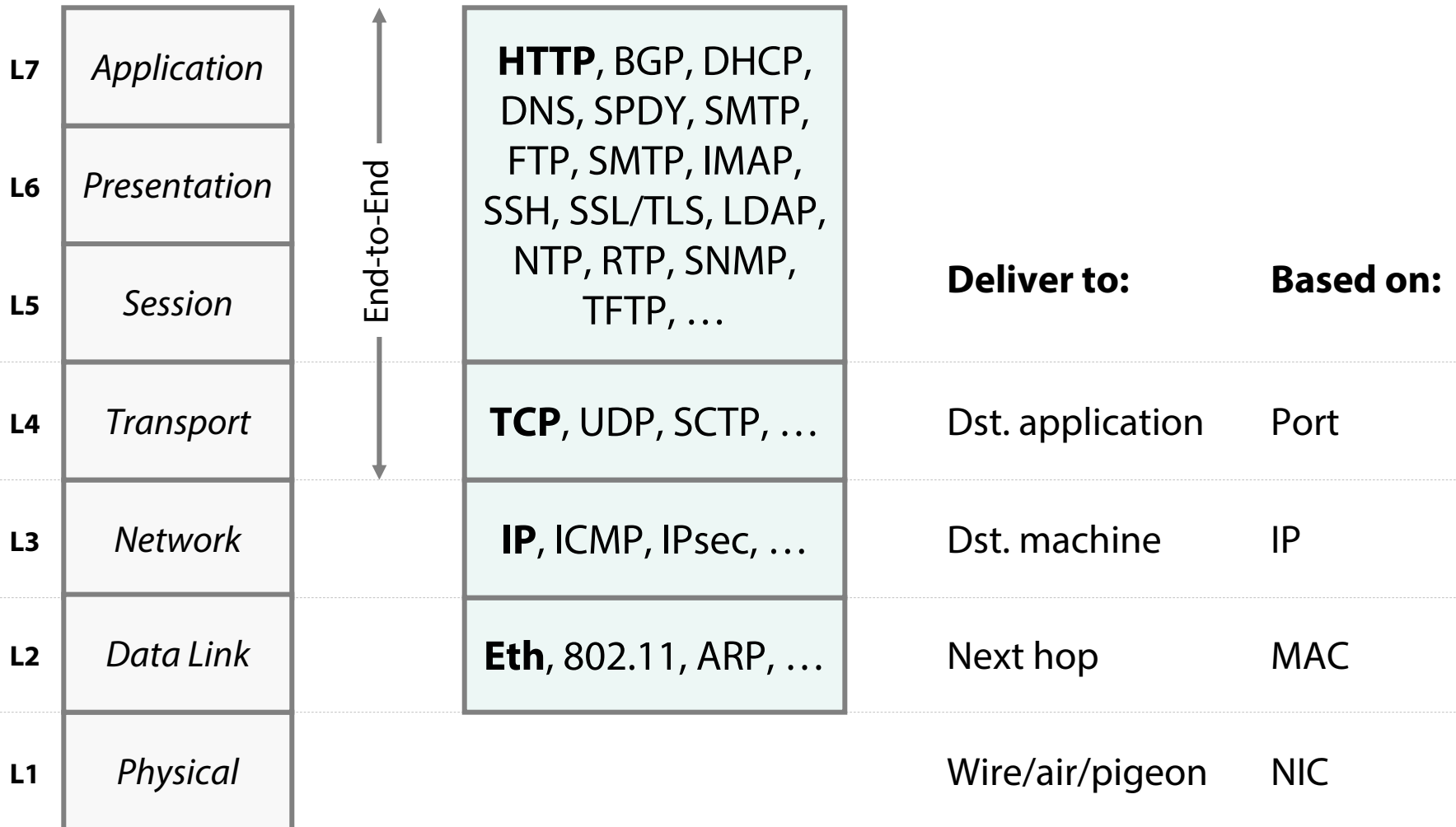
CSE508 Network Security (PhD Section)

2/3/2015 **Lower Layers and Core Protocols**

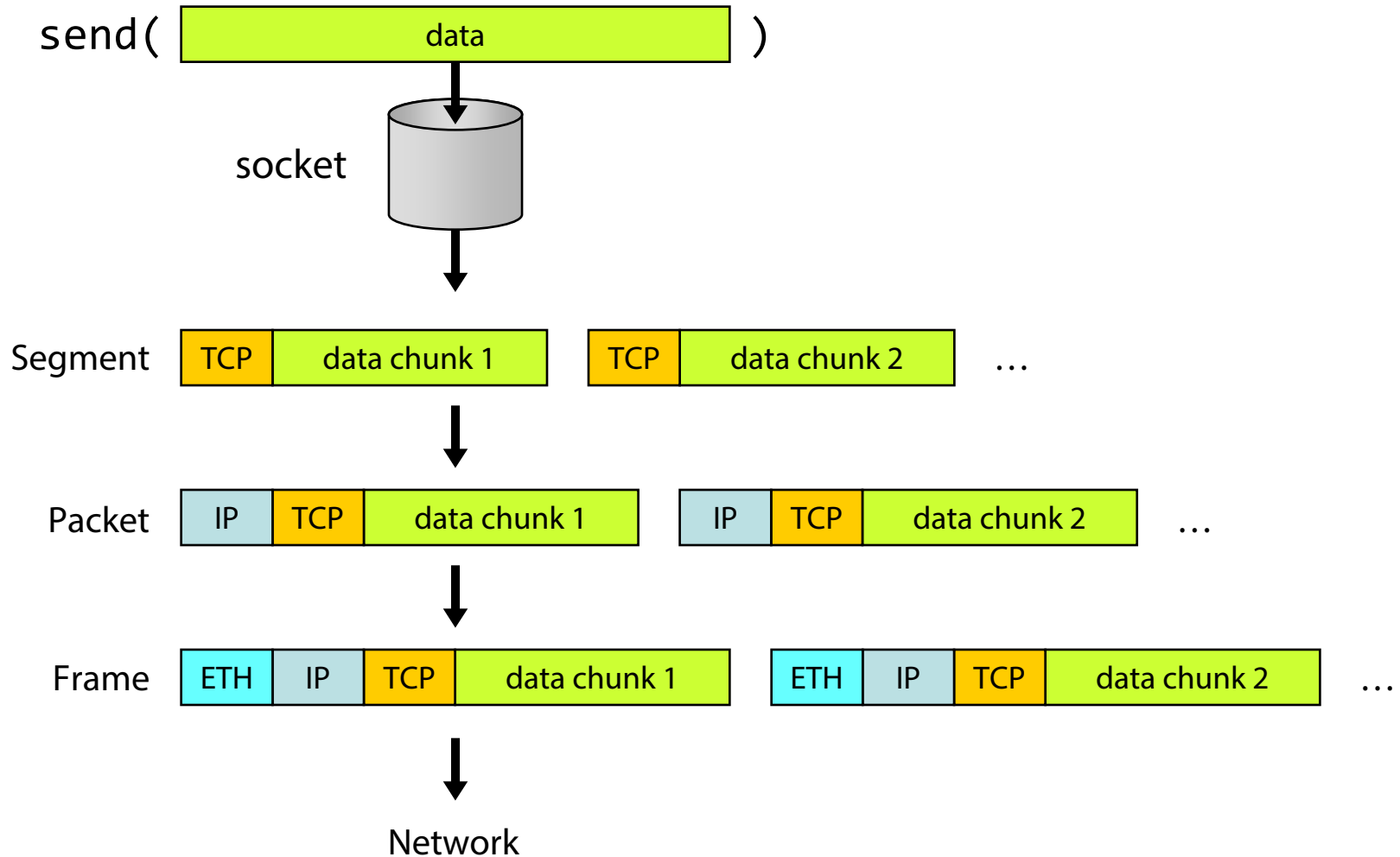
Michalis Polychronakis

*Stony Brook University*

# Basic Internet Protocols (OSI Model vs. Reality)



# Streams vs. Packets



# Physical Layer Attacks

## Wiretapping

Not needed for WiFi networks! → WPA

## Wirecutting

## Jamming

## Electronic emanations

## Tracking

Device fingerprinting

Physical device localization



# Link Layer Attacks

## Eavesdropping

### Hubs vs. switches

CAM table exhaustion: can turn a switch into a hub  
macof (part of dsniff)

### ARP Spoofing

## Spoofing

Impersonate another machine and receive its traffic

Change MAC address to get 30' more of free WiFi

Hide the device's vendor (first three bytes of MAC address)

## DoS

Flooding

DHCP starvation

Deauth (WiFi)

## Rogue access point

## ARP Cache Poisoning

Address Resolution Protocol: a new machine joins a LAN; How can it find the MAC addresses of neighbors?

ARP request (broadcast): who has IP 192.168.0.1?

ARP reply by 192.168.0.1: Hey, here I am, this is my MAC address

ARP replies can be *spoofed*: IP to MAC mapping is not authenticated

Traffic sniffing/manipulation through MitM

ARP reply to victim, mapping gateway's IP to attacker's MAC

ARP reply to gateway, mapping victim's IP to attacker's MAC

Just forward packets back and forth

Tools: arpspoof (ss1strip), ettercap, nemesis, ...

Defenses: static ARP entries, ARPwatch, managed switches

# Deauth Attacks

Send a spoofed deauth frame to AP with victims' address (no authentication!)

Recently a hotel chain was fined for deauthing customers' devices

- Force clients to pay for hotel WiFi

But, deauthing sometimes is also used as a protection mechanism

- Prevent rogue access points

Tools: `aireplay-ng` (`aircrack-ng`), `deauth` (`metasploit`)



Search



Take Act

**Federal Communications Commission**  
445 12th Street, S.W.  
Washington, D.C. 20554

News Media Information 202 / 418-0500  
Internet: <http://www.fcc.gov>

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action.  
See MCI v. FCC, 515 F 2d 385 (D.C. Cir. 1974).

FOR IMMEDIATE RELEASE:  
October 3, 2014

NEWS MEDIA CONTACT:  
Neil Grace, 202-418-0506  
E-mail: [Neil.Grace@fcc.gov](mailto:Neil.Grace@fcc.gov)

## **MARRIOTT TO PAY \$600,000 TO RESOLVE WIFI-BLOCKING INVESTIGATION**

*Hotel Operator Admits Employees Improperly Used Wi-Fi Monitoring System to Block Mobile Hotspots;  
Agrees to Three-Year Compliance Plan*

Washington, D.C. –Marriott International, Inc. and its subsidiary, Marriott Hotel Services, Inc., will pay \$600,000 to resolve a Federal Communications Commission investigation into whether Marriott intentionally interfered with and disabled Wi-Fi networks established by consumers in the conference facilities of the Gaylord Opryland Hotel and Convention Center in Nashville, Tennessee, in violation of Section 333 of the Communications Act. The FCC Enforcement Bureau's investigation revealed that Marriott employees had used containment features of a Wi-Fi monitoring system at the Gaylord Opryland to prevent individuals from connecting to the Internet via their own personal Wi-Fi networks, while at the same time charging consumers.



## Rogue Access Points

No authentication of the AP to the client

Set up fake access point with an existing SSID or just an enticing name

Starbucks-FREE-WiFi

“Auto-connect”/“Ask to join network”  
features greatly facilitate this kind of attacks

Pineapple, Power Pwn, ...

Wireless backdoor

Ship an iPhone/special purpose device to  
an office and use 4G connection for C&C

Hide a tiny AP in a wall plug etc.

Detection

NetStumbler: show all WiFi networks

RF monitoring systems

Wireless IDS/IPS



# Network Layer Attacks

ICMP (Internet Control Message Protocol): Used to exchange error messages about IP datagram delivery

- Smurf Attack (DoS with spoofed broadcast Echo request)

- Reconnaissance

- Exfiltration using ICMP Tunneling

- Organizations typically block incoming/outgoing ICMP traffic

IP spoofing: conceal the real IP address of the sender

- Mostly used in DDoS attacks

- Ingress and egress filtering limit its applicability

# TCP Handshake

## Sequence/acknowledgement numbers

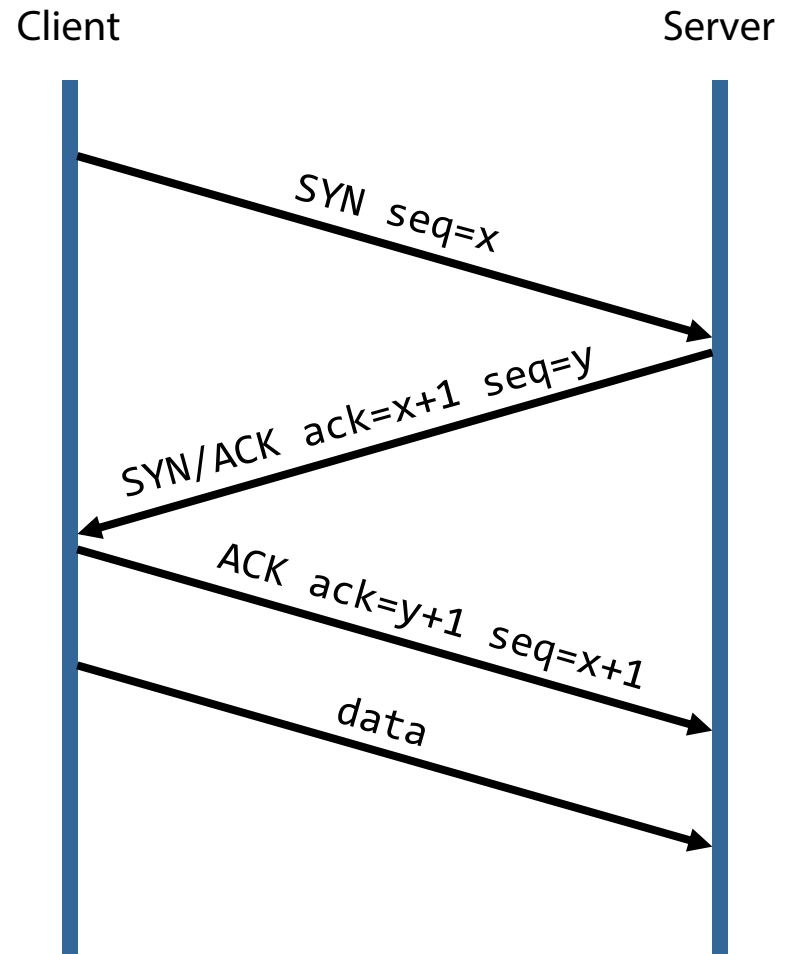
Retransmissions, duplicate filtering, flow control

*Seq*: the position of the segment's data in the stream

*The payload of this segment contains data starting from X*

*Ack*: the position of the next expected byte

*All bytes up to X received correctly, next expected byte is X+1*



# TCP Issues

## Sequence Number Attacks (next lecture)

- TCP connection hijacking/spoofing

- DoS (connection reset)

## Port scanning (future lecture)

## OS Fingerprinting

- Intricacies of TCP/IP stack implementations

## DoS:

- Resource exhaustion

- Blind RST injection

# SYN Flooding

Flood server with spoofed connection initiation requests (SYN packets)

Saturate server's max number of concurrent open sockets: no more connections can be accepted

Each half-open connection consumes memory resources

SYN/ACKs sent, but ACKs never come...

## Mitigation

Drop half-open connections after reaching a certain threshold (FIFO/random)

SYN cookies

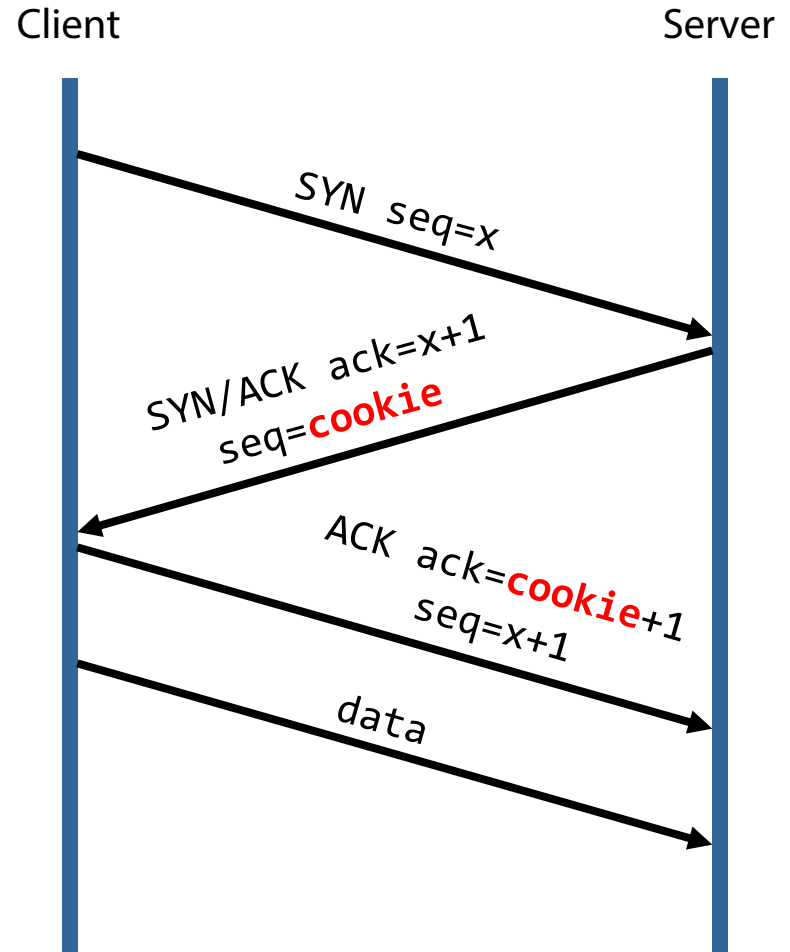
# SYN Cookies

Don't drop connections after SYN queue fills up

Send SYN/ACK with special "cookie" seq

Secret function of the src/dst IP, src/dst port, coarse timestamp

Stateless! SYN queue entry is rebuilt based on the returned cookie value in the ACK



# Connection Flooding

DDoS: saturate the server with many established connections

Can't use spoofing: just use bots...

For forking servers, the whole system might freeze (process exhaustion)

Slowloris attack: slowly send a few bytes at a time to keep the connections open

Keep the server busy with "infinite" requests by periodically sending more and more HTTP headers

Requires minimal bandwidth

# Amplification/Reflection Attacks

Like the ICMP Smurf attack

Abuse services that reply to requests with large responses

Attacker sends a *small* packet with a forged source IP address  
Server sends a large response to the victim (forged IP address)

UDP: connectionless protocol → easy to spoof

Used by many services:

NTP, DNS, SSDP, SNMP, NetBIOS, QOTD, CharGen, ...





# Technical Details Behind a 400Gbps NTP Amplification DDoS Attack

13 Feb 2014 by [Matthew Prince](#).

[g+](#) 118 [in](#) Share 209 [f](#) Like 26 [t](#) Tweet 933



On Monday we mitigated a large DDoS that targeted one of our customers. The attack peaked just shy of 400Gbps. We've seen a handful of other attacks at this scale, but this is the largest attack we've seen that uses NTP amplification. This style of attacks has grown dramatically over the last six months and poses a significant new threat to the web.

## CloudFlare blog

Contact our team

- US callers**  
1 (888) 99-FLARE
- UK callers**  
+44 (0)20 3514 6970
- International callers**  
+1 (650) 319-8930

[Full feature list and plan types](#)

CloudFlare provides performance and security for any website. More than 2 million websites use CloudFlare.

There is no hardware or software. CloudFlare works at the DNS level. It takes only 5 minutes to sign up. To learn more, please visit our website

## CloudFlare features

- [Overview](#)
- [CDN](#)
- [Optimizer](#)
- [Security](#)

# Amplification Factor

Christian Rossow. *Amplification Hell: Revisiting Network Protocols for DDoS Abuse* – NDSS'14

Protocol	BAF			PAF <i>all</i>	Scenario
	<i>all</i>	50%	10%		
SNMP v2	6.3	8.6	11.3	1.00	<i>GetBulk</i> request
NTP	556.9	1083.2	4670.0	3.84	Request client statistics
DNS <sub>NS</sub>	54.6	76.7	98.3	2.08	ANY lookup at author. NS
DNS <sub>OR</sub>	28.7	41.2	64.1	1.32	ANY lookup at open resolv.
NetBios	3.8	4.5	4.9	1.00	Name resolution
SSDP	30.8	40.4	75.9	9.92	<i>SEARCH</i> request
CharGen	358.8	n/a	n/a	1.00	Character generation request
QOTD	140.3	n/a	n/a	1.00	Quote request
BitTorrent	3.8	5.3	10.3	1.58	File search
Kad	16.3	21.5	22.7	1.00	Peer list exchange
Quake 3	63.9	74.9	82.8	1.01	Server info exchange
Steam	5.5	6.9	14.7	1.12	Server info exchange
ZAv2	36.0	36.6	41.1	1.02	Peer list and cmd exchange
Salinity	37.3	37.9	38.4	1.00	URL list exchange
Gameover	45.4	45.9	46.2	5.39	Peer and proxy exchange

TABLE III: Bandwidth amplifier factors per protocols. *all* shows the average BAF of all amplifiers, 50% and 10% show the average BAF when using the worst 50% or 10% of the amplifiers, respectively.

# Routing

Packets are routed based on their dst IP address and the routers' forwarding tables

Interdomain routing: **BGP** (Border Gateway Protocol)

Exchange routing and reachability information between ASes

Advertisements contain a prefix and a list of ASes to traverse to reach that prefix

## Attack types

*Blackholing*: false route advertisements to attract and drop traffic

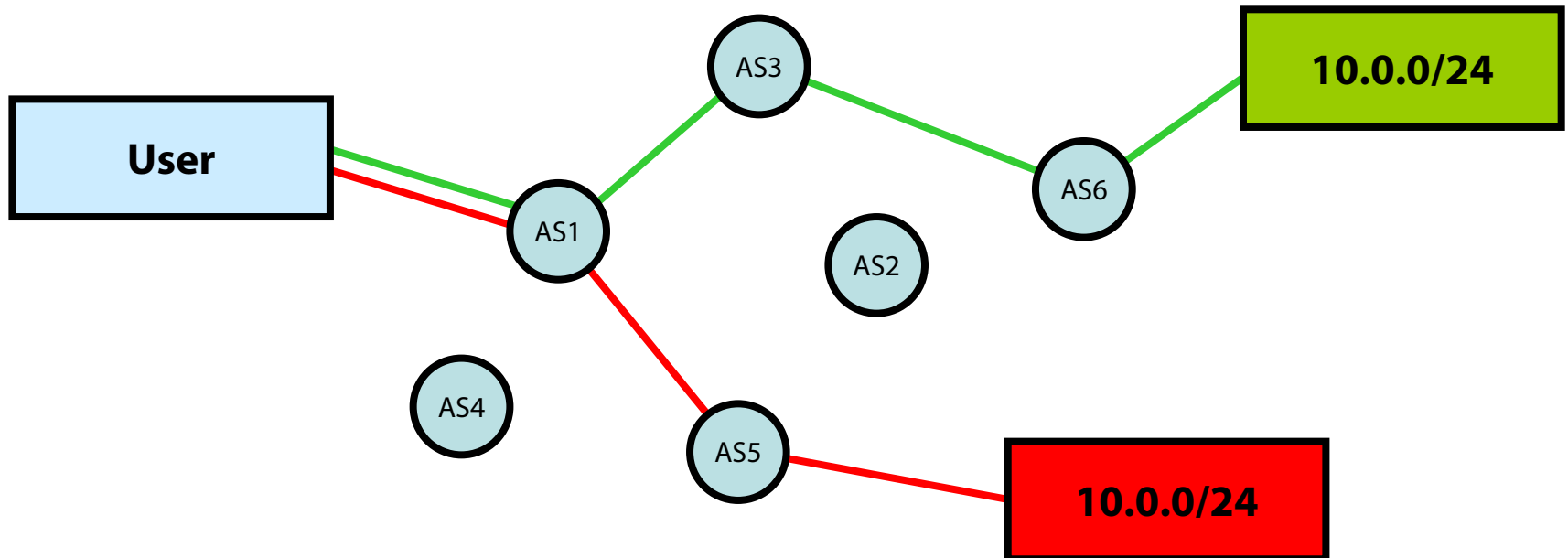
*Redirection*: force traffic to take a different path, either for eavesdropping/manipulation (MitM) or causing congestion

*Instability*: frequent advertisements and withdrawals and/or increased BGP traffic to cause connectivity outages

# Prefix Hijacking

Announce someone else's prefix

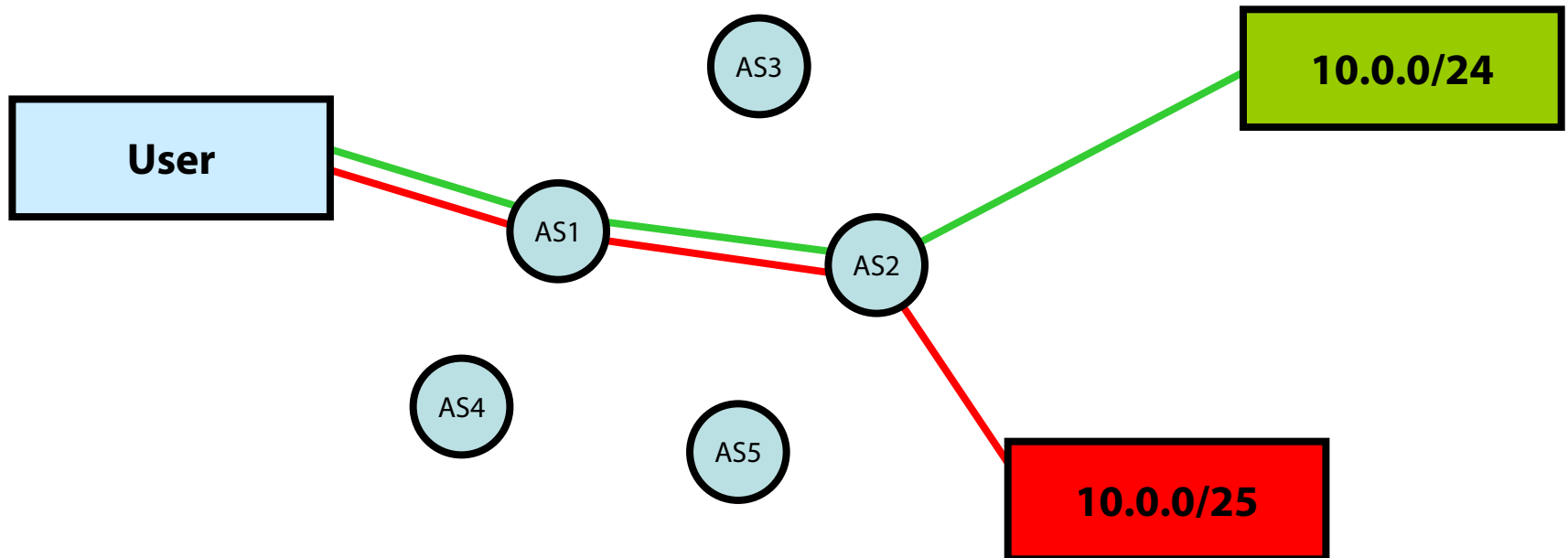
Victim prefers shortest path



# Prefix Hijacking

Announce a more specific prefix than someone else

Victim prefers more specific path





What network are you living on? SEE WHAT FiOS INTERNET CAN DO FOR YOU.

Learn More

6 MONTHS FOR \$5 + FREE HAT.

SUBSCRIBE GIVE A GIFT RENEW INTERNATIONAL ORDERS

THREAT LEVEL

Glitches and Bugs Sunshine and Secrecy

FOLLOW WIRED [Twitter] [Facebook] [RSS]

# Pakistan's Accidental YouTube Re-Routing Exposes Trust Flaw in Net

BY RYAN SINGEL 02.25.08 | 10:37 AM | PERMALINK

[Facebook Share] 4 [Twitter Tweet] 4 [Google+ +1] 0 [LinkedIn Share] [Pinterest Pin It]



Secure Your Cloud



cavirin.com

Free download: Best Practices For Ensuring Cloud Compliance.

Threat Protection Tool

C++ Static Analysis

AVG® Business Research

Security White Papers

Cisco® ACI Virtualization

IoT Security Explained

Immediate Risk Assessment

# Domain Name Service

DNS maps domain names to IP addresses

- Distributed database

- Hierarchically divided name space

- Local caching resolvers

- UDP (TCP sometimes used for long queries and zone transfers)

## Main security issues

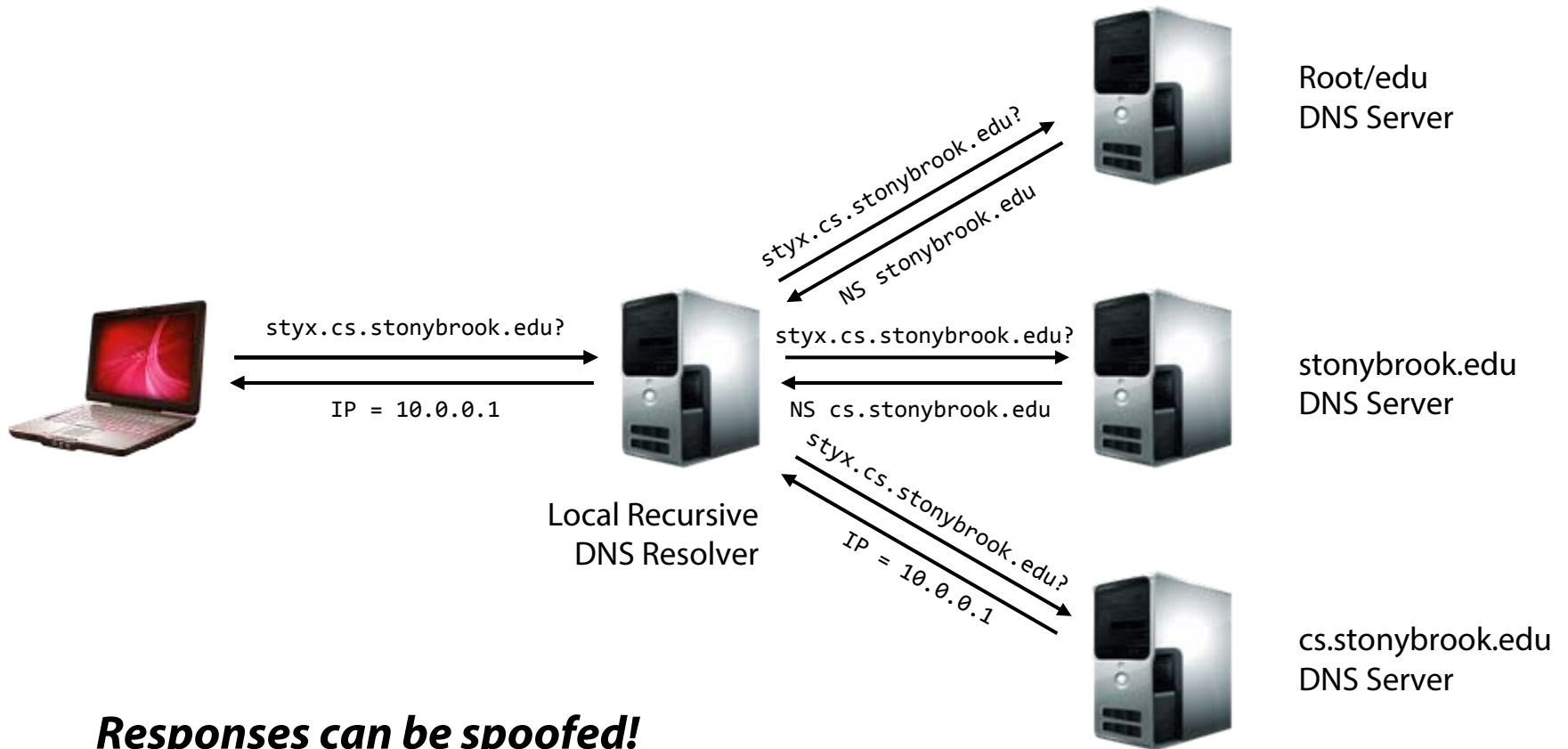
- DNS spoofing (also used for censorship)

- DNS cache poisoning

- Name-based authentication



# Recursive DNS resolution



***Responses can be spoofed!***

*Cached result will point to attacker's address*



# DNS TXID

Synchronization mechanism between  
DNS clients and servers

## 16-bit transaction identifier

Randomly chosen for each query

Response accepted only if TXIDs match

Cached according to TTL (e.g., one day)

## Attacker has to win a race

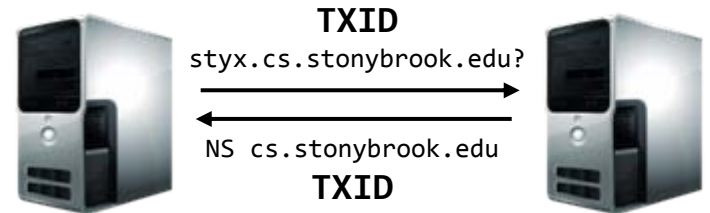
Guess correct TXID

Response's src IP and dst port should match  
query's dst IP and src port

## It's possible!

Bellovin's cache contamination attacks (1991)

Kaminsky attack (2008)



# Kaminsky Attack

Attacker wants to compromise example.com

Query the target resolver with any subdomain not in the cache

Non-existent subdomains are fine: foo1.example.com

Not affected by TTL (e.g., as would be the case for www.example.com)

Causes the target resolver to query the authoritative server(s) for this domain

The attacker floods the resolver with a large number of forged responses

each containing a different guess of the query's TXID

**Fake referral**

```
;; ANSWER SECTION:  
foo1.example.com.      120  IN  A   10.0.0.10  
;; AUTHORITY SECTION:  
example.com.          86400  IN  NS  
www.example.com.  
;; ADDITIONAL SECTION:  
www.example.com.     604800  IN  A   10.6.6.6
```

***If the race is lost, repeat with a different subdomain!***

# Misc DNS Attacks

## Attacking registrars

Social engineering, stolen credentials, ...

## Drive-by pharming

A malicious web page contains JavaScript code that alters the local router's DNS server

## Malware can change the system's DNS server

DNSChanger

## DoS on root/critical servers

# Passive Network Monitoring

## Packet capture

- Headers or full payloads

- Network taps

- Router/switch span/mirror ports

- Not only for sniffing passwords!*

## Netflow export

- Connection-level traffic summaries

- Built-in capabilities in most routers

## Non-intrusive: invisible on the network

## Basis for a multitude of defenses

- IDS/IPS

- Anomaly detection

- Network forensics

## Sophisticated attackers might erase all evidence on infected hosts

- Captured network-level data might be all that is left

```
15:07:16.609603 IP 139.91.171.116.1049 > 239.255.255.250.1900: UDP, length 122
15:07:16.821980 IP 139.91.171.116.1049 > 239.255.255.250.1900: UDP, length 122
15:07:16.822297 IP 139.91.70.148.8008 > 239.255.255.250.1500: UDP, length 122
15:07:16.822370 IP 139.91.70.26.8008 > 239.255.255.250.1900: UDP, length 122
15:07:16.825070 IP 139.91.70.254 > 224.0.0.13: P:IPv2, Assert, length: 28
15:07:16.826708 IP 139.91.70.253 > 224.0.0.13: P:IPv2, Assert, length: 28
15:07:16.869700 endnode-hello endnode vers 2 eco 0 ueco 0 src 1.10 blksize 2
rtr 0.0 hello 10 data 2
15:07:16.929894 IP 139.91.171.116.1049 > 239.255.255.250.1900: UDP, length 122
15:07:17.043099 IP 139.91.171.116.1049 > 239.255.255.250.1900: UDP, length 122
15:07:17.119970 IP 139.91.70.254.1985 > 224.0.0.2.1985: HSRPv0-hello 20:
tandby group=70 addr=139.91.70.80
15:07:17.149897 IP 139.91.171.116.1049 > 239.255.255.250.1900: UDP, length 122
15:07:17.259974 IP 139.91.171.116.1049 > 239.255.255.250.1900: UDP, length 122
15:07:17.284411 802.ld config 2000 00:d0:00:dc:50:45.2105 root 2000.00:d0:
50:45 pathcost 0 age 0 max 20 hello 2 fdelay 15
15:07:17.369924 IP 139.91.171.116.1049 > 239.255.255.250.1900: UDP, length 122
15:07:17.696390 endnode-hello endnode vers 2 eco 0 ueco 0 src 1.10 blksize 2
rtr 0.0 hello 10 data 2
15:07:18.764737 IP 139.91.70.253 > 224.0.0.13: P:IPv2, Assert, length: 28
15:07:18.963784 IP 139.91.70.253.1985 > 224.0.0.2.1985: HSRPv0-hello 20:
active group=70 addr=139.91.70.80
15:07:18.988021 IP 139.91.70.254 > 224.0.0.10: EIGRP Hello, length: 40
15:07:18.999754 IP 139.91.70.253 > 224.0.0.10: EIGRP Hello, length: 40
15:07:19.291410 802.ld config 2000 00:d0:00:dc:50:45.2105 root 2000.00:d0:
50:45 pathcost 0 age 0 max 20 hello 2 fdelay 15
15:07:19.351836 00:d0:d3:36:67:54 > 01:00:0c:dd:dd:dd sap aa u:/c
15:07:19.923630 endnode-hello endnode vers 2 eco 0 ueco 0 src 1.10 blksize 2
rtr 0.0 hello 10 data 2
15:07:20.004023 IP 139.91.70.254.1985 > 224.0.0.2.1985: HSRPv0-hello 20:
tandby group=70 addr=139.91.70.80
15:07:20.821598 IP 139.91.70.148.8008 > 239.255.255.250.1500: UDP, length 122
15:07:21.292518 802.ld config 2000 00:d0:00:dc:50:45.2105 root 2000.00:d0:
50:45 pathcost 0 age 0 max 20 hello 2 fdelay 15
15:07:21.609511 IP 139.91.70.46.631 > 139.91.70.255.631: LDP, length 153
15:07:21.883722 IP 139.91.70.253.1985 > 224.0.0.2.1985: HSRPv0-hello 20:
active group=70 addr=139.91.70.80
15:07:22.129438 IP 139.91.70.46.41988 > 139.91.70.255.111: UDP, length 117
15:07:22.864093 IP 139.91.70.254.1985 > 224.0.0.2.1985: HSRPv0-hello 20:
tandby group=70 addr=139.91.70.80
15:07:23.293656 802.ld config 2000 00:d0:00:dc:50:45.2105 root 2000.00:d0:
50:45 pathcost 0 age 0 max 20 hello 2 fdelay 15
15:07:23.443208 IP 139.91.70.254 > 224.0.0.10: EIGRP Hello, length: 40
15:07:23.671846 IP 139.91.70.253 > 224.0.0.10: EIGRP Hello, length: 40
15:07:24.009474 IP 139.91.70.46.631 > 139.91.70.255.631: LDP, length 117
15:07:24.594258 arp who-has 139.91.70.181 tell 139.91.70.254
15:07:24.755842 IP 139.91.70.253.1985 > 224.0.0.2.1985: HSRPv0-hello 20:
active group=70 addr=139.91.70.80
15:07:25.294625 802.ld config 2000 00:d0:00:dc:50:45.2105 root 2000.00:d0:
50:45 pathcost 0 age 0 max 20 hello 2 fdelay 15
15:07:25.609338 IP 139.91.70.46.631 > 139.91.70.255.631: LDP, length 138
15:07:25.864144 IP 139.91.70.254.1985 > 224.0.0.2.1985: HSRPv0-hello 20:
tandby group=70 addr=139.91.70.80
15:07:26.139315 IP 139.91.70.46.41988 > 139.91.70.255.111: UDP, length 117
15:07:26.869271 endnode-hello endnode vers 2 eco 0 ueco 0 src 1.10 blksize 2
rtr 0.0 hello 10 data 2
15:07:27.295746 802.ld config 2000 00:d0:00:dc:50:45.2105 root 2000.00:d0:
50:45 pathcost 0 age 0 max 20 hello 2 fdelay 15
15:07:27.695642 endnode-hello endnode vers 2 eco 0 ueco 0 src 1.10 blksize 2
rtr 0.0 hello 10 data 2
15:07:27.743866 IP 139.91.70.253.1985 > 224.0.0.2.1985: HSRPv0-hello 20:
active group=70 addr=139.91.70.80
15:07:28.067904 IP 139.91.70.253 > 224.0.0.10: EIGRP Hello, length: 40
15:07:28.264320 IP 139.91.70.254 > 224.0.0.10: EIGRP Hello, length: 40
```

# Packet Capture Tools

Libpcap/Winpcap: user-level packet capture

Standard interface used by most passive monitoring applications

PF\_RING: High-speed packet capture

Zero-copy, multicore-aware

tcpdump: just indispensable

Wireshark: tcpdump on steroids, with powerful GUI

dsniff: password sniffing and traffic analysis

ngrep: name says all

Kismet: 802.11 sniffer

*many more...*

# Packet Generation/Manipulation

Decode captured packets (L2 – L7)

Generate and inject new packets

## Tools

Libnet: one of the oldest

Scapy: powerful python-based framework

Nemesis: packet crafting and injection utility

Libdnet: low-level networking routines

dpkt: packet creation/parsing for the basic TCP/IP protocols

*many more...*

# Man-on-the-Side Attack

Packet capture + packet injection

Sniff for requests, and forge responses

Requires a privileged position between the victim and the destination server

- Race condition: attacker's forged response should arrive before the actual server's response

- Most OSes will accept the first packet they see as valid

No need to guess TCP seq/ack numbers!

- The rest of the original stream can follow after the injected packet

Powerful: redirect to malicious server, manipulate content, inject exploits, ...

Particularly effective in WiFi networks...

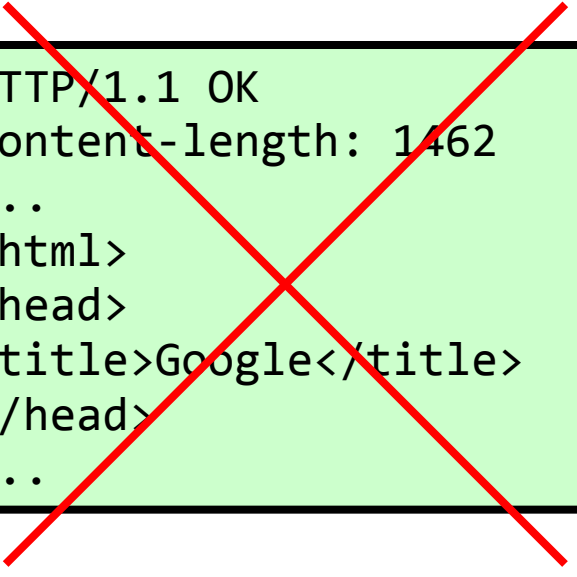
# Airpwn

Listens to wireless packets and acts on interesting HTTP requests based on predefined rules

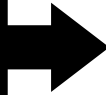
Beating server's response is easy: the server is several hops away (10s-100s ms) while the attacker is local

```
GET / HTTP/1.1  
Host: www.google.com  
...
```

```
HTTP/1.1 OK  
Content-length: 1462  
...  
<html>  
<head>  
<title>Google</title>  
</head>  
...
```



```
HTTP/1.1 OK  
Content-length: 1462  
...  
<html>  
<head>  
<title>Airpwned!</title>  
</head>  
...
```





# A Close Look at the NSA's Most Powerful Internet Attack Tool

BY NICHOLAS WEAVER 03.13.14 | 12:47 PM | PERMALINK

[Facebook Share] 52 [Twitter Tweet] 27 [Google+1] 162 [LinkedIn Share] 8 [Pinterest Pin it]



### MOST RECENT WIRED POSTS

[Image of a facility] New WI Rules of Surveillance Short, F Group S

[Image of a stork] Is It Eth Create I Three D Sources Absolut

[Image of a road] Lack of the Onl Behind Brutal D

[Image of a car interior] Robot C Rescue Its Clas Drivers

[Image of a red balloon] Animat Lego M