Network Access Control

COS 316: Principles of Computer System Design

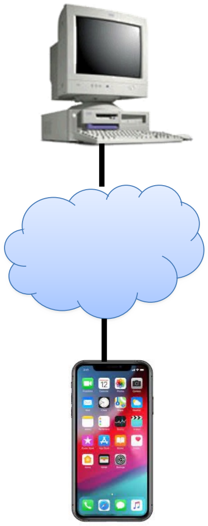
Lecture 20

Amit Levy & Jennifer Rexford

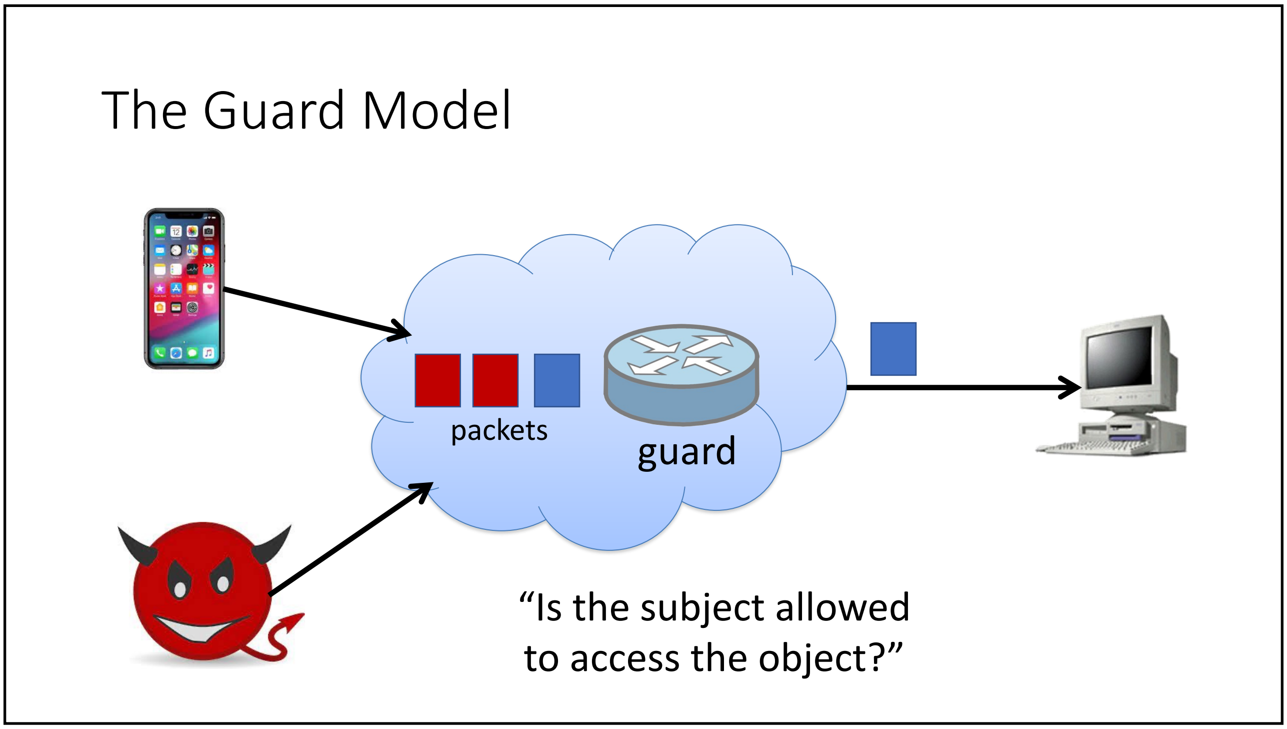
1

Controlling Which Packets Get Delivered

- **Objects**: the things being accessed
  - Services (possibly) running at the destination host machine
  - Identified by fields in the packet headers
  - E.g., destination IP address and TCP port number address
- **Subjects**: entity requesting access to an object
  - Sender of the packet on the source host machine
  - Identified by fields in the packet headers
  - E.g., source IP address, source TCP port number, …
- **Authorization**: rules governing subject’s access to objects



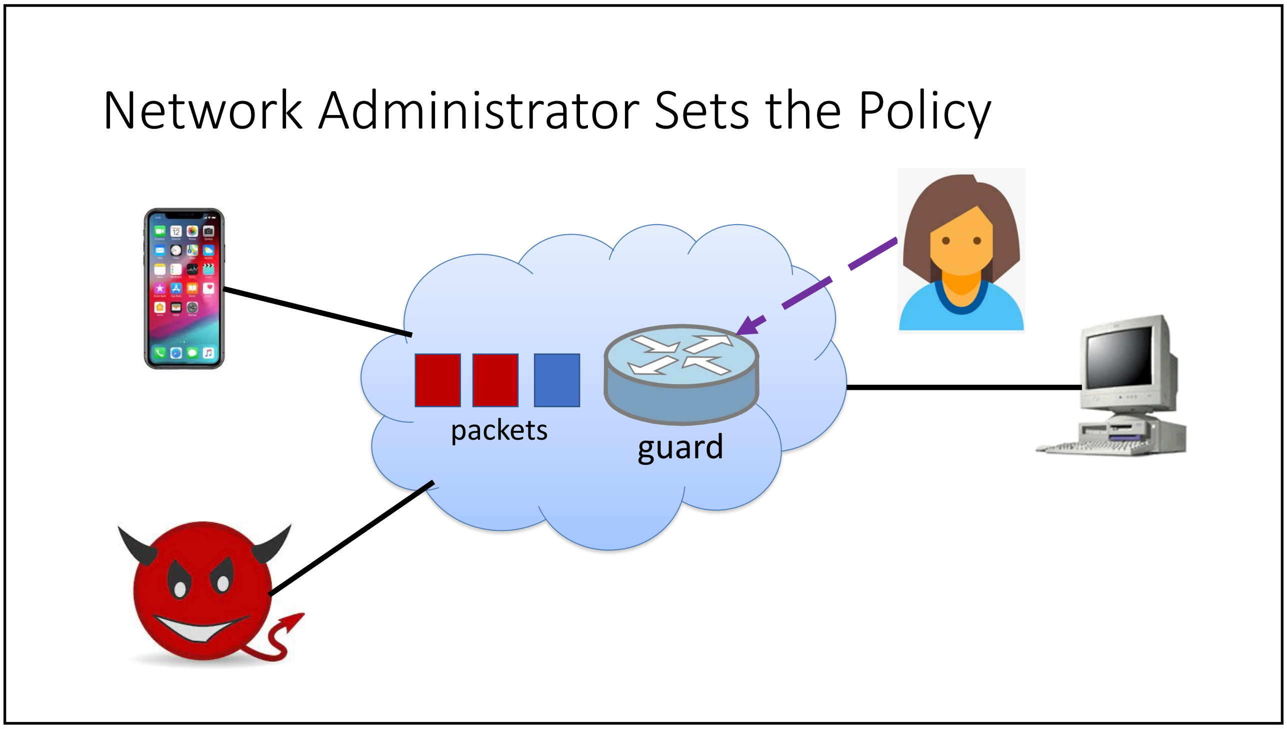
2



The Guard Model

“Is the subject allowed to access the object?”

3



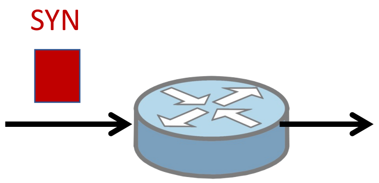
Network Administrator Sets the Policy

4

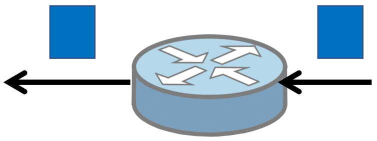
Policy Language: Access Control Rule

- An access control rule has two parts
  - Match: pattern on packet header fields and location
  - Action: permit (forward) or deny (drop)

- Block external initiation of a TCP connection
  - Match: external link, TCP protocol, TCP SYN flag
  - Action: deny



- Allow traffic from Princeton clients
  - Match: internal link, source IP in 128.112.*.*
  - Action: permit



Policy Language: Access Control Lists

- Access control list (ACL)
  - List of rules, possibly overlapping
  - Ordered list to disambiguate overlaps

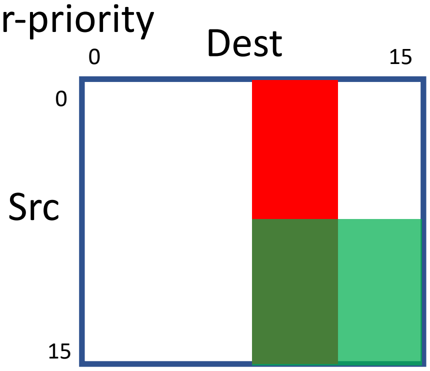
- Example:

Priority	Match	Action
1	Src=1.2.3.4, Dest=5.6.7.8	Deny
2	Dest=1.2.3.8, Dport=53	Allow
3	Dest=1.2.3.*	Deny
4	Src=1.2.3.7, Dport=100	Allow
5	Dport=100	Deny

Visualizing an Access Control List

- Overlapping shapes
  - Rules are multi-dimensional rectangles
  - Higher-priority rules on top of lower-priority
- Example with 4-bit addresses

Pri	Match	Action
1	Src=1***, Dest=1***	Permit
2	Src=****, Dest=10**	Deny

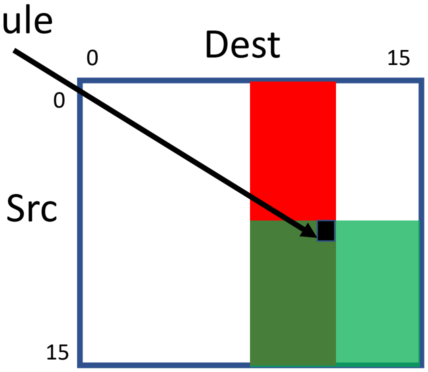


7

Applying an Access Control List

- Classifying a packet
  - Packet header: Src=1000, Dest=1011
  - Find the highest-priority matching rule
- Apply the associated action

Pri	Match	Action
1	Src=1***, Dest=1***	Permit
2	Src=****, Dest=10**	Deny



8

Simple Packet Classification Algorithm

- Classification problem
  - Given a packet (e.g., Src=1000, Dest=1011)
  - … and an Access Control List
  - Find the highest-priority matching rule
- Simple algorithm
  - Scan the rules in priority order
  - Stop after the first match
- Does not scale!

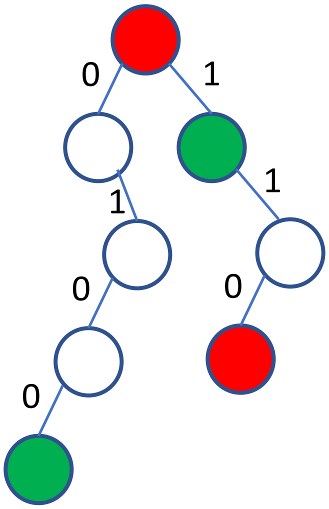
Pri	Match	Action
1	Src=1***, Dest=1***	Permit
2	Src=****, Dest=10**	Deny
3	Src=****, Dest=****	Permit

Special Case: One-Dimensional Prefix Matching

Pri	Match	Action
1	Dest=110*	Deny
2	Dest=0100	Permit
3	Dest=1***	Permit
4	Dest=****	Deny

Longest-prefix match

Binary Trie



Packet Classification: CAM Hardware

- Random Access Memory
  - Given a memory address
  - … return the data word stored at that address

00	b
01	a
10	d
11	c

- Content-Addressable Memory
  - Given some key
  - … find the data word (if any) associated with the key

1010	b
0110	a
1110	d
0001	c

11

Packet Classification: Ternary CAM Hardware

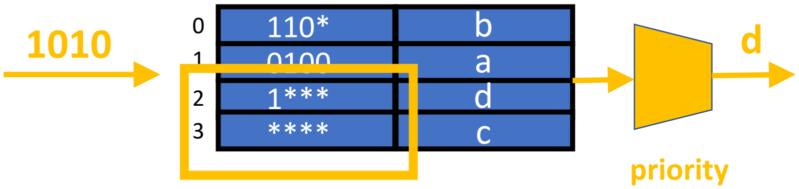
- Ternary Content-Addressable Memory (TCAM)
  - Ternary: 0, 1, or * (wildcard)
  - Matching patten can have wildcards
  - Entries in the TCAM in priority order

0	110*	b
1	0100	a
2	1***	d
3	****	c

12

Packet Classification: Ternary CAM Hardware

- Ternary Content-Addressable Memory (TCAM)
  - Ternary: 0, 1, or * (wildcard)
  - Matching patten can have wildcards
  - Entries in the TCAM in priority order



0	110*	b
1	0100	a
2	1***	d
3	****	c

Packet Classification in Practice

- Software access control
  - End-host network stack and software switches
  - Using algorithms for multi-dimensional packet classification
  - With optional caching of “popular” classification results

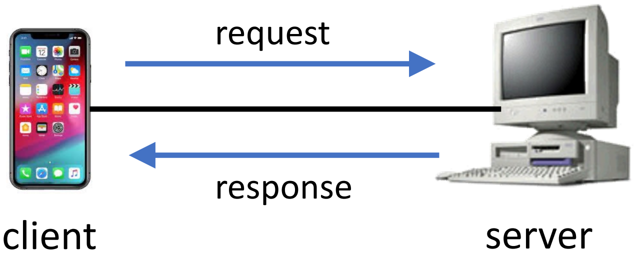
- Hardware access control
  - High-speed switches and network interface cards
  - Using Ternary Content Addressable Memory (TCAM)
  - With small TCAMs to reduce chip area and power consumption

Dynamic Access Control

- So far, we have discussed *static* ACLs
  - Configured by a network administrator
  - Based on network administrator knowledge of (in)valid traffic
- More sophisticated policies are dynamic
  - Adapted to the ongoing traffic (e.g., stateful firewall, SYN cookies)
  - Adapted to the routing protocol (e.g., reverse path forwarding)

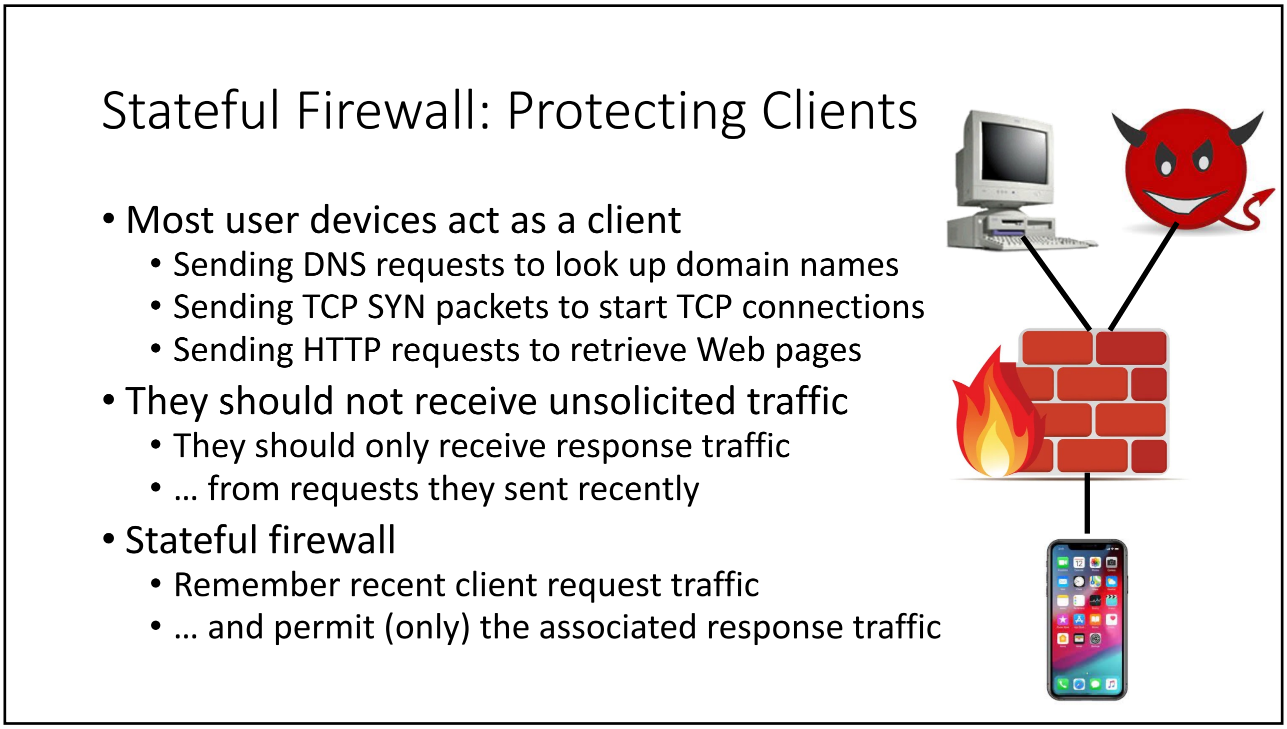
15

Internet Clients and Servers



- Request-response protocols
  - Client initiates communication by sending a *request* message
  - Server accepts the request and sends a *response* message

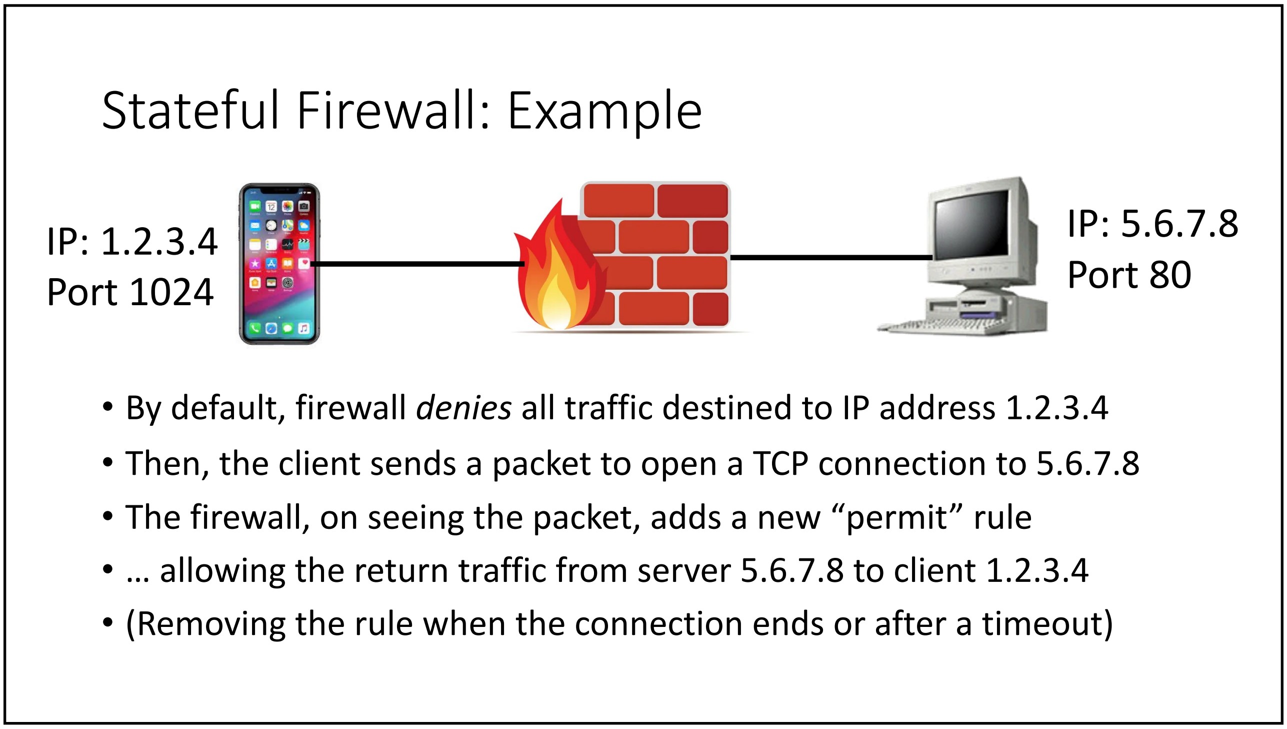
16



Stateful Firewall: Protecting Clients

- Most user devices act as a client
  - Sending DNS requests to look up domain names
  - Sending TCP SYN packets to start TCP connections
  - Sending HTTP requests to retrieve Web pages
- They should not receive unsolicited traffic
  - They should only receive response traffic
  - … from requests they sent recently
- Stateful firewall
  - Remember recent client request traffic
  - … and permit (only) the associated response traffic

17



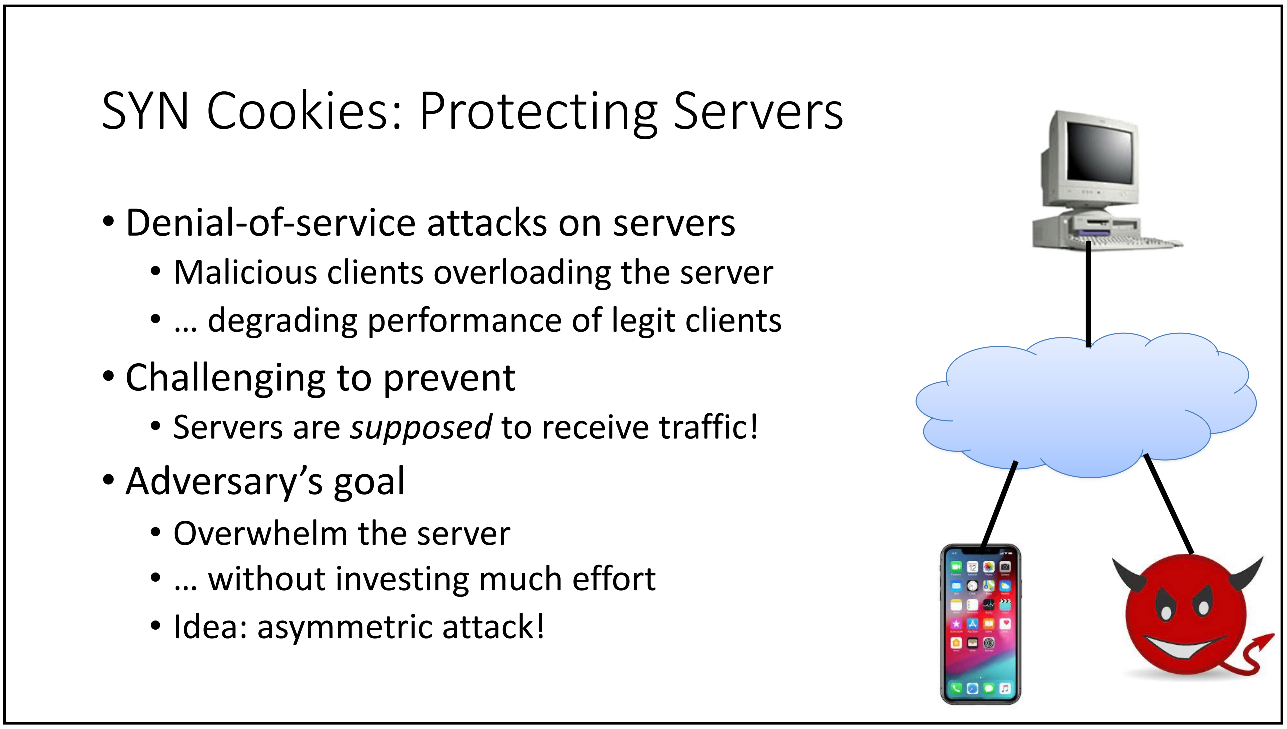
Stateful Firewall: Example

IP: 1.2.3.4
Port 1024

IP: 5.6.7.8
Port 80

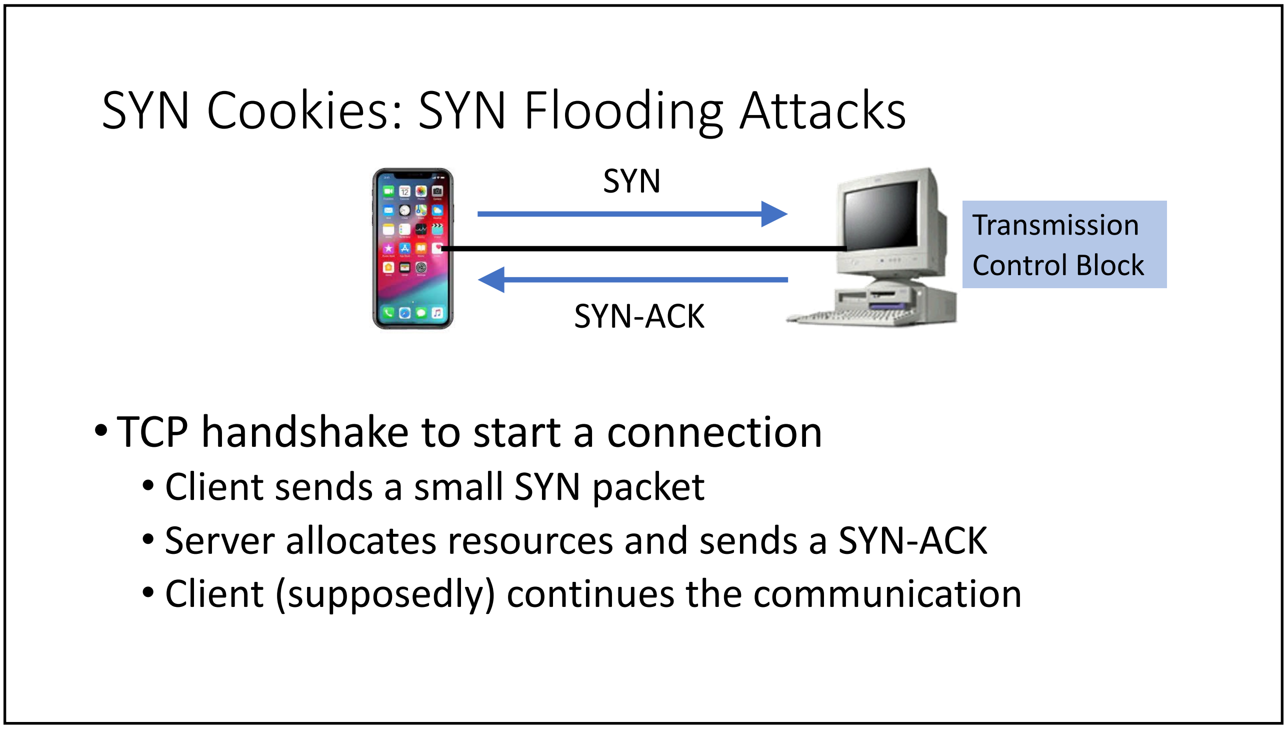
- By default, firewall *denies* all traffic destined to IP address 1.2.3.4
- Then, the client sends a packet to open a TCP connection to 5.6.7.8
- The firewall, on seeing the packet, adds a new “permit” rule
- … allowing the return traffic from server 5.6.7.8 to client 1.2.3.4
- (Removing the rule when the connection ends or after a timeout)

18



SYN Cookies: Protecting Servers

- Denial-of-service attacks on servers
  - Malicious clients overloading the server
  - … degrading performance of legit clients
- Challenging to prevent
  - Servers are *supposed* to receive traffic!
- Adversary’s goal
  - Overwhelm the server
  - … without investing much effort
  - Idea: asymmetric attack!

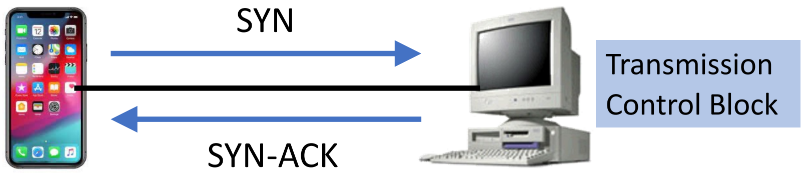


SYN Cookies: SYN Flooding Attacks

SYN
Transmission Control Block
SYN-ACK

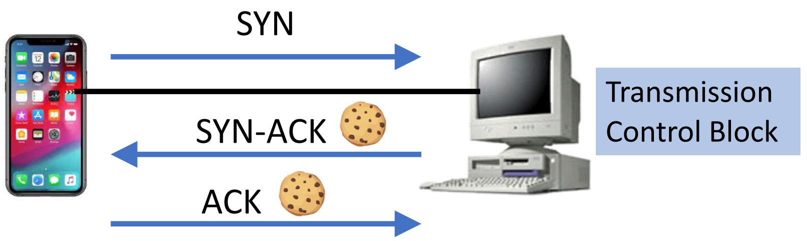
- TCP handshake to start a connection
  - Client sends a small SYN packet
  - Server allocates resources and sends a SYN-ACK
  - Client (supposedly) continues the communication

SYN Cookies: SYN Flooding Attacks



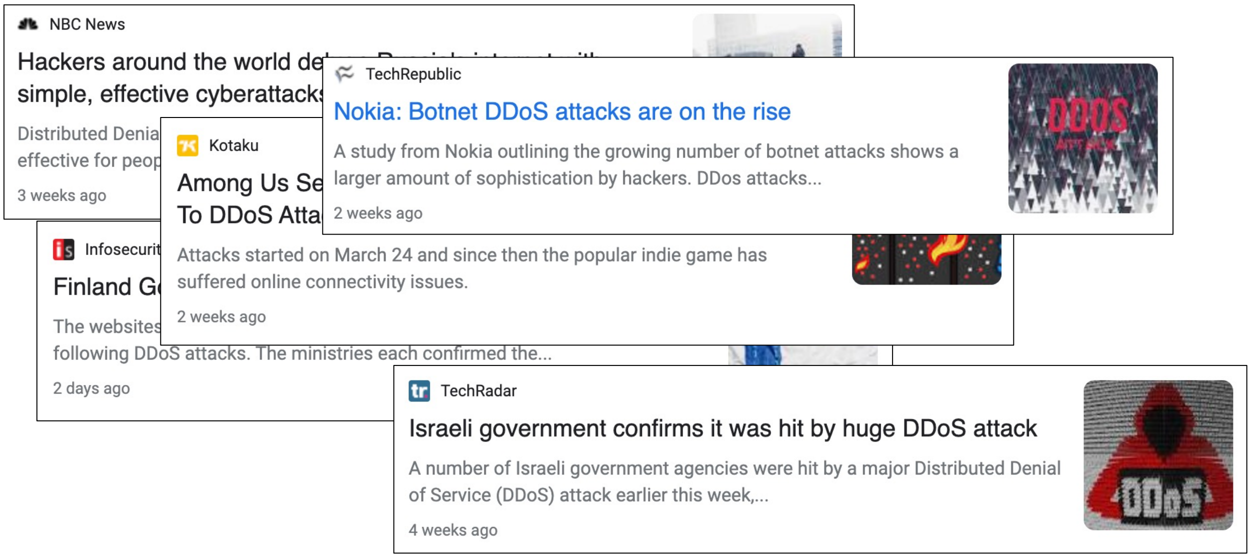
- Asymmetric attack
  - Client sends a 40-byte SYN packet
  - Server does a lot of work
- Crafty adversary
  - Send from a spoofed source IP address (hard to trace!)
  - Send from compromised hosts (very little overhead for adversary!)

SYN Cookies: Push the Work to the Client



- Server ensures the client has some “skin in the game”
  - Server puts a cryptographic “SYN cookie” in the SYN-ACK
  - Client must return the cookie in its ACK packets
  - Server verifies the cookie before dedicating resources
- Deny any ACK packets that fail the cookie check

Denial-of-Service Attacks are Common



NBC News

Hackers around the world de

simple, effective cyberattacks

Distributed Denia

effective for peop

3 weeks ago

TechRepublic

Nokia: Botnet DDoS attacks are on the rise

A study from Nokia outlining the growing number of botnet attacks shows a larger amount of sophistication by hackers. DDos attacks...

2 weeks ago

Kotaku

Among Us Se

To DDoS Atta

Attacks started on March 24 and since then the popular indie game has suffered online connectivity issues.

2 weeks ago

Infosecurit

Finland G

The websites

following DDoS attacks. The ministries each confirmed the...

2 days ago

TechRadar

Israeli government confirms it was hit by huge DDoS attack

A number of Israeli government agencies were hit by a major Distributed Denial of Service (DDoS) attack earlier this week,...

4 weeks ago

23

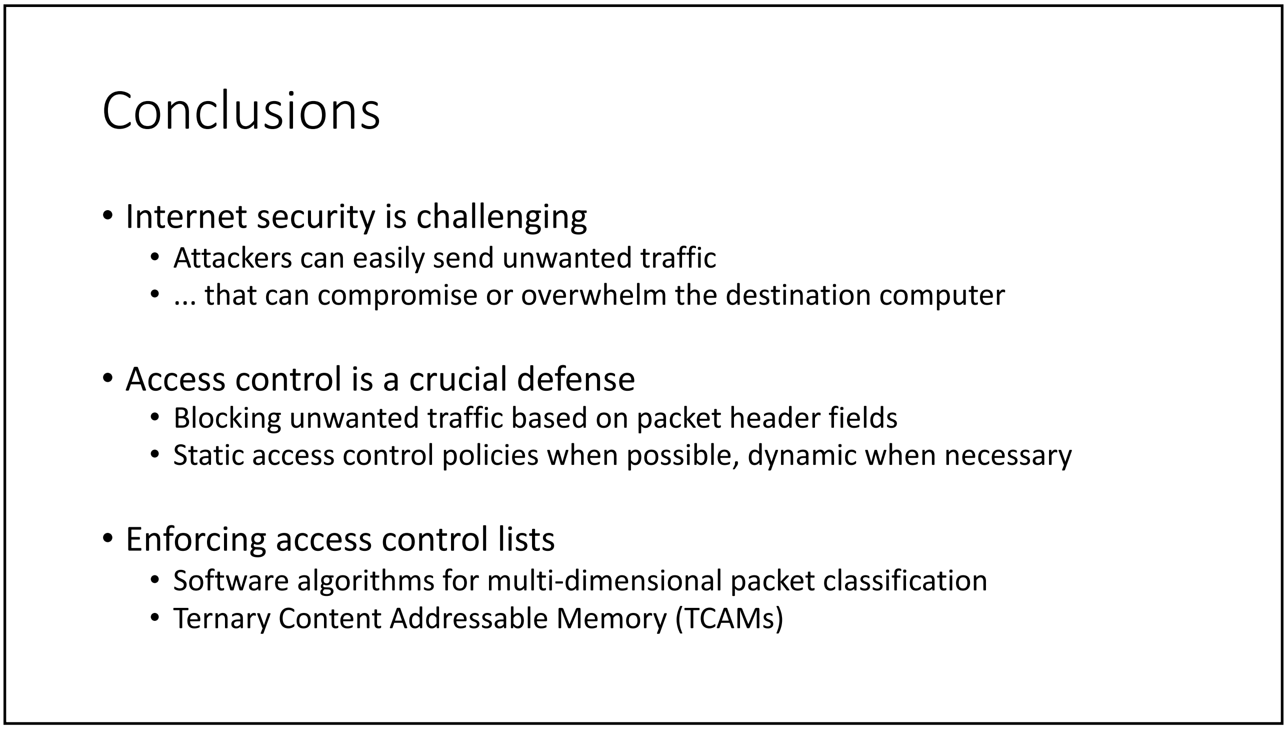
Wider Range of Detection Techniques

- Traffic measurement
  - Identify anomalous traffic destined to the server
  - Identify command-and-control for botnets
- Known suspicious IP addresses or entire networks
- Known suspicious other header fields (ports, Time-to-Live)
- Tracing attack traffic across the Internet back to the origin
- Comparing analysis across different victims

- Enforcement all comes done to access control!

https://www.youtube.com/watch?v=TP3H_GefL-0

24



Conclusions

- Internet security is challenging
  - Attackers can easily send unwanted traffic
  - ... that can compromise or overwhelm the destination computer
- Access control is a crucial defense
  - Blocking unwanted traffic based on packet header fields
  - Static access control policies when possible, dynamic when necessary
- Enforcing access control lists
  - Software algorithms for multi-dimensional packet classification
  - Ternary Content Addressable Memory (TCAMs)

25