NETWORK SECURITY

EE122 Section 12
QUESTION 1
A sends a RESET (RST) to B

- E.g., because application process on A crashed
- B does not ack the RST
- Thus, RST is not delivered reliably
- And: any data in flight is lost
- But: if B sends anything more, will elicit another RST
END-TO-END SECURITY

- Application layer
  - TLS/SSL encrypts all application layer data
  - … but does not encrypt the TCP header!
END-TO-END SECURITY

- **Application layer**
  - TLS/SSL encrypts all application layer data
  - … but does not encrypt the TCP header!

- **Transport layer**
  - TCP sequence number defends against blind spoofing
  - … but not man-in-the-middle attacks

- **Network layer**
  - IPsec encrypts the entire IP payload, including the TCP header
END-TO-END SECURITY

- Encrypted Content
- TCP Header
- IP Header
- TLS/SSL (Application Layer)

- IP Header
- Encrypted IP Header
- Encrypted TCP Header
- IPsec (Network Layer)
- Encrypted Content
BLIND SPOOFING

- Need to know the sequence number
TCP Conn. Setup & Data Exchange

Client (initiator)
IP address 1.2.1.2, port 3344

Server
IP address 9.8.7.6, port 80

SrcA=1.2.1.2, SrcP=3344,
DstA=9.8.7.6, DstP=80, SYN, Seq = x

Client picks an Initial Sequence Number (ISN)
TCP Conn. Setup & Data Exchange

Client (initiator)
IP address 1.2.1.2, port 3344

Server
IP address 9.8.7.6, port 80

SrcA=1.2.1.2, SrcP=3344,
DstA=9.8.7.6, DstP=80, SYN, Seq = x

SrcA=9.8.7.6, SrcP=80,
DstA=1.2.1.2, DstP=3344, SYN+ACK, Seq = y, Ack = x+1

Server also picks an ISN …
(spec says to use local clock)

... and acknowledges the client's ISN
TCP Conn. Setup & Data Exchange

Client (initiator)
IP address 1.2.1.2, port 3344

Server
IP address 9.8.7.6, port 80

\[
\begin{align*}
\text{SrcA}=1.2.1.2, \text{SrcP}=3344, \\
\text{DstA}=9.8.7.6, \text{DstP}=80, \text{SYN, Seq} = x
\end{align*}
\]  

\[
\begin{align*}
\text{SrcA}=9.8.7.6, \text{SrcP}=80, \\
\text{DstA}=1.2.1.2, \text{DstP}=3344, \text{SYN+ACK, Seq} = y, \text{Ack} = x+1
\end{align*}
\]  

\[
\begin{align*}
\text{SrcA}=1.2.1.2, \text{SrcP}=3344, \\
\text{DstA}=9.8.7.6, \text{DstP}=80, \text{ACK, Ack} = y+1
\end{align*}
\]  

Client completes 3-way handshake by ack’ing server’s ISN
BLIND SPOOFING

- Need to know the sequence number
- How? Guess all 65536 numbers!

- Alternatively, infer
  - first send a legitimate TCP SYN
  - Let’s say the receiver responds with sequence number A
  - Then spoof a TCP SYN assuming the receiver responds with A+1

- Defenses?
QUESTION 2
Source IP: 188.0.0.1

Egress Filtering

228.147.0.0/16
Source IP: 228.147.5.5

Ingress Filtering

228.147.0.0/16
What’s missing?

Source IP: 228.147.5.5

Ingress Filtering

228.147.0.0/16
Receiver

Attacker

Source

SYN

SYNACK (seqno = y)

ACK (ackno = k?)

???
Defenses?
Receiver

Attacker

Nonce

Confirmation Response (456?)

Confirmation Request (123)

Source

???
QUESTION 3
Web server X can comfortably handle the load you generate.
DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

Control traffic directs slaves at victim

Slave 1
src = random
dst = victim

Slave 2

Slave 3

Slave 4

Slaves send streams of traffic (perhaps spoofed) to victim

Victim
REFLECTORS

- Cause one *non-compromised* host to attack another
- E.g., host A sends TCP SYN with source V to server R
- R sends reply to V
**DIFFUSE DDOS: REFLECTOR ATTACK**

Request: src = victim
dst = reflector

Control traffic directs slaves at victim & reflectors

Reflectors send streams of non-spoofed but unsolicited traffic to victim

Reply: src = reflector
dst = victim
MITIGATING DDOS

- No good defense…

- Solutions so far
  - Overprovision
  - Distribute service to multiple machines
QUESTION 4
Andrew \rightarrow E(M, Steve_{pub}) \rightarrow \text{Steve}
Andrew \rightarrow E(M, \text{Steve}_{\text{pub}}) \rightarrow \text{Man-In-The-Middle} \rightarrow \text{Steve}
Andrew

E(M', Steve_{pub})

Man-In-The-Middle

Steve
Andrew

E(M, Steve_{pub})

MAC(H(M), Andrew_{private})

Steve

Andrew_{pub}???
Andrew

$E(M, \text{Steve}_{pub})$

MAC($H(M), \text{Andrew}_{private}$)

$E(\text{Andrew}_{pub}, \text{Steve}_{pub})$

Steve
$E(M, Steve_{pub})$
$E(Andrew_{pub}, Steve_{pub})$
$MAC(H(M), Andrew_{private})$
Andrew

Man-In-The-Middle

E(M', Steve_{pub})
E(MITM_{pub}, Steve_{pub})
MAC(H(M'), MITM_{private})

Steve