6.858
Network Security
Liveness
Internet
ISP
Peering
Internet today
Core: Liveness
Security: end nodes
Good design
telnet  ethernet

Attacker

modify data
inject data
listen steal pw
mitm
Klogin.

don't send pw trusted host file

diff hard to fake src address.
TCP handshake

SYN = SNS
ACK = SNC
Seq = SYN
Ack = SYN + 1
Data = SNC
Ack = SNC + 1
Guess S/N's

15x1

+128 per sec

+64 per new conn.

=> make regular

+64
Seq # => attack
1) forge src address
2) DoS BGP
3) Hijack 2016
Mitigations

- E2E crypto-based auth (SSL/SSH)
- ISP & Her packet
  (but multihoming)
- Firewalls
Harden tcp

- Random seq?
- Random incr?

\( \langle \text{src, dst} \rangle \)

\( \text{SNs} = \text{ISN}\text{old} + \text{SHA256}(\text{src, dst, secret}) \)

No extra state
SYN cookies

\[ S\text{N}s = S\text{N}/c + (t_s || \text{SHA1}(\text{SRC}, \text{DST}, \text{SECRET}, t_s)) \]

\[ \rightarrow S\text{N}/c + 1 \]

\[ S\text{N}s \]
Amplification

Access

Memcached
Routing protocols.

- DHCP (ARP)
- BGP (RIP)
- open net

SBGP, ...

MANRS
Summary

Open net
Core: liveness
Pos
Higher-level SSL/TLS
top
IP
physical