Preventing Denial of Service Attacks

Steven M. Bellovin
smb@research.att.com
http://www.research.att.com/~smb

Fudd's First Law of Opposition

"Push something hard enough and it will fall over."

--Firesign Theater, circa 1971.

What is Denial of Service?

- By enemy action, you don't have use of your own resources.
- The enemy -- or a third party -- may or may not have (productive) use of them; that's irrelevant.
- Any sort of resource -- CPU, memory, bandwidth, personnel, sleep time -- can be attacked.

Why Does DoS Happen?

- Denial of Service can occur any time it is cheaper for the enemy to make a request than it is for you to process it.
- Besides, we've rarely designed our systems to resist.

Example: UNIX

```
while true
do
    mkdir x
    cd x
done
```

Example: Networking

- TCP uses 3-way handshake
- Send forged first message to victim; reply goes nowhere.
- Third message never shows up.
- Victim's memory is consumed.

Defenses: First Cut

- On hosts, limit resources consumed per user.
- For network protocols, let the network protocol hold the state.
- What of other attacks?

Cryptographic Authentication

- Security folks like cryptographic authentication -- it's quite strong.
- It's also expensive, especially if public key crypto is used.
- When we get ubiquitous crypto, will we get ubiquitous DoS attacks?
- Must use *layered* authentication.

Network DoS and DDoS

- Objective: Consume network bandwidth.
- A *true* network security problem -- not solvable by hosts.
- Network itself must deflect it -- packet flow must be authorized.
- Can't use crypto -- it's too expensive.
- Use network concepts: return address or input link.

General Rules

- Everything must be authenticated and authorized.
  - (But what about privacy and anonymity?)
- Strength and cost of authentication must be commensurate with resource being protected.
- Can ramp up to strong authentication.