Internet Security

The Border Gateway Protocol

Overview

* BGP Review (super fast)
* Threat Models
* BGP Attack Trees
* Examples

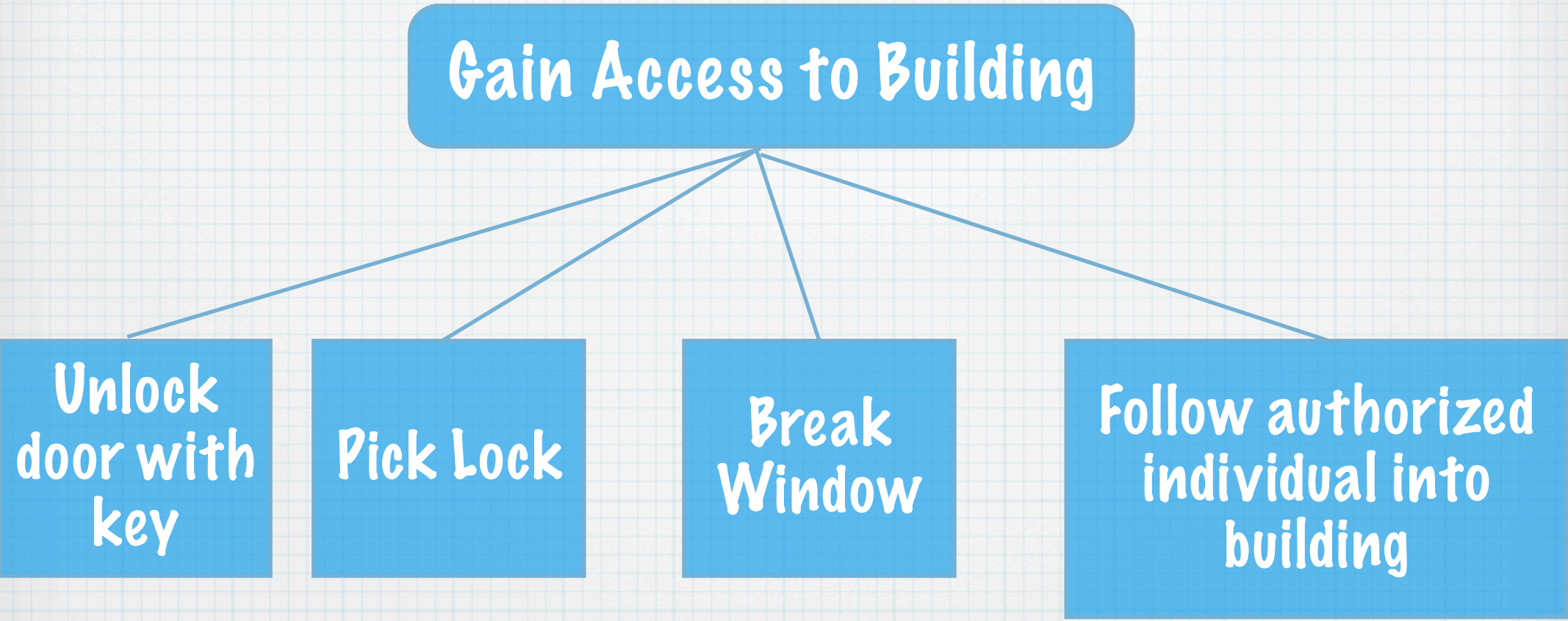
BGP

* RIP, OSPF, EIGRP, IS-IS
  * Local traffic
* BGP
  * Traffic between Autonomous Systems
  * Advertises routes to other networks

Threat Models

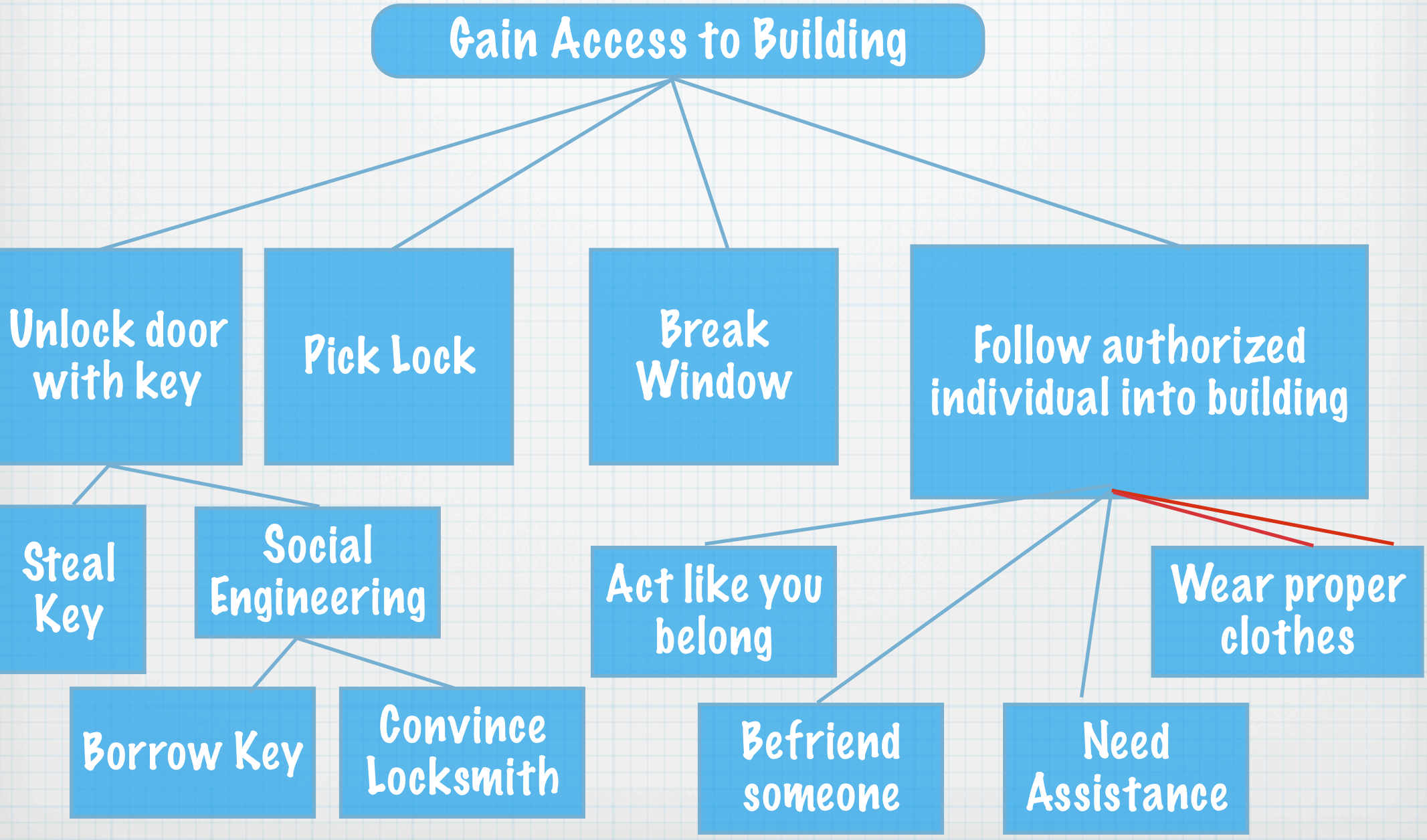
- Internet attacks more of a threat
- Threat Models
  - What kind of an attack? Who? How? When?
- Attack trees provide answer

Attack Trees



Nodes: Goals & Subgoals
Need sub-goals (how to achieve goals)
Levels of abstractions

A Better Attack Tree



Different Format

Goal: Gain unauthorized physical access to a building

Attack:

OR 1. Unlock door with key

OR 1. Steal Key

2. Social Engineering

OR 1. Borrow key

2. Convince locksmith to unlock door

2. Pick Lock

3. Break Window

4. Follow authorized individual into building

OR 1. Act like you belong and follow them in

2. Befriend someone authorized to go in

3. Appear in need of help (carrying box)

AND 4. Wear appropriate clothing for location

Attack Tree Uses

* Subordinate Goals
  * Analysis at multiple layers
* Common attacks = re-useable modules
* Comparison between tech & non-tech
* Which attack is the easiest? Hardest? Most likely?

BGP Attack Trees

* Impact
* Ease
* Cost
* Countermeasures?
* Access/Trust Requirements

Attacking BGP

Goal: Originate Unauthorized Prefix/Attribute into Peer Routing Table

Attack:

OR 1. Send from valid Router

OR

1. Misconfigured router
2. Compromise Router (separate tree)

2. Send from invalid Router

AND 1. Gag valid router

OR 1. Kill Router

OR 1. Power off/Physical Layer
2. Crash & prevent reboot
3. Conduct DoS attack (separate tree)
4. Steal IP address

2. Introduce rogue router

OR 1. Steal IP Addr (separate tree)
2. Establish unauth BGP session w/ peer

3. Send spoofed BGP Update from Non-Router

OR 1. Conduct TCP Sequence Number Attack (separate)
2. Conduct Man-in-the-Middle (sparate)

AND 4. Craft BGP Message

Attack Goals

* Atomic Goals
  * Compromise MD5 authentication
  * Establish unauth BGP session w/ peer
  * Originate unauth prefix into peer routing table
  * Change path preference of a prefix
  * DoS against BGP process
  * Reset BGP session
  * Spoof BGP message

More Goals

- Supporting Atomic Goals
  - Compromise Router
  - Denial of Service (DoS)
  - Man-in-the-Middle (MITM)
  - TCP Sequence Number Attack
  - Sniff Traffic

Supporting Attack

Denial of Service

Attack:

OR 1. Physical destruction of router
2. Link layer attacks
OR 1. Protocol attack using link layer protocol
2. Physical link attack
3. ARP attacks
4. IP attacks
OR 1. ICMP Message
OR 1. Flooding
2. Malformed message
2. IP Fragmentation Attack
5. UDP Attacks

6. TCP Attacks
   OR 1. SYN Flood
      2. Connect()
      3. LAST_ACK
      4. New/undiscovered DoS against TCP
   7. Application-Layer DoS
   OR 1. Telnet
      2. SSH
      3. SNMP
      4. Other application layer protocol

Questions???