802.11 Networking in Hostile Environments

Mike Kershaw
dragorn@Kismetwireless.net

August 19, 2004

Hostile networking environments

Sometimes it's necessary to network users despite their best efforts to the contrary – we're talking about extremely hostile network environments:

- "Hacker" conferences (HOPE-5, Defcon, etc)
- "Security" conferences (Is there a difference?)
- Political events where activists may target the wireless network
- Any other public venue with mischievous users (Popular cafes, etc)

Key vulnerabilities

1. Denial of Service - Probably the most common attack, a DoS is pure malice. Theres nothing to be gained other than disrupting the network and making it useless. Any number of tools can launch DoS attacks against 802.11.

2. Spoof/MITM - 802.11 is terribly easy to spoof. If your users are not using good crypto, they're vulnerable – and even if they are, a spoofed AP can null-route them and kill the network as effectively as a DoS

802.11 DoS attacks

- Disassociation & Deauthentication spoofing
  - Attack targets clients – single or all with broadcast frames
  - Forging 2 packets from the BSSID of the access point
  - Disassociate frame tells clients that the AP is removing them
  - Deauthenticate frame tells clients that the previous authentication is no longer valid
  - Precursor to MITM or DoS
  - Performed by Airjack, Void11, others
- Client-source disassociation – same method of attack but client is spoofed to tell AP to end association

802.11 DoS attacks

- False client power-save
  - Attacker spoofs client to inform the AP that it is entering powersave mode
  - AP no longer sends data to the client until the powersave timeframe has completed
  - Alternately, attacker spoofs clients legitimately in power-save mode and requests all queued packets be delivered immediately
  - More difficult to perform due to firmware restrictions but not impossible
- Man-in-the-middle attacks – separates client from the legitimate access point, attaches them to a spoofed access point, and owns layer2

Mitigating hostility

- Some attacks which target the AP can be mitigated with APs smart enough to ignore them
- We CANNOT (realistically) prevent attacks against clients!
- Best solution is to make intelligent, adaptive access points and enough coverage and power to overwhelm casual attackers
- Having full-spectrum coverate (4 channels) per zone with strong radios raises the difficulty of knocking out the entire network
- Most clients pick associations by strongest signal strength – a user looking for a network will be more likely to stick to the strong legit network than a weaker spoofed network.

SmartAP software

- Written for & first tested at Hope-5
- SSL encryption of management protocol
- Automatically allocates channels across APs in a zone to avoid overlapping channels
- Uses Kismet for IDS to detect spoofs and attacks
- Raw transmission to counterattack spoofed access points and mitigate other attacks
- Centrally managed to prevent escalating counterattacks

Network topology

- Network is divided into non-overlapping zones. All APs in a zone are assumed to be able to see each other

- Central management is configured with the preferred number of radios for each pool:
  1. Sniffer – Sniffer radios run Kismet and report alerts and spoofs to the central system

  2. RawTX – Raw transmit radios do packet injection counterattacks against spoofed networks

  3. Access Points – All radios not assigned to the previous pool become access points

- 802.1q tagged backbone – user data and AP control data is segregated

Configuring the access point

Access points were designed to be as interchangeable as possible.
The only configuration per AP is:

- SSL certificate signed by the central CA & cert password
- IP address of the central management server
- Zone number

Allocation

- Each AP contacts the server and reports available interfaces, capabilities, MAC addresses, etc

- Centrol does smart pool allocation for each zone:
  1. Zones with 3 radios or fewer operate in fallback mode – all access points, no smart abilities

  2. If requested, at least one radio is allocated to sniffer and rawtx pools

  3. Pool allocation is divided across physical APs to prevent all resources of a pool being allocated on the same hardware.

  4. Unallocated radios are configured as access points – 11 channel spectrum is divided by the number of AP radios and channels are allocated as far apart as possible to prevent overlap

Allocation

- Control pushes configuration out to APs
- Control activates configured APs

Dynamic pool adjustment

- APs may be added or removed during the course of the event, either due to failure of the AP or of the wired network, or to account for increased demand
- New APs connect to the central controller and announce zone exactly as above
- Pool allocations are only recalculated at regular intervals – the controller will not cause a zone to flap if an AP is constantly rebooting
- Existing pool allocations are kept where ever possible to minimize mode switching

Statistics and logging

- Central server presents network socket for statistics gathering
- Per-radio statistics for each AP logged over server protocol
  - Transmit and receive byte counts
  - Tx, rx, and error packet counts
  - Client counts
  - Attacks and counterattacks logged
  - Any stats client could connect – realtime displays, RRD, etc

Attack detection

- Kismet runs on the radios assigned to the sniffer pool
- AP watches Kismet output and processes alerts
- Alerts passed to central control server for logging and dispatching
- Able to process both fingerprint and trend alert conditions
- Relevant alerts Kismet Kismet currently generates:
  - Unauthorized BSSIDs
  - BSSID MAC Spoof detection via BSS timestamp tracking
  - Deauthentication and Disassociation floods

Attack detection

- Broadcast deauth and disassoc
- Firmware attacks against clients

Attack Avoidance

- Most attacks target BSSID
- Changing the BSSID of an AP could avoid some attacks
- Unfortunately, could not implement it because prism2 firmware cannot dynamically change the BSSID
- Other cards may be able to dynamically change the BSSID

Counterattack

- Counterattacks are brokered by the central control server and limited by frequency and target
- Escallating counterattacks would make the network useless. APs cannot initiate counterattacks on their own.
- Counterattack abilities are limited by the firmware abilities of the rawtx cards

Spoofed SSID Counterattack

- Each AP in the network reports the MAC of all cards. We know which ones are legitimate
- Illegitimate APs can be used for MITM or simply be a nuisance by not routing users currently
- Broadcast deauth & discon used to kick all the users off the fake AP so they reconnect to the legitimate APs
- Assoc & authenticate flood used to fill up fake AP AID slots
- Most APs will fall down for 10-15 minutes with 30 seconds of flooding

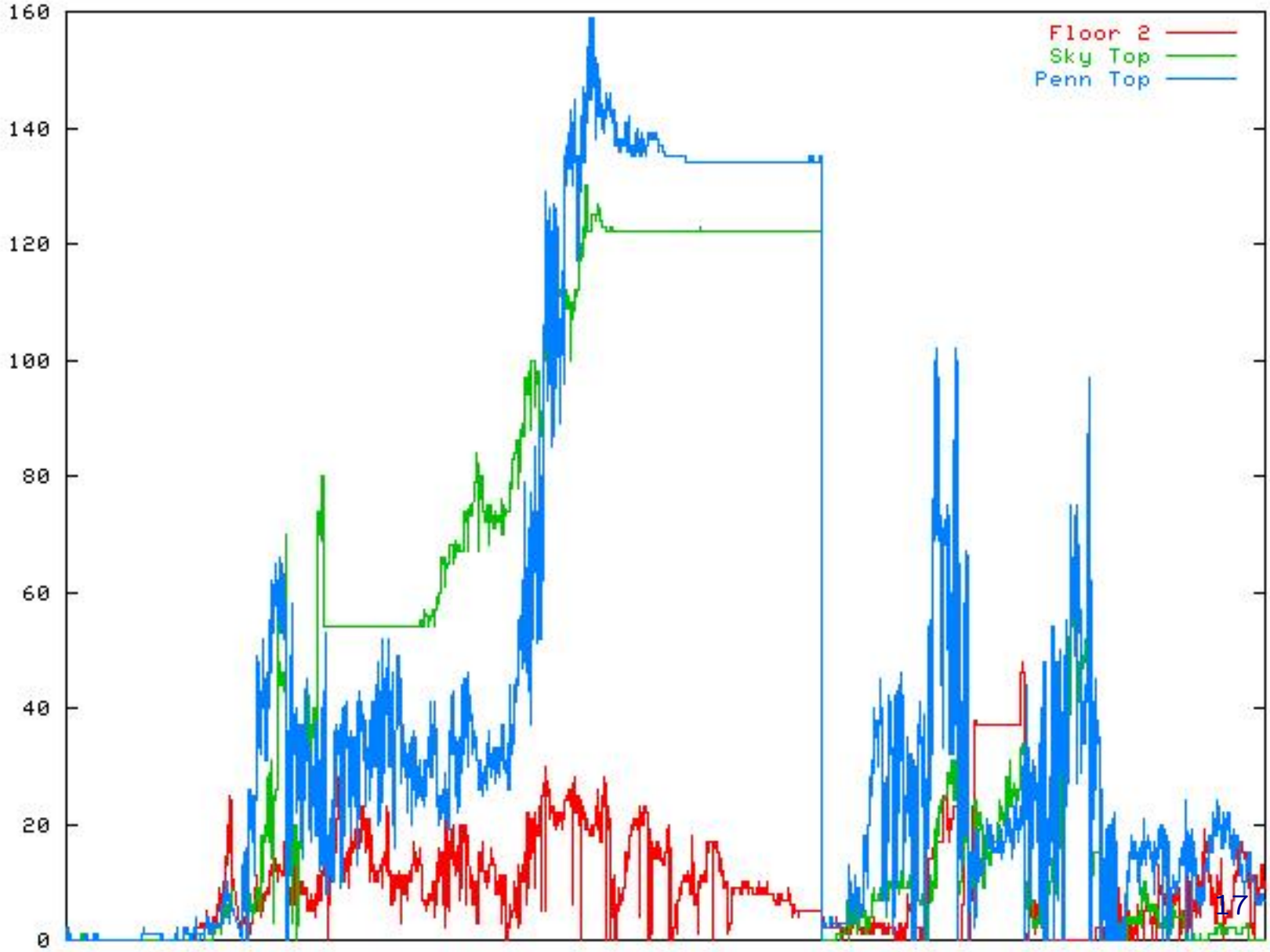
Hope-5 Network

- Access Points
  - Downclocked Cyrix MediaGX running at 33mhz
  - 100mbit Ethernet with 802.1q tagging
  - 2 SMC 200mW Prism2 cards
  - 64mb IDE-Flash drive
  - Linux running HostAP
- Network backend
  - 100mbit Ethernet
  - 802.1q tagging

Hope-5 Network

- Common VLANs and address space between 2nd and 18th floors
- DHCP, routing, firewalling all done in common network core

Hope-5 Network Usage



Hope-5 Network Numbers

- 849 DHCP leases
- 620 wireless leases
- Approximately 400 wireless users at one time during peak
- Approximately 80% uptime
- 1500+ attacks (that we noticed)
- 1700 packets/sec on one channel during height of attacks
- Typical DoS attacks, some AP spoofing, powersave attacks

Plans for the future

- Public release "Really Soon Now"
- Currently very specific for the Hope conference – generalization being added for public release
- Detect and respond to power save attacks
- Automatic zone allocation and adjacent AP discovery
- Per-radio capability info to allow non-prism2 based radios
- Decentralized management

Contact

- Email: `dragorn@kismetwireless.net`
- Presentation download:

  `http://www.kismetwireless.net/presentations/`
- Software download:

  `http://www.kismetwireless.net`

  `http://smartap.kismetwireless.net`