802.11 Security & Kismet

Mike Kershaw

mike@kismetwireless.net

August 20, 2004

1

- Do you have wireless at home?

- Do you have wireless at work?

- How many businesses you frequent use wireless?

- Do you think they are secure?

- Is your doctor?

- Your lawyer?

Kismet

- 802.11 sniffer

- Can sniff 11a, 11b, and 11g with the right hardware

- Completely passive

- Signature and Trend Layer2 IDS

- Runs on Linux, some BSD, OSX

- Plays nice with the other kids on the block (snort, driftnet, etc)

- Can log GPS coordinates for mapping of network positions

- Can run on extremely lightweight devices (APs, handhelds, etc)

3

- Client/server so multiple displays can connect to one server, custom clients can perform additional logging, GUIs, etc

- Linux – Core development is on Linux, most supported platform.

- OSX – Original airport cards work, Airport Extreme will not. For a pretty GUI, check out Kismac

- *BSD – Prism2 cards in OpenBSD, Atheros and Prism2 on FreeBSD5, unknown on NetBSD. Freebsd Radiotap system will bring more support

- OSX – Support for Airport but not Airport Extreme

- Windows – Currently no free drivers for doing monitor mode. Kismet can read from WSP100 embedded sniffers, or Kismet drones on a supported platform.

4

- Sniffers like Ethereal, Tcpdump, or Kismet capture raw data frames. Kismet always operates in monitor mode, other sniffers can. Sniffers can see data packets.

- Stumblers query the card firmware to see what networks are detectable in the area. They usually see fewer networks than sniffers, and can't capture data packets, but they don't require special drivers, either.

- Monitor mode (rfmon) puts the card into a state that is not connected to any network, and will report all packets including management frames to the OS.

- Promisc mode has less meaning in wireless - with most drivers, will report all data frames on the associated network, but not from other networks or management frames

- Monitor mode requires support from the chipset and the driver. Most chipsets can do it, but not all drivers support it on all platforms.

Passive network detection

- Monitor mode gets us all management frames

- Management frames define the network

- Able to directly detect the presence of APs and infer the presence of hidden networks from other traffic

- Able to decloak hidden SSIDs by watching client connections

- Passive network detection just that – passive. No packets are sent by the sniffer

- Passive sniffers can also detect active sniffers like Netstumbler

7

Kismet demo goes here

8

- Vendors try to add security by modifying the protocol, but it really has no benefit

- Cloaked SSID: APs don't put the SSID in the beacon frame. This is supposed to prevent people who don't know the network name from connecting, but the SSID was never designed to be a security feature, and is still sent cleartext by the AP when a client joins.

- Nonbeaconing: Some APs attempt to turn off or slow down the beacon rate so that they're invisible, but as soon as a user exchanges data on the network, it can be seen.

- Hiding networks from passive sniffers is impossible, as long as the sniffer is capable of understanding the protocol and listening on the frequency.

9

- Easiest is fingerprint matching - some tools always send a certain frame which is indicative of an alert condition

- Netstumbler, Lucent Site Survey, Wellenreiter, and some 802.11 layer attacks are all fingerprint based.

- Trend based alerts detect events which are normal in small amounts or in some sequences, but constitute attacks in other situations.

- Flooding, AP spoofing, and generic active sniffer detection are all trend-based alerts

- Can be put in embedded consumer APs for sniffing+AP functions

- Fingerprint – Under some conditions, NetStumbler sends packets containing the text "This space intentionally left blank". When a frame of the appropriate type is seen with this payload, it definitely comes from NetStumbler

- Trend – Netstumbler doesn't always send fingerprintable frames, and other stumblers may not be fingerprintable. Under normal operation, stumblers act like standard clients, however by monitoring clients that constantly probe for networks, are accepted into the networks, but never join, we can assume that it is probably a stumbler and raise an alert.

Distributed IDS

- Kismet drones are a super-stripped down version of the Kismet core which report packets over a wired network

- Even more lightweight than the server

- Runs well on 486s, APs, etc

- Distributed net of drones linked to one server running WEP decryption and IDS

- An entire building can report to one Kismet engine for logging and IDS

- Unix philosophy - Smaller tools that work with other tools

- Kismet dumpfiles are standard tcpdump format - any tool that can read pcap files can read a Kismet dump, ie tcpdump, ethereal

- Live packet streaming via FIFO pipe for other tools, including de-wepping of networks with known keys.

- FIFO pipe allows tools like Snort to attach to the stream of packets processed by Kismet and perform layer3+ IDS functions.

- Entire building-wide drone network can be routed to snort for TCP IDS

13

- XML logfiles for external parsers to reprocess network data for web sites, databases, audit logs, etc

13

- Processes gpsxml and netxml files generated by Kismet to plot on graphical maps

- Pulls from various public map sources

- Does extensive data sifting to clean up bad sample data caused by GPS glitches

- Sample grouping and averaging to find the "most likely" set of sample points for the center of the network

- Several drawing modes for different visualizations of the data: Estimated network range, interpolated signal level graphing, travel path, estimated network center point, convex hull of all sample points, etc. Networks can be colored by channel or WEP type

14

15
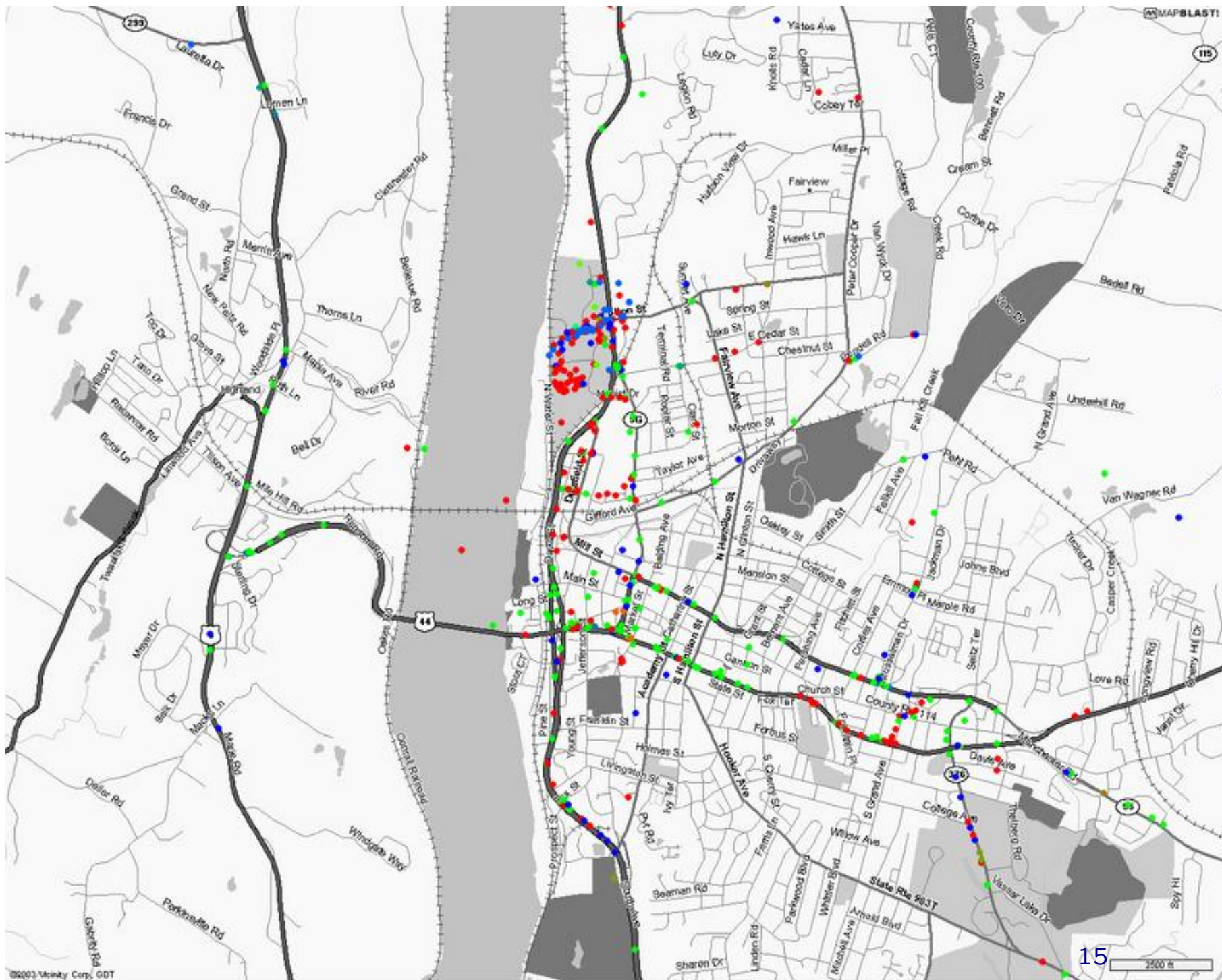
Map Coordinates : 41.711624,-73.931358 @ scale 20000
Visible networks: 1166
Map Created   : Tue Mar 23 11:50:14 2004

Channel Number

1   11

Map generated by Kismet/GPSMap 2004.03.devel - http://www.kismetwireless.net

Map Coordinates : 41.723209,-73.934006 @ scale 6000
Total networks   : 2747
Visible networks : 732
Map Created   : Thu Mar 4 15:56:50 2004

WEP Encrypted - 153 (20.90%)
Unencrypted - 464 (63.39%)
Factory Default - 115 (15.71%)

Signal Level
<- Weaker   Stronger ->

Map generated by Kismet/GPSMap Feb.04.01 - http://www.kismetwireless.net

- Prism2/2.5/3 – Excellent 11b card that is very well understood with good drivers. Best chipset for wireless hacking

- Orinoco – Old Orinocos work very well. New Orinocos have changed to HermesII which cannot yet do rfmon

- Atheros – 11a/11b/11g chipset with good general and monitor support

- PrismGT – Monitor capable drivers in Linux

Cards that work

- Airport – OSX airport rfmon drivers work but can be touchy

- Centrino – Drivers have rfmon in Linux, but currently report invalid packets with no method to validate them

- Cisco – Hardware is good, drivers are unreliable

- Acx100 – Drivers with rfmon for some platforms

- Admtek – Binary drivers for Linux with a monitor mode hack, GPL drivers under development

- Broadcom — many cards use a broadcom chipset. Broadcom will not release specs to write open drivers.

- Airport Extreme — Rebadged broadcom

- Atmel — Atmel cards have no monitor ability in the chipset

- Realtek — Primarily software driven, but no monitor support

- HermesII — No monitor support yet in the drivers

- Centrino 2200 — No useable open drivers yet for the 802.11g chipset

- Ralink — No rfmon support in the drivers

- Netstumbler – http://www.netstumbler.com – Windows stumbler

- Kismac – http://www.binaervarianz.de/projekte/programmieren/kis[
  – OSX native passive sniffer similar to Kismet

- Ethereal – http://www.ethereal.com – Graphical general sniffer for many platforms

- Tcpdump – http://www.tcpdump.org – Text-based general sniffer for many platforms

20

Following passwords are just some of those captured in half an hour between talks today. Any look familiar? Remember: never trust random wireless networks, and WEP where everyone knows the key is the same as no WEP at all.

```
Passwords removed from the online copy of this
presentation to protect the vulnerable.
```

Contact

- Email: `mike@kismetwireless.net`
- Presentation download: `http://www.kismetwireless.net/presentation`
- Software download: `http://wwww.kismetwireless.net`