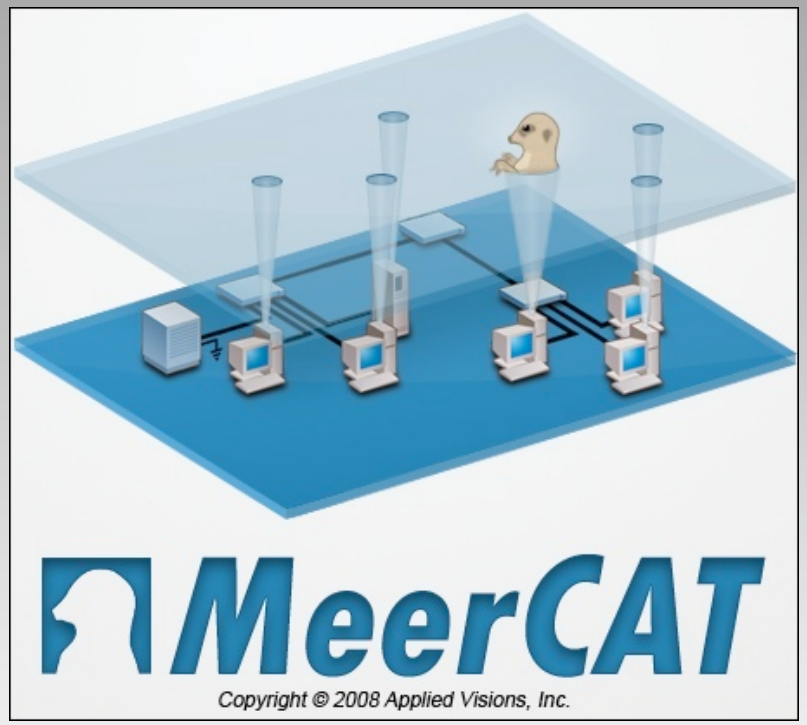
Wireless Cyber Assets Discovery Visualization

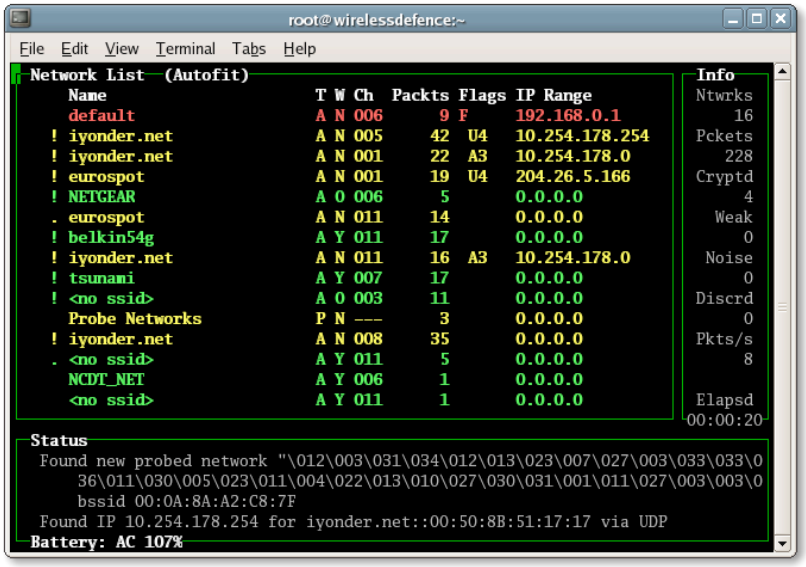
VizSec 2008- September 15, 2008



Ken Prole, John R. Goodall, Ph.D,
Anita D. D'Amico, Ph.D, Jason K. Kopylec

Problem

- Analysts ‘look’ through wireless discovery and intrusion detection data
  - Security audit for policy compliance
  - Locate vulnerabilities and threats
  - Assess risks
  - Verify remediation
- Significant data, expertise to interpret



Operational Application

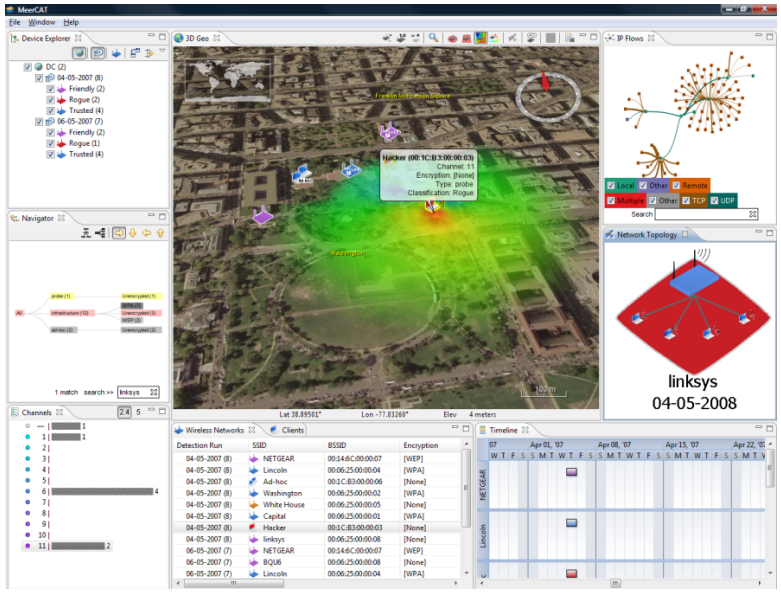
- **Wireless Discovery**
  - Typically mobile collection of large areas
  - Discover and analyze threats from and risks to wireless devices
  - Periodic audit, e.g. military or corporate campuses
  - DoD's Flying Squirrel, Kismet discovery tool, packet data

Operational Application

- **Wireless Intrusion Detection System**
  - Pre-positioned sensors, usually limited area
  - Wired and wireless enterprise network risk management
  - Real-time in-building monitoring
  - Government and commercial WIDS

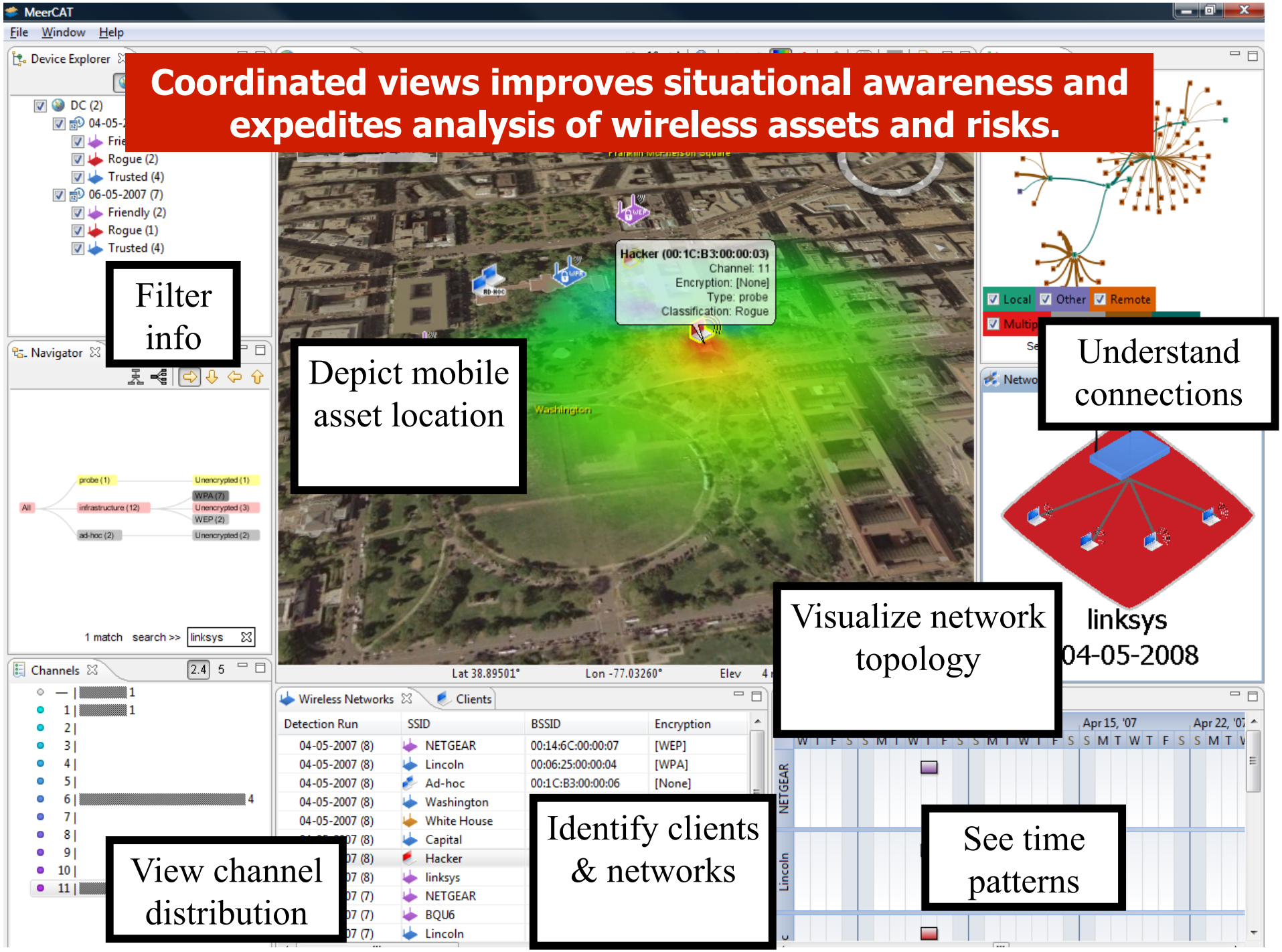
MeerCAT – Viz of Cyber Asset Tracks

- Phase II DARPA Small Business Innovative Research (SBIR)
- Multiple, linked visualization of WiFi Discovery/Security
  - **Location:** geographic and topological
  - **Security:** threats and vulnerabilities
  - **Communication Flows**
  - **Temporal Patterns**
  - **Mission:** cyber assets
- Cross platform, native UI
- Undergoing beta testing
  - Government sites and security consultant



MeerCAT

MeerCAT provides cross-platform, visual tools to analyze mobile cyber asset security and location information.


MeerCAT
File Window Help
Device Explorer
DC (2)
Rogue (2)
Trusted (4)
06-05-2007 (7)
Friendly (2)
Rogue (1)
Trusted (4)
Coordinated views improves situational awareness and expedites analysis of wireless assets and risks.
Filter info
Navigator
probe (1)
Unencrypted (1)
All
WPA (7)
infrastructure (12)
Unencrypted (3)
WEP (2)
ad-hoc (2)
Unencrypted (2)
1 match search >> linksys
Depict mobile asset location
Hacker (00:1C:B3:00:00:03)
Channel: 11
Encryption: [None]
Type: probe
Classification: Rogue
Washington
Lat 38.89501° Lon -77.03260° Elev
Local Other Remote
Understand connections
linksys
04-05-2008
Visualize network topology
Channels
2.4 5
View channel distribution
Wireless Networks
Clients
Detection Run SSID BSSID Encryption
04-05-2007 (8) NETGEAR 00:14:6C:00:00:07 [WEP]
04-05-2007 (8) Lincoln 00:06:25:00:00:04 [WPA]
04-05-2007 (8) Ad-hoc 00:1C:B3:00:00:06 [None]
04-05-2007 (8) Washington
04-05-2007 (8) White House
Capital
Hacker
linksys
NETGEAR
BQU6
Lincoln
Identify clients & networks
Apr 15, '07
Apr 22, '07
NETGEAR
Lincoln
See time patterns