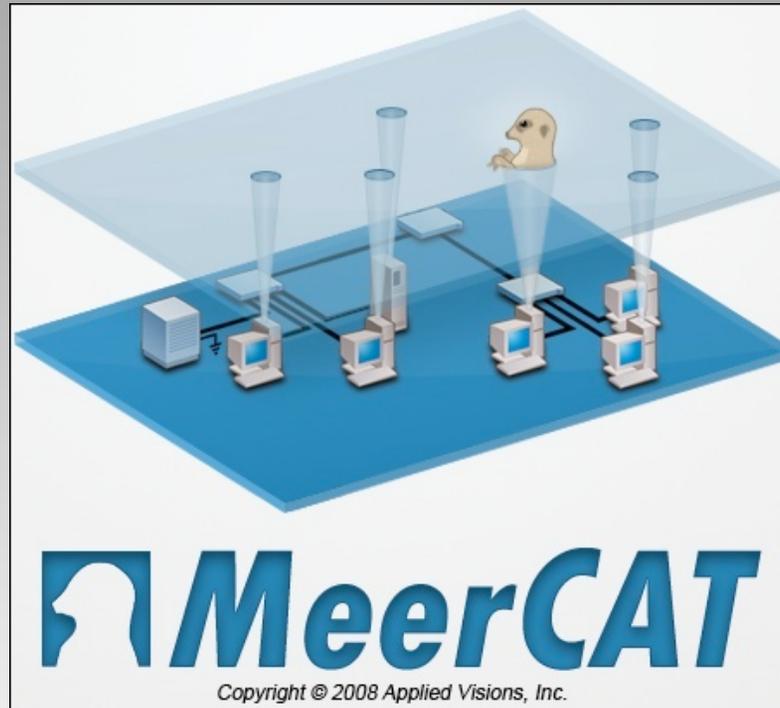


Wireless Cyber Assets Discovery Visualization

VizSec 2008- September 15, 2008



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



SBIR Data Rights (DFARS 252.227-7018 (June 1995))

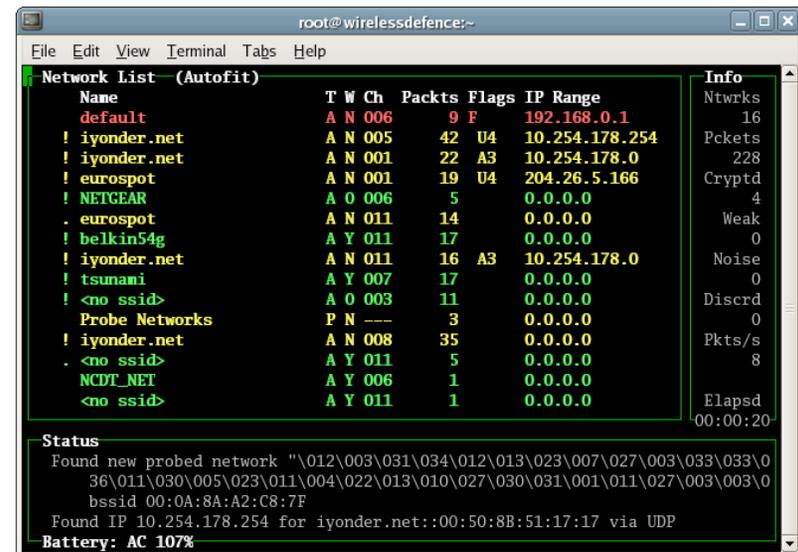
Contract No.: W31P4Q-07-C-0022, Contractor Name: Secure Decisions, a division of Applied Visions, Inc., Address: 6 Bayview Ave, Northport, NY 11768

Expiration of SBIR Rights Period: 5 years from completion date of the above SBIR Contract.

The Government's rights to use, modify, reproduce, release, perform, display or disclose technical data or computer software marked with this legend are restricted during the period shown as provide in paragraph (b)(4) of the Rights in Noncommercial Technical Data and Computer Software – Small Business Innovation Research (SBIR) Program clause in the above identified contract. No restrictions apply after the expiration date shown above. Any reproduction of technical data, computer software, or portions thereof marked with this legend must also reproduce the markings.

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



The screenshot shows a terminal window titled 'root@wirelessdefence:~' with a menu bar (File, Edit, View, Terminal, Tabs, Help). The main content is a 'Network List (Autofit)' table with columns: Name, T, W, Ch, Packts, Flags, IP Range, and Info. Below the table is a 'Status' section with several lines of text.

Name	T	W	Ch	Packts	Flags	IP Range	Info
default	A	N	006	9	F	192.168.0.1	Ntwrks 16
! iyonder.net	A	N	005	42	U4	10.254.178.254	Pckets 228
! iyonder.net	A	N	001	22	A3	10.254.178.0	Cryptd 4
! eurospot	A	N	001	19	U4	204.26.5.166	Weak 0
! NETGEAR	A	O	006	5		0.0.0.0	Noise 0
. eurospot	A	N	011	14		0.0.0.0	Discrd 0
! belkin54g	A	Y	011	17		0.0.0.0	Pkts/s 8
! iyonder.net	A	N	011	16	A3	10.254.178.0	Elapsd 00:00:20
! tsunami	A	Y	007	17		0.0.0.0	
! <no ssid>	A	O	003	11		0.0.0.0	
Probe Networks	P	N	---	3		0.0.0.0	
! iyonder.net	A	N	008	35		0.0.0.0	
. <no ssid>	A	Y	011	5		0.0.0.0	
NCDT_NET	A	Y	006	1		0.0.0.0	
<no ssid>	A	Y	011	1		0.0.0.0	

Status
Found new probed network "\012\003\031\034\012\013\023\007\027\003\033\033\036\011\030\005\023\011\004\022\013\010\027\030\031\001\011\027\003\003\0 bssid 00:0A:8A:A2:C8:7F
Found IP 10.254.178.254 for iyonder.net::00:50:8B:51:17:17 via UDP
Battery: AC 107%

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

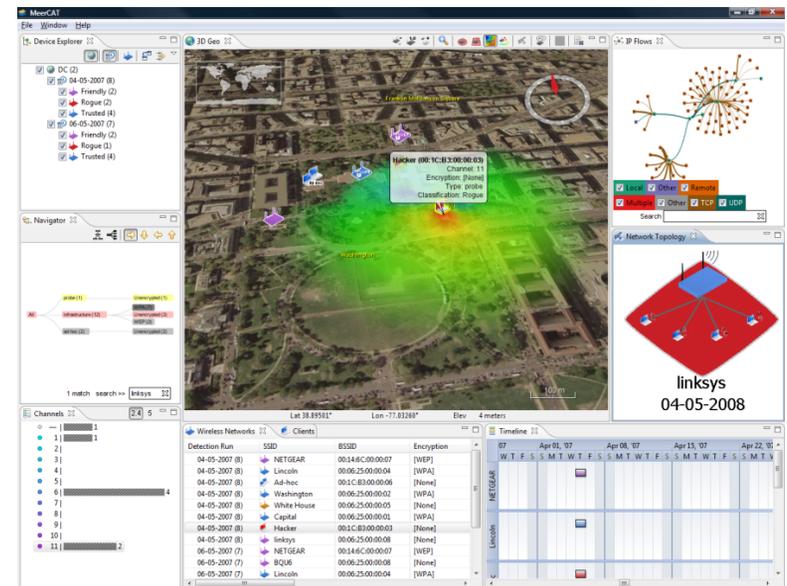


◆ Wireless Intrusion Detection System

- 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.

Coordinated views improves situational awareness and expedites analysis of wireless assets and risks.

Filter info

Depict mobile asset location

Understand connections

Visualize network topology

View channel distribution

Identify clients & networks

See time patterns

The screenshot displays the MeerCAT software interface with several key components:

- Device Explorer:** A tree view on the left showing device categories such as DC (2), 04-05-2007 (7), Rogue (2), Trusted (4), and others.
- Navigator:** A central navigation pane with icons for search and zoom.
- Channels:** A view at the bottom left showing channel distribution with a search for 'linksys'.
- Wireless Networks & Clients:** A table at the bottom center listing detected networks and clients.
- Map:** A central satellite map showing a geographic area with a heatmap overlay and a 'Hacker' asset icon.
- Network Topology:** A diagram on the right showing a central node connected to several peripheral nodes.
- Calendar:** A calendar view at the bottom right showing activity patterns over time.

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		
04-05-2007 (8)	Capital		
04-05-2007 (8)	Hacker		
04-05-2007 (8)	linksys		
04-05-2007 (8)	NETGEAR		
04-05-2007 (7)	BQU6		
04-05-2007 (7)	Lincoln		