Secure Decisions WildCAT is a turn-key system that helps assure the security of the IEEE 802.11 ("Wi-Fi") wireless space

WildCAT

Detection and Interdiction of Wireless Threats and Vulnerabilities

The Need

Wireless networking technologies have introduced new vulnerabilities to computer networks that existing wired defenses such as firewalls and intrusion detection / prevention systems are unable to address.

Even organizations that do not have a wireless infrastructure are susceptible to wireless attacks. End users can create vulnerabilities on an otherwise secure network by simply turning on wireless cards in their laptops while connected to the wired network, providing an entry point for outsiders into the wired network.

Existing wireless defenses such as wireless intrusion detection/prevention systems (WIDS/WIPS) and manual patrolling, also known as "wardriving", are not sufficient. WIDS/WIPS require a wireless infrastructure that is too costly to provide coverage of large areas like military bases, maritime ports, oil refineries, and nuclear power plants. Wardriving is time consuming, provides only an occasional sample of the wireless space, and requires specially trained staff to perform collection.

The Solution

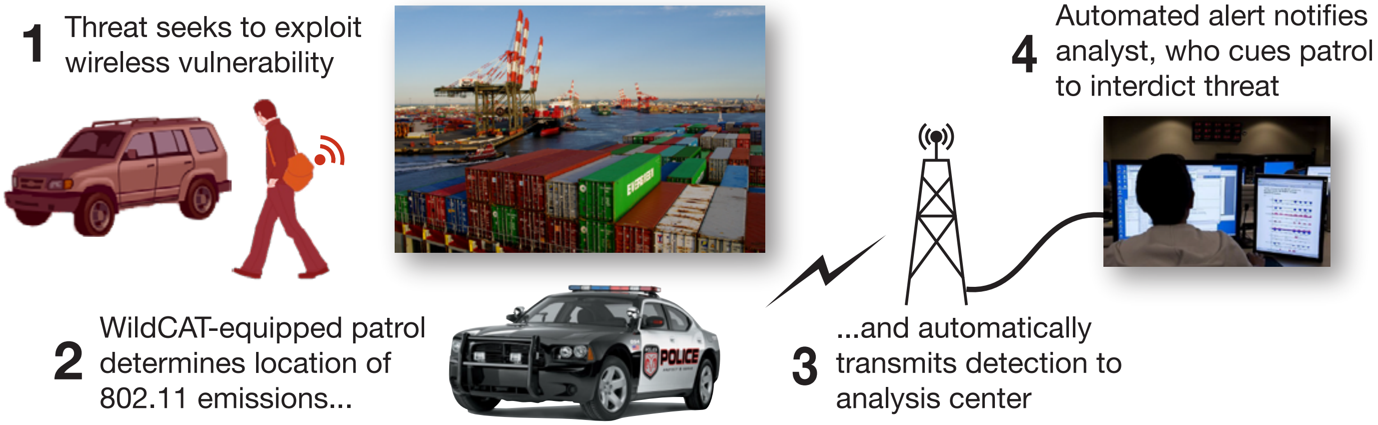
The innovative WildCAT design leverages existing physical security forces to help assure information systems security. It provides a rich visual interface for analyzing wireless networks and supports automated alerting based on risk categories to minimize time and labor costs associated with analysis.

Our approach outfits existing security/maintenance/delivery vehicles with a small wireless discovery system. This discovery system, which operates whenever the ignition is on, collects 802.11 network data and securely transmits it over a cellular data network to a centralized monitoring and analysis center. There, analysts use automated alerts and a visual analysis software tool to identify suspicious events in the incoming data stream. If an analyst discovers a potential threat, he can send a message to a display inside the patrol vehicle. This allows the physical security force to interdict the threat.

The combination of a persistent physical security force presence with the computer security expertise of remotely located network defenders allows WildCAT to:

- Detect and locate wireless network threats and vulnerabilities
- Assess compliance with defensive network policies (e.g., wireless ban)
- Respond to wireless network attacks and vulnerabilities

WildCAT provides a much greater degree of coverage than manual patrols. If we use our assumption that personnel currently have time conduct 2 hour manual patrols 3 times per week, this means that the "time under patrol" is only 6 hours per 168 hour week – only 3.5% of the time. Employing WildCAT would allow for 2 patrols to be run per shift, increasing the time under patrol to 84 hours – a much more comprehensive 50% of the time.



1 Threat seeks to exploit wireless vulnerability

2 WildCAT-equipped patrol determines location of 802.11 emissions...

3 ...and automatically transmits detection to analysis center

4 Automated alert notifies analyst, who cues patrol to interdict threat

SECURE DECISIONS
A DIVISION OF APPLIED VISIONS, INC.

Secure Decisions performs cyber security research and develops software products for government and commercial customers

SECUREDECISIONS.COM
info@securedecisions.com
(631) 759-3988

6 Bayview Avenue
Northport, NY 11768

Uses

Facility security
Threat monitoring & analysis
Compliance reporting
Insider threat detection
Vulnerability assessment

Questions that WildCAT helps answer:

- ✓ Are there any unauthorized wireless access points detected within 1 km of the boundaries of the facility?
- ✓ Has that SSID been seen near the property within the past month?
- ✓ Has that same SSID been spotted at other, perhaps distant, sites?
- ✓ Have unauthorized access points connected to the enterprise?
- ✓ To whom did they connect?
- ✓ Are they located within or outside the boundaries of the site?
- ✓ Are our wireless access points encrypted in accordance with policy?

Users

Network administrators
Physical security teams
Compliance auditors
Information security professionals
Vulnerability assessors

With WildCAT, users can analyze data collected over time and drill down for details. The workstation is based on the MeerCAT visual analysis system. MeerCAT was originally developed by Secure Decisions for DoD analysis of wireless vulnerabilities, and now has ~1,600 users throughout the DoD, NSA, and private defense contractors. The proven MeerCAT design helps network defenders locate 802.11-based wireless assets and networks to assess their risks using data from tools like Flying Squirrel, Kismet, and NetStumbler.

Key Benefits

Enhanced threat detection Increase time under wireless security coverage from 3.5% to 50% and identify hard-to-see patterns in volumes of data

Speed response Reduce cycle time from detection, to analysis, and response

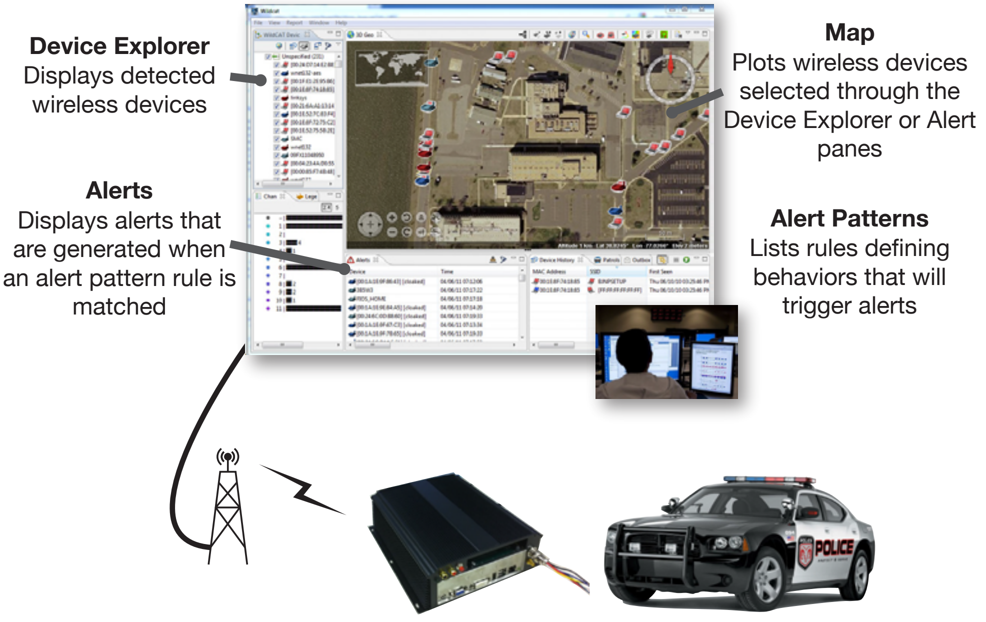
Save money Reduce recurring cost of wireless security patrols by using existing facility security personnel and save analysis time with WildCAT visual analysis tool

Easy reporting Create documents and presentations directly from WildCAT

Affordability Low capital expenditure to instrument fleet or facility with a reasonable software license fee

Ease of use Up and running quickly

Analysis workstation



Device Explorer
Displays detected wireless devices

Alerts
Displays alerts that are generated when an alert pattern rule is matched

Map
Plots wireless devices selected through the Device Explorer or Alert panes

Alert Patterns
Lists rules defining behaviors that will trigger alerts

In-vehicle collector

About WildCAT

WildCAT was sponsored by DHS Science & Technology, in contract to the Long Island Forum for Technology (LIFT). WildCAT is an extension of our MeerCAT Phase III SBIR. MeerCAT (TRL 9) is a wireless security visualization technology originally sponsored by DARPA under contract W31P4Q-07- C-0022. It has been transitioned to operational use through collaboration with Naval Research Laboratory using DISA maintenance and support funding.

Support From

Homeland Security
Science and Technology

LIFT
LONG ISLAND FORUM FOR TECHNOLOGY

APPLIED SCIENCE FOUNDATION FOR HOMELAND SECURITY
Public Safety • Research • Economic Development • Education