WildCAT

Detection and Interdiction of Wireless Threats and Vulnerabilities

WIRELESS SECURITY

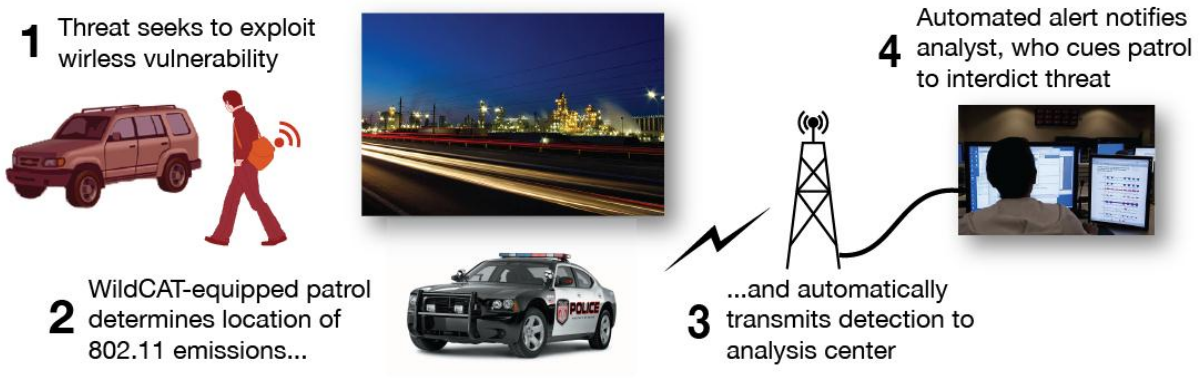
Wireless networking technologies have introduced new vulnerabilities to computer networks that existing wired defenses such as firewalls and intrusion detection/prevention systems are unable to address. Even organizations that do not have a wireless infrastructure are susceptible to wireless attacks. 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.

WILDCAT

In response to this need, Secure Decisions has developed a turn-key system, called WildCAT, which can assure the security of the IEEE 802.11 ("Wi-Fi") wireless space. 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.

WILDCAT SYSTEM OPERATIONS



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 device ban)
- Respond to wireless network attacks and vulnerabilities

Applied Visions, Inc.
Secure Decisions Division
Anita.DAmico@securedecisions.com 631-759-3909

WildCAT

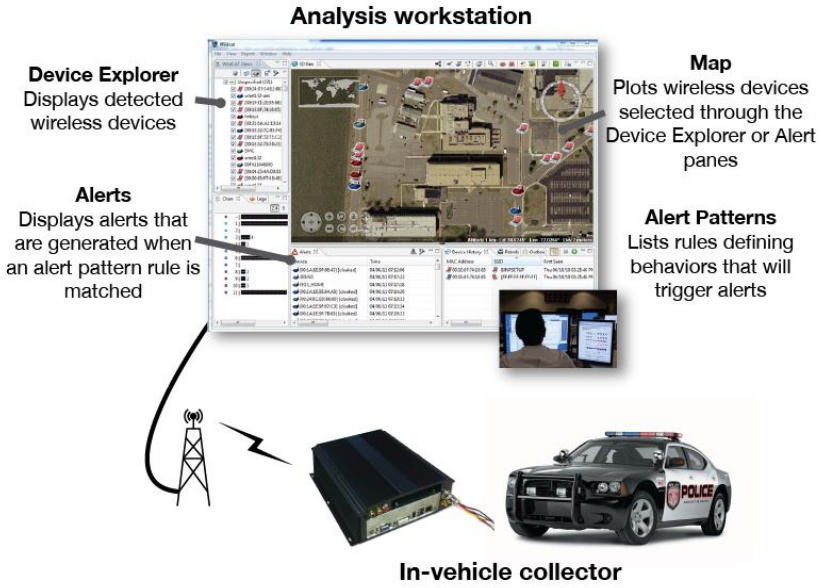
Detection and Interdiction of Wireless Threats and Vulnerabilities

SYSTEM OVERVIEW

A simplified overview of the WildCAT system is shown below. The two visible components of the system are the "collectors" and the "analysis workstation". Not shown is server software that receives data from the collector hardware and makes it available to the analysis workstation software.

The ruggedized in-vehicle collector is equipped with an 802.11 network detector, a GPS device, and cellular network connectivity. This collector runs a modified version of the Naval Research Laboratory ***Flying Squirrel*** wireless discovery software and also consists of a magnetically mounted, omnidirectional antenna, and an in-vehicle display for showing messages sent by an analyst.

The analysis workstation allows analysts to drill down more deeply into the collected wireless data. The workstation has been designed to support the visual information-seeking mantra of "overview first", then "zoom and filter", and "details on-demand". This approach allows analysts to efficiently sift through large volumes of data and aids detection of suspicious wireless activity.



Increase time under wireless security coverage by 1400%

Low capital expenditure

Reduce recurring cost of wireless security patrols

Save analyst time

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. MeerCAT provides a 3D geographic map display of wireless devices, their attributes, and relationships – as well as visual representations that support comparisons over time. Multiple coordinated views support rapid exploration of the data.

FUNDING

WildCAT (TRL 5) 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.

Applied Visions, Inc.
Secure Decisions Division
Anita.DAmico@securedecisions.com 631-759-3909