Integrating Physical and Cyber Security Resources to Detect Wireless Threats to Critical Infrastructure

Anita D'Amico, Christina Verderosa, Christopher Horn, Timothy Imhof
Applied Visions Inc., Secure Decisions Division
Northport, NY, USA
{anitad, christinav, chrish, timothyi}@securedecisions.com

***Abstract*— Critical infrastructure can be vulnerable to cyber attacks through 802.11 wireless networks. Because wireless intruders are within short range of the targeted network, they can be directly observed by security forces cued to their presence. WildCAT is a prototype system that extends the reach of a physical security force into the cyber realm to detect and respond to wireless threats and vulnerabilities. Its design uses physical security vehicles as the platform for collecting wireless network activity that is then sent via a cellular network to an analysis center. At the analysis center, cyber security specialists detect suspicious activity and cue the physical security force to its location. WildCAT will be tested in comparison to traditional approaches to wardriving, as well as a supplement to wireless intrusion detection systems.**

Keywords- critical infrastructure protection; cyber attack; computer security; physical security; wireless intrusion detection; wireless security

I. INTRODUCTION

Over the past decade, the adoption and deployment of wireless networking technology has soared. Notably popular is the IEEE 802.11 family of wireless standards. These standards, which describe the technical details of how to modulate radio frequency signals to facilitate data communications, are more commonly known as Wi-Fi wireless technology.

The ubiquity of 802.11 wireless computer networks renders critical infrastructures vulnerable to cyber attack. Wireless attacks via 802.11 are distinct from other methods of network attack in that the intruder must physically locate his wireless communications equipment within a relatively short range of the targeted network in order to execute an attack [1]. This represents a unique opportunity for network defenders to detect, geographically locate, and physically respond to network attack threats.

A. Approach

Conventional network defense is conducted from a centralized operations center that is often geographically distant from the network and infrastructure being defended. This works well for network-based attacks, but fails to leverage the defensive advantage introduced by the physical aspect of 802.11-based attacks.

A challenge to leveraging this defensive advantage, however, is that it requires a physical presence. Today, cyber vulnerability specialists, armed with specialized wireless discovery equipment and software, "wardrive" through an area only intermittently. Many organizations cannot afford the cost of using cyber vulnerability specialists to provide more continuous wireless surveillance. This limits their windows of opportunity for detecting both authorized devices that are not complying with security policies and unauthorized devices on or near the protected area.

The WildCAT concept of operations (CONOPS) leverages the persistent presence of a physical security force near a high-value target with the computer security expertise of remotely located network defenders to address this problem. Its turn-key, real-time wireless vulnerability assessment system provides more persistent detection and assessment of compliance with defensive network policies (e.g., prohibition of unauthorized wireless devices), identification of unauthorized wireless devices, and response to wireless network attacks.

Figure 1 depicts the CONOPS for the WildCAT system. Our approach outfits existing mobile security forces with a wireless discovery system that is installed in the trunk of patrol cars. This discovery system, which operates automatically upon turning the ignition key, passively collects 802.11 network data when the vehicles are on patrol and securely transmits the captured data over a cellular data network to a centralized monitoring and analysis center. There, analysts work with the incoming, real-time data stream to filter and parse the data using a visual analysis software tool. If an analyst discovers a potential threat or compliance violation, he or she can send a message back to an information display inside the patrol car, providing the physical security officer with instructions on how to proceed along with a map of the estimated location.

B. Vulnerabilities and Threats

Vulnerabilities and attacks on 802.11 technologies exist in addition to those that operate at the network layer and higher. While improved methods of encryption aid in protecting wirelessly transmitted information, wireless access points are still vulnerable to attacks, whether they are in a home, at a power plant, or serving other critical infrastructure.

Vulnerabilities are easily created with wireless technology – either intentionally (e.g. insider threat, policy circumvention)

This research project is sponsored by the US Department of Homeland Security Science & Technology under the Applied Science Foundation for Homeland Security (contract number HSHQDC-10-C-00062). Any opinions, findings and conclusions or recommendations presented in this material are those of the author(s) and do not necessarily reflect the views of the Department of Homeland Security.

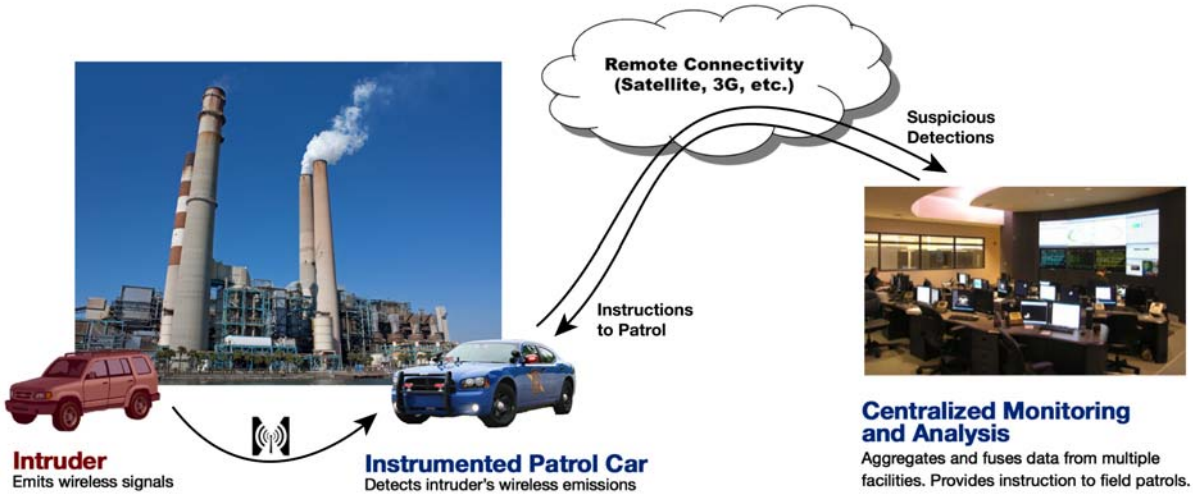

Figure 1. CONOPS for the WildCAT system

or unintentionally (e.g. through ignorance or mistake). Devices can be misconfigured, creating open windows through which attackers may send network data or eavesdrop. Staff may set up unauthorized wireless devices, or bring them into secure facilities (e.g., smartphones) for convenience, without malicious intent. Finally, staff can connect their wireless devices to external or rogue networks – either intentionally (e.g., to circumvent network policy) or unintentionally (e.g., falling prey to an evil twin attack). These connections can expose sensitive information to an unsecured network.

These vulnerabilities can be exploited by attackers. One common attack specific to wireless is the "evil twin" attack. The objective of an evil twin attack is to lure clients into associating with an unauthorized access point (AP). This unauthorized AP, which is controlled by the attacker, is configured to mimic the appearance of a legitimate AP. When clients connect through this AP, the attacker can read and/or alter all of the data that the client transmits through the AP.

Another type of attack uses an unauthorized device to connect to a trusted network. In this situation, an attacker may simply be trying to establish a wireless network connection with a target network in order to launch other non-wireless attacks. This was the case in a theft incident at TJX, a major off-price retailer of apparel and home fashion.

In 2007, TJX publically announced that they had begun investigating suspicious software that was found on their computer system. As the investigation unfolded, it was discovered that over 45 million credit card numbers and other personal information was stolen. Cyber criminals had gained unauthorized access to a server that housed confidential information via a poorly encrypted wireless access point. The attackers had launched this attack from the parking lot of a TJX store using a typical laptop computer. They successfully managed to stay under the radar for over a year while extracting millions of records of customers' personal information.

Unfortunately, critical infrastructures of any facility are susceptible to attacks similar to those on TJX [2][3]. Technical solutions to the problem of detecting and responding these incidents exist, but have not been implemented as uniformly as necessary.

The WildCAT CONOPS offers a means to cost effectively extend the reach of a physical security forces into the cyber realm by equipping them with a means to persistently monitor the wireless space around a facility and respond to wireless threats and vulnerabilities in near real-time.

The WildCAT can identify vulnerabilities and behavior associated with these attacks and vulnerabilities by looking at the attributes of wireless network devices such as the type of encryption, network type, MAC address, physical location, detection frequency, connection patterns, channel usage, and broadcast SSID. The potential for high false positive detection rates is mitigated through the use of a whitelist-based approach that looks for wireless device traffic and configuration data that differs from a known and trusted setup

C. Current Methods of Vulnerability & Threat Detection

There are currently two common ways in which a wireless threat can be detected: a technique known as wardriving and use of wireless intrusion detection systems (WIDS). WildCAT is based on wardriving.

Wardriving is a technique for collecting wireless network data that involves driving around in a vehicle collecting information about the wireless network traffic that is detected. Wardriving requires a laptop running a wireless discovery program such as Kismet, NetStumbler or Flying Squirrel, a GPS device, and an antenna. This technique usually lacks real-time threat detection because it requires further analysis that cannot be performed while driving. It is also a time-consuming process, requiring specially trained staff in order to perform the collection and vulnerability analysis. A WIDS consists of a system of sensors, which collect 802.11 data and forward it to a central management system where it is processed and stored. Although WIDS are effective, they are expensive, difficult to deploy and maintain, and limited to the boundaries of the sensors [4].

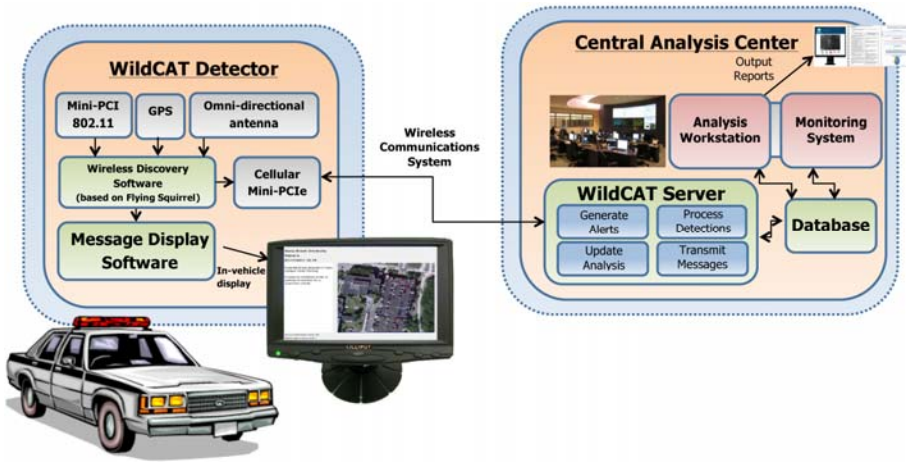

Figure 2. WildCAT system architecture

Both WIDS and wardriving techniques do have some documented problems with unreliable hardware performance and high false alarms rates [3].

Due to the pervasiveness of wireless networks, both wardriving and WIDS collect an overwhelming amount of data [5]. It is difficult to identify relatively infrequent security risks amidst the massive amounts of information collected. Cyber analysts are specially trained to parse through this data to quickly identify and respond to any wireless threats. The WildCAT approach maximizes the time spent by cyber analysts on threat analysis by removing the need for them to conduct wardrives.

II. ARCHITECTURE

An overview of the WildCAT system architecture is shown in Figure 2. There, we can see the two major components: the WildCAT Detector and the Central Analysis Center. The Central Analysis Center can be broken down into two major components, the Monitoring System and Analysis Workstation. Each of these components is described below.

To address the data collection challenges encountered with wardriving, we designed the WildCAT Detector based on the Flying Squirrel 802.11 collection system developed by the Naval Research Laboratory (NRL) [6]. Modifications to Flying Squirrel software were made to run the software automatically upon starting the patrol car. This software package was loaded onto a heat and vibration resistant computer pod that can be installed in the trunk of a car. These modifications were performed by NRL to leverage a similar capability developed for use in unmanned aerial vehicles.

The WildCAT Detector is responsible for collecting and sending three types of data, GPS, network packet, and transmitter every second. The GPS metadata includes date, time, latitude, longitude, altitude, fix quality, and number of satellites in view. The GPS data is used to display the wireless devices/clients and patrol vehicle locations in the correct position on the maps in the Central Analysis Center. The transmitter metadata consists of transmission data collected between a client and an access point and includes source MAC addresses, destination MAC addresses, number of packets, and relative signal strength. The network packet data consists of beacon frame or probe responses, which includes an IEEE 802.11 header, followed by an IEEE 802.11 management header. A single network packet data message will be sent for each Beacon or probe response that was detected.

The WildCAT Detector is a single board computer equipped with an 802.11 network card, a GPS device, and a cellular network card packed in a ruggedized pod. This computer runs a modified version of the Flying Squirrel wireless discovery software and an application to receive messages from the Analysis Center. The WildCAT Detector also consists of an omni-directional antenna magnetically mounted on the roof of a car, and an in-vehicle display fixed on the dashboard, to receive instructional messages sent from an analyst. The WildCAT Detector under ideal conditions has a range of approximately 820 feet [7]. The WildCAT Detector automatically starts up and begins collection when the vehicle is started and requires no human interaction with the hardware.

WildCAT's Analysis Center uses information visualization and visual analytics techniques to filter and highlight the large volumes of data, and to aid detection of suspicious wireless behavior. The Analysis Center incorporates the overview, zoom, drill down for details mantra of information visualization [8]. The Analysis Center is configured to handle incoming detection data from the WildCAT Detectors every second. Multiple WildCAT Detectors can be used to provide adequate coverage of a physical location.

The Analysis Center consists of both a Monitoring System and an Analysis Workstation. The Monitoring System provides the analyst with an overview of each site being analyzed; it

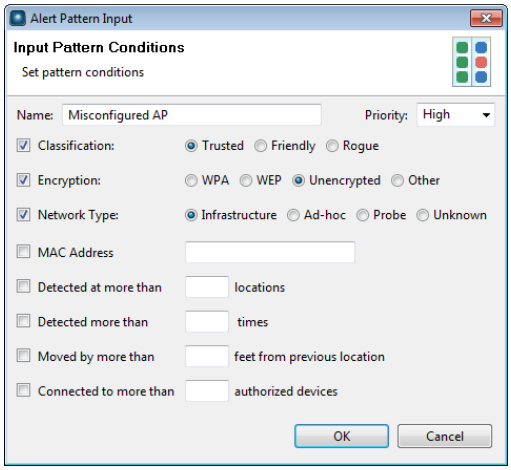

Figure 3. Dialog for rules configuration in the Analysis Workstation

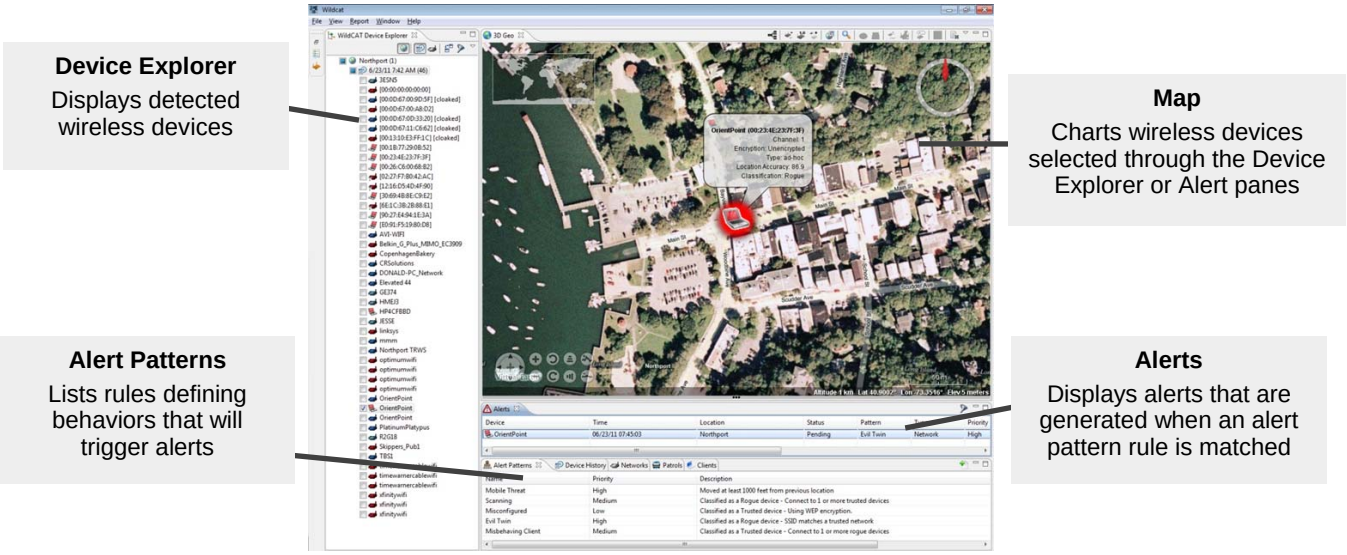

Figure 4. Overview of alert handling in the WildCAT Analysis Workstation

displays wireless threat alerts at each location and allows for quick filtering based on several alert attributes. The Monitoring System is dynamically updated as detection data is automatically relayed from the vehicle to the Analysis Center. Inside the Monitoring System, the analyst can drill down to a specific alert and view high-level details. Wireless threat alerts are generated automatically in the Analysis Center when incoming detections match rules that define suspicious behavior patterns. In order to reduce false positives, WildCAT requires the cyber-analyst to communicate the alert to the physical security patrols through a messaging system.

The Analysis Workstation is where the analyst can drill down more deeply into the data. Figure 4 depicts an overview of the Analysis Workstation user interface that analysts interact with to view and manage alerts. The rules which generate alerts are defined by an analyst in the Analysis Workstation using the dialog shown in Figure 3. WildCAT by default defines various rules that are common examples of suspicious behavior including misconfigured trusted access points, rogue devices connecting to trusted devices, and rogue devices found changing locations.

The Analysis Workstation is based on the MeerCAT visual analysis system originally developed for Department of Defense analysis of wireless vulnerabilities [9]. MeerCAT is a visualization tool that helps network defenders and decision makers locate 802.11-based wireless assets and networks, and assess the risks to their organization from unauthorized wireless devices. It is designed for post-hoc analysis of data acquired from a variety of sources that discover and locate wireless transmitters. MeerCAT provides a 3D geographic fly-through visualization showing satellite imagery, graphical views of physical objects, their attributes and relationships, and visual representations comparing data that has been collected over time. All of the MeerCAT views are linked to provide multiple perspectives of the data and an intuitive interactive visual environment where highlighting or filtering in one view is reflected in all other views [10]

III. Test and Demonstration

An important component of our development plan is to test and demonstrate the WildCAT system. Our plan is divided into two phases: first, we verified WildCAT performance in a testing environment created by an independent third party, and second we plan to verify and validate WildCAT at a site with existing wireless infrastructure.

A. Phase I Test Plan & Results

Our plan for the first phase of testing was to create an environment that would allow us to evaluate the ability of the WildCAT system to perform baseline functionality, as well as detect a predetermined set of suspicious behaviors. In July 2011, we collaborated with Assured Information Security (AIS), Inc. to plan and conduct this testing. AIS set up a wireless network testing environment at the Griffiss Business and Technology Park in Rome, NY and staged attacks on this network.

Trusted wireless APs and authorized clients were installed in four locations around the test site, according to the layout shown in Figure 5. The APs were four Linksys Wireless-G Wireless Broadband Routers (WRT54GL). The clients were four Dell laptops (Inspiron 6400, Inspiron 9400, Inspiron 6000, Precision M4400) running Windows XP and four Gateway LT2802U netbooks running Windows 7 Starter.

At each site, the clients were configured to associate with the AP at that site; one of the sites had three clients, one site had one client, and the other two sites had two clients. Into the Central Analysis Center, we imported the list of and configuration data for the trusted APs and authorized clients. WildCAT Detectors were installed in two vehicles.

For five consecutive days, both vehicles performed twice-daily patrols of the area for approximately 30 minutes. On each day, at least one of five adversarial scenarios was practiced.

For the first baseline patrol, we verified that the WildCAT system:

- Determined the correct geographic coordinates for trusted APs
- Recognized correct configuration of trusted APs and authorized clients
- Recognized the correct association pairings of trusted APs and authorized clients

The five scenarios were run as follows:

1. **An evil twin access point** An evil twin access point was set up with the same SSID and encryption settings as one of the trusted APs, but with a different MAC address. A WildCAT Detector was driven past the evil twin and the Central Analysis Center was checked to confirm that it fired an "evil twin alert".
2. **Access point with configuration changes** A trusted access point had its configuration altered to downgrade its encryption setting. A WildCAT Detector was driven past the re-configured trusted access point and the Central Analysis Center was checked to confirm that it fired a "misconfigured AP alert".
3. **Authorized client leaving a trusted access point** An authorized client was configured to associate to an additional access point that had a different SSID, encryption setting, and MAC address from any of the trusted APs. A WildCAT Detector was driven past the authorized client and additional access point and the Central Analysis Center checked to confirm that it fired a "misbehaving client alert".
4. **Targeted MAC address transmitting** The Central Analysis Center was configured with a custom alert pattern to identify when wireless transmissions from a radio with a specific MAC address were identified. A WildCAT Detector was driven past the client with the targeted MAC address and the Central Analysis Center checked to confirm that it fired the custom alert.
5. **Rogue client connected to an access point** An additional client was configured to associate with a trusted access point. A WildCAT Detector was driven past the additional client and trusted access point and the Central Analysis Center checked to confirm that it fired a "scanning alert".

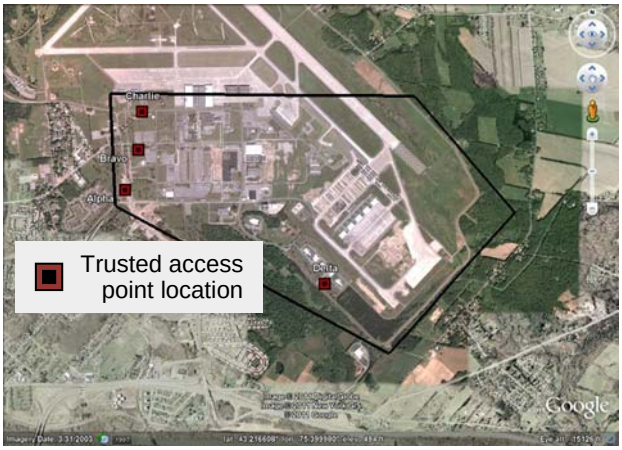

Figure 5. Map of Phase 1 test area in Rome, NY

For the baseline patrol and each of the five scenarios the WildCAT system performed as intended.

B. Phase II Test Plan

The second testing and demonstration phase is to be conducted over a period of at least two weeks at a site with a well-defended wireless network. Once again, a red team will conduct common wireless attacks; for example, performing an evil twin attack, attempting unauthorized access, and installing a misconfigured access point. The effectiveness of WildCAT will be compared with the test site's existing wireless security practice – periodic wardrives, a WIDS, or a combination of the two – using a set of performance metrics described below. Each method of providing wireless security (WildCAT, wardriving, and/or the WIDS) will be characterized using these performance metrics and the results compared.

- **Area under surveillance and duration of coverage** What is the footprint of the monitored area and how often is that area under surveillance? A WIDS will have a fixed area that can be monitored 24/7; WildCAT and wardriving can monitor a much broader and more flexible area, but not each location in that area continuously.
- **Wireless device detections over a fixed time period** Does each security practice detect the same devices? Analyzing device detection log data will allow us to see whether WildCAT provides greater visibility into wireless activity than other wireless discovery methods.
- **Location accuracy of detected wireless devices** For wireless devices of a known location, how close is the calculated location to the actual, ground truth location of the detected wireless device?
- **Response time to interdict detected wireless devices** How long does it take for a response to be mounted to a suspicious device or wireless attack?
- **Required training and skill to employ system** What skills are required of the operator to conduct the tasks associated with employing each system?
- **Correctness of suspicious behavior classification** For the known attacks and suspicious behavior, did the system correctly classify each detected behavior? For example, was an evil twin AP identified as such by WildCAT, the WIDS, or a wardrive analyst?

IV. Potential Applications

Wireless communication is continuing to expand in industrial, residential, and government sectors as many people value the mobility and installation ease that wireless networking enables. However, an easy persistent method of monitoring wireless threats is needed to mitigate attacks to critical infrastructure through wireless vectors. WildCAT is designed to offer a flexible, low-cost, and easy method of wireless monitoring with existing patrol fleets.

A. *Continuous Sustained Surveillance*

High-value targets such as ports, power generation facilities, refineries, embassies, and organizations interested in protecting confidential data and critical infrastructure can use WildCAT to continuously monitor their wireless networks. The visibility of wireless activity can be increased by instrumenting WildCAT sensors into any roving vehicle (maintenance, security, delivery, etc.). If an unauthorized, or rogue, device is attempting to connect to known, authorized wireless access point, security forces should be notified immediately.

B. *Targeted Monitoring and Tracking*

Law enforcement needs the ability to link a client device and person responsible for illegal traffic observed at the ISP or IP level. With courts now recognizing that an IP does not link network activity to a person, it is crucial to collect evidence that can geo-locate a Wi-Fi client and record the network traffic being exchanged with an access point. Such evidence can successfully link a child pornographer or copyright infringer to their wireless network traffic. WildCAT is designed to be a rapidly deployable, shared resource within a group (grab & go-type device that requires little to no user training), or as silently vigilant standard vehicle equipment that is always monitoring and reporting its findings.

C. *Multiple Site Security*

Instead of configuring a WIDS at each and every location, security professionals can use WildCAT as a low cost roving sensor that travels between sites. Alternatively WildCAT sensors can be mounted to vehicles and rotated between sites.

D. *Extend WIDS Coverage*

WildCAT can reach areas that are not typically covered by fixed WIDS sensors such as parking lots, thereby adding visibility beyond a WIDS. Wireless APs can be connected to a wired LAN and as a result expose an organization to attack outside the range of deployed wireless access points and WIDS sensors.

V. Future of WildCAT

We have interviewed representatives from potential test sites and transition partner organizations regarding their detailed wireless security needs. A goal of these interviews has been to identify specific ways that WildCAT can be tailored to meet these needs.

In the course of these interviews, we discovered organizations that could benefit from the capability of a WildCAT system, but whose operational environment is not conducive to a vehicle-mounted system – for example, organizations that operate within large buildings that can even extend underground. Such organizations currently monitor 802.11 devices inside their buildings by conducting periodic scans using specialized staff, independent of their more conventional physical security force.

This presents an opportunity to develop a man-portable variant of the current vehicle-based WildCAT system to address the requirements of organizations described above. Such work, however, is non-trivial. Indoors, GPS and cellular data wireless signals are often unreliable or unavailable. Additionally, there is a real likelihood that potential WildCAT users will exhibit concerns over using a cellular data network as part of their security system.

Most of the organizations that we have spoken with employ a 24/7/365 security force. Leveraging this existing capability by equipping security personnel with small backpack-mounted 802.11 sensors offers the ability to enhance the security posture of an organization with a minimal marginal cost. Working indoors will require non-GPS-based position information. NRL has a hybrid accelerometer and GPS-based location system called Caribou [6][11] that can be adapted to work as the source of location information in the WildCAT collection system.

Another growth path is beyond 802.11 signals. Although 802.11 is the most commonly used wireless networking standard, however many industries are using different radio frequencies and standards within their organizations. Through our interviews, for example, we have learned that industrial automation systems employ 900MHz technology, IEEE 802.15.4 (ZigBee), and proprietary mesh technologies in addition to 802.11. In a future version of WildCAT, these standards plus IEEE 801.16 (WiMAX), Bluetooth, and various 3G cellular standards (e.g., UMTS, CMDA2000, and EDGE/GPRS) may also be supported.

References

[1] D. Welch, "Wireless security threat taxonomy," in *2003 IEEE Workshop on Information Assurance*, West Point, NY, 2003.

[2] Office of the Privacy Commissioner of Canada, (2007, September 24). Report of an Investigation into the Security, Collection and Retention of Personal Information, TJX Companies Inc./Winners Merchant International L.P. [Online]. Available: http://www.oipc.ab.ca/ims/client/upload/Investigation%20Report%20P2007_IR_0061.pdf

[3] B. Ngugi et al., "Lessons from the Computer Intrusion at TJX," *The CASE J.*, vol. 5, no. 2, pp. 17-25, 2009.

[4] Ken Hutchinson. (2004, October 18). *Wireless Intrusion Detection Systems* [Online]. Available: http://www.sans.org/reading_room/whitepapers/wireless/wireless-intrusion-detection-systems_1543

[5] P. Brutch and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks," in *2003 Symposium on Applications and the Internet Workshops*, 2003, pp. 368-373.

[6] United States Naval Research Laboratory. *Mobile Systems Security: Flying Squirrel* [Online]. Available: http://www.nrl.navy.mil/chacs/5545/flyingsquirrel

[7] Phil Belanger. (2007, May 31). *802.11n Delivers Better Range* [Online]. Available: http://www.wi-fiplanet.com/tutorials/article.php/3680781

[8] S. Card et al, *Readings in Information Visualization: Using Vision to Think*. San Francisco, CA: Morgan Kaufmann Publishers, Inc., 1999.

[9] K. Prole et al, "Wireless Cyber Assets Discovery Visualization," in *Proc. of the 5th Int. Workshop on Visualization for Computer. Security*, Lecture Notes in Computer Science, vol. 5210, pp. 136-143, 2008.

[10] Defense Advanced Research Projects Agency. (2010). *DARPA SBIR/STTR Success Stories* (Volume 3) [Online]. Available: http://sbir.darpa.mil/sbpo/epub/success/volume3/index.html#page27

[11] U.S. Naval Research Laboratory. *Flying Squirrel Wireless Assessment Tool Suite* [Online]. Available: http://www.nrl.navy.mil/chacs/5545/documentation/flyingSquirrel.pdf