Wireless Cyber Assets Discovery Visualization

Kenneth Prole, John R. Goodall, Anita D. D'Amico, and Jason K. Kopylec

Secure Decisions division of Applied Visions, Inc.
6 Bayview Avenue, Northport, NY 11768
{kennyp,johng,anitad,jasonk}@securedecisions.avi.com

Abstract. As wireless networking has become near ubiquitous, the ability to discover, identify, and locate mobile cyber assets over time is becoming increasingly important to information security auditors, penetration testers, and network administrators. We describe a new prototype called MeerCAT (Mobile Cyber Asset Tracks) for visualizing wireless assets, including their location, security attributes, and relationships. This paper highlights our latest iteration of our prototype for visual analysis of wireless asset data, including user requirements and the various coordinated visualizations.

Keywords: Visual analytics, wireless discovery, wireless security, coordinated views, geographic visualization, information visualization, wardriving.

1 Introduction

Wireless networks (WiFi, 802.11 protocols) are becoming increasingly more prevalent. Wireless network devices and cards are cheap; most laptops and even desktops are coming with wireless network interface cards preinstalled. While traditional wired networks can be secured from external attackers through firewalls, intrusion prevention systems, and the like, wireless networks open an entirely new kind of security threat for network administrators. Even organizations that do not have a wireless infrastructure are susceptible to wireless attacks. Unwitting end-users can open to outsiders an otherwise secure internal network by simply turning on their wireless cards while connected to the wired network, providing a bridge for malicious outsiders to access the wired network. Attackers can breach wireless networks to steal bandwidth, capture sensitive data, or attack and gain control of computers on both wireless and wired networks. Wireless security vulnerabilities have been gaining media attention. For example, the Wall Street Journal reported that the worst reported security breach of credit card data, which resulted in at least 45 million stolen credit and debit card numbers from TJX's retail stores, stemmed from wardriving and weak wireless encryption keys [1]. These types of occurrences are leading toward the enforcement of various compliance standards, such as PCI DSS [3], the mandated security program created by Visa and MasterCard for their merchants and service providers to safeguard credit cardholder information.

To combat this new threat, security professionals have turned towards tools that attempt to discover, identify, and locate wireless transmitters. This can help them pinpoint rogue access points – wireless transmitters that act as a bridge between the

J.R. Goodall, G. Conti, and K.-L. Ma (Eds.): VizSec 2008, LNCS 5210, pp. 136–143, 2008.

wireless and wired networks – that are setup by attackers to sniff wireless traffic and hijack legitimate users' wireless communications. In other cases, wireless users inadvertently plug in access points without any security measures enabled, leaving them completely open to attack and misuse. Attackers can easily identify access points with weak or no encryption.

There are several commonly used free tools for wireless discovery, such as NetStumbler [4] and Kismet [5]. NetStumbler is an active wireless discovery tool for Windows. Kismet is a passive wireless sniffer for Linux and Unix; it is often used for wardriving, and can save GPS location-based data in addition to information related to each of the wireless transmitters it detects. Because it listens for all wireless communication passively, there are some kinds of traffic – such as access points that do not broadcast their name to the world, an increasingly common setting, which Kismet can capture.

Security professionals have some limited visual tools (e.g. GPSMAP, which is included with Kismet) for presenting the results of a single wardrive, but there are no widely adopted visual analysis tools for performing the analysis of many wireless discovery sessions. Without these tools, security professionals report difficulty in detecting changes in the wireless threats over time or geographic region.

Our prototype system, called MeerCAT (Mobile Cyber Asset Tracks), is designed to provide a visual analytic tool for analysis of wireless discovery data. It visualizes wireless transmitter locations, their security attributes, and the relationships among transmitters. We currently use Kismet as our data source, but intend on extending our prototype to visualize NetStumbler data as well.

Our goal is to support the analytic process of information security auditors, penetration testers, and network administrators after performing a wardrive or site survey. To do so, we have incorporated both information and geographic visualizations into a visual analytics system that security practitioners can use for post hoc, interactive analysis of wireless discovery data.

2 Related Work

Hurley [6] identifies and describes two of the most popular tools for visualizing wireless discovery results, GPSMAP and StumbVerter. GPSMAP provides various features, including travel path and interpolated signal ranges. GPSMAP is a command line tool and does not provide interactive analysis of the data collected.

StumbVerter [7] is a wireless visualization tool that relies on Microsoft's MapPoint mapping library. It plots wireless transmitters on a street map using size and color to denote signal strength and encryption mode. It lacks signal range mapping and it does not appear to provide imagery data.

Other popular wireless visualization tools include KNSGEM [8] and Kismet Earth [9], which convert discovery log files into 3D plots in Google Earth. One of the limitations of this approach is that the visualization is constrained to the Google Earth framework; it cannot be embedded in a custom application that adds additional visual displays.

A collaborative effort led by University of Kansas, performed a three-year study tracking statistics on wireless market's growth, vendor saturation, and security attributes [11]. Using ESRI's ArcGIS and gathered data, they generated various wireless visualization

maps, which show signal propagation of an access point and its potential security risks. Dartmouth College has also performed extensive research on the various existing wireless visualization and also presented techniques for generating wireless visualization coverage map [12].

Lacking in existing wireless security visualizations is the ability to perform comparisons over time, visual interactivity (most were static images), and difficulty in accessing background imagery. Most importantly, these tools lack visual analytic capabilities for parsing through the copious amount of data to find the most interesting information.

3 User Requirements

We interviewed several potential commercial and military users to determine the requirements for a wireless visualization system. This group included information security auditors, penetration testers, and network administrators. This section highlights the results of these interviews.

Although wardriving does not provide the fidelity of a Wireless Intrusion Detection System (WIDS), many users find it is the best solution for performing ad hoc security audits and for covering large areas, such as military bases or college campuses, due to the low cost and ease of setup. A WIDS normally requires a large number of costly sensors to be installed throughout the monitoring area to attain full coverage.

Many of the users we met with perform periodic security audits, from daily to quarterly. During these audits they are looking for rogue, misconfigured, or suspicious devices, such as probing transmitters or ad hoc networks. *Probe networks* represent clients trying to join a network; this could also indicate an active probe performing reconnaissance of the wireless area. *Ad hoc networks* are peer-to-peer networks in which computers can discover and communicate without involving a central access point; there are inherent security issues with ad hoc networks [14].

The first step for many users to assess their current wireless security state is to perform a baseline wireless discovery. During this process, devices are compared with a list of known devices and configurations. Many organizations set security configuration policies in which devices are checked against, such as encryption requirements or SSID naming convention.

Unknown devices are analyzed to determine if they are a friendly neighbor or a rogue device. These rogue devices are further analyzed, normally starting with determining the most likely location. The location area of uncertainty will be needed if in-depth network monitoring is to be done. Having easily accessible detailed geographic imagery was also deemed important for the users we interviewed. This is required when trying to pinpoint the location of devices for remediation.

For known devices, analysts want to understand the signal leakage associated with the transmitters. Ideally, analysts would like the network range not to protrude beyond their building or campus perimeter, therefore reducing their security risk. Analysts also look for overlapping channels from neighboring devices, which may interfere with the availability and reliability of the networks.

When performing follow-up wardrives, analysts frequently performed the arduous task of manually comparing device configurations against their baseline data. Analysts currently have no tools to visually analyze the data collected, especially when it comes to comparing changes over time. Having the ability to quickly filter and group discovery data was also valued, yet lacking in existing tools.

A driving force to these security audits is the various compliance standards being mandated by government (DoD Directive Number 8100.2) [15], healthcare (HIPAA) [16], retailers (PCI DSS), and various other markets. To accommodate these new requirements, reporting is becoming an important requirement in wireless auditing, not just for compliance reporting, but also as a way to report to management and collaborate with others.

We found that many users find great value in having a visualization to describe the current state of devices of interest to others. Having a simple picture makes the intricacies of wireless network security easy to describe to less technical savvy people. These reports are general desired in both texture and visual representation and in various formats, including PDF, PowerPoint, Word, and e-mail.

As we iteratively design and implement our system, we continue to work with our identified user groups to elicit ongoing feedback that is incorporated in future iterations.

4 Coordinated Views for Wireless Security Analysis

The primary visualization in MeerCAT is the two dimensional geographic visualization as shown in Fig. 1. The background imagery is provided by ESRI's ArcGIS Online repository [17], which provides 1 meter or better aerial imagery for the contiguous United States and satellite imagery for the world at 500-meter and 15-meter resolutions, as well as detailed street map data.

This screenshot shows the 11 devices that were detected during a wardrive. The device icon shows whether it is an access point or a client computer. Although color is configurable, in this case it is used to indicate classification of devices: blue for trusted, red for rogue or probe, purple for friendly, and orange for misconfigured. Encrypted devices show a lock symbol and the level of encryption is shown on the icon itself, either WPA (strong encryption) or WEP (weak encryption).

Some interesting items can be quickly spotted looking at the 2D geographic view. We can see many trusted assets (in blue), one ad hoc network (two computers side-by-side), one probing client (red laptop), and one rogue access point (red). The misconfigured device in orange with an SSID of "linksys" is indicating that a known device was found to be in a configuration other than what was expected. In this case the security policy states this device should have WPA encryption enabled, but the device was detected with no encryption. This device can be annotated and flagged as something to watch during follow-up wireless surveys.

MeerCAT contains multiple views as shown in Fig. 2. These views are linked together with the same data to provide an interactive visual analytic environment; highlighting or filtering in one view is reflected in the others. The following highlights each of these views:

- *Device Tree* (Fig. 2a): A hierarchy of the detection runs (an individual wardrive) and the wireless transmitters and clients discovered during each run.

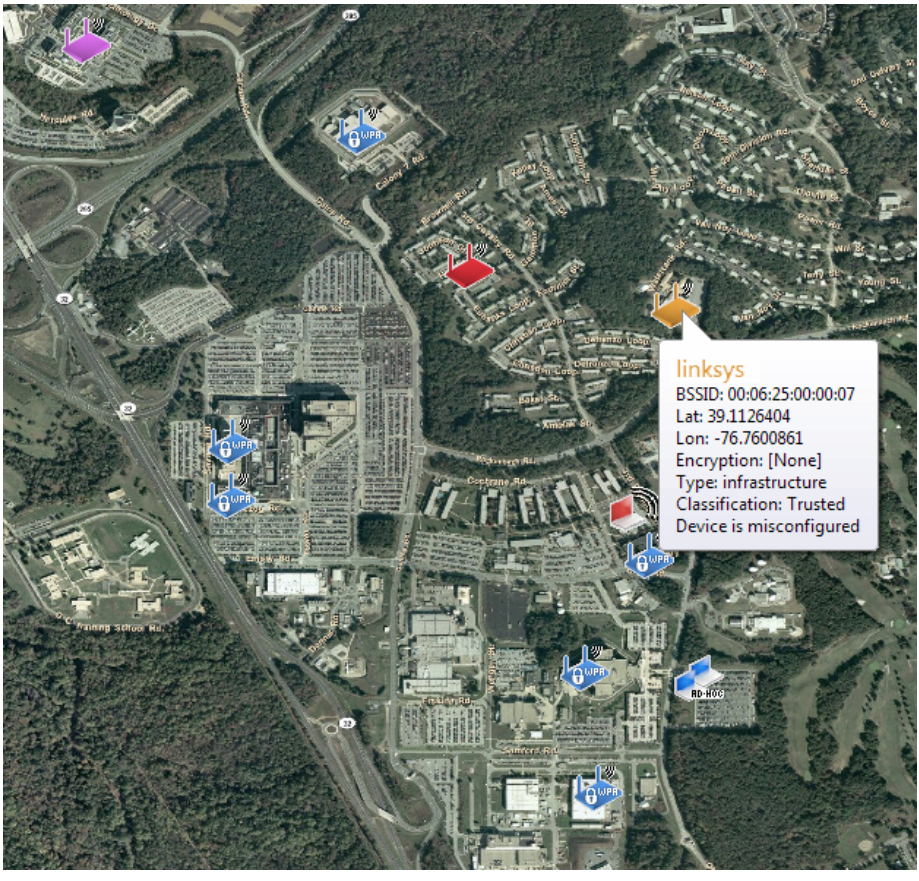

Fig. 1. 2D geographic visualization

Devices can be sorted, filtered, and grouped in various ways to help analyst quickly find the information they are looking for.

- *Geographic Visualizations* (Fig. 2b, c): Two and three-dimensional geographic fly-through visualizations showing satellite imagery locating the discovered wireless transmitters. These views allow for displaying tooltips, popup captions, signal ranges, drive path, and attached clients.
- *Device Visualization* (Fig. 2d): A tree visualization organizing the discovered wireless transmitters according to their type, encryption, and connected clients, colored according to the relative number of packets collected in that branch of the tree.
- *Network Visualization* (Fig. 2e): A graph visualization showing the discovered access points and clients that are connected to them. This view uses small multiples [18] to show a given network's change over time as shown. In the figure, the same device is shown in four different wardrives (showed by the dates under the device name, linksys); this device changed between wireless surveys, from unencrypted (red without lock) to encrypted (blue with lock).

This view can also be useful for quickly identifying networks with many clients connected to it.

- *Channel Visualization* (Fig. 2f): A histogram showing selected transmitters channel distribution. This provides a color legend when using geographic range displays for analyzing signal propagation.
- *Detail Tables* (Fig. 2g): A tabular display showing the details of a selected wireless transmitter and clients, allowing for sorting on columns of interest.

One of the use cases we have designed for is the need to see changes over time. When performing follow-up detection runs, analysts can use MeerCAT's various features to perform this type of temporal analysis. These include the ability to filter the device list to only show items that have changed one or more attributes, such as encryption, SSID, channel, type, or if the location moved a certain number of feet. The table view allows analysts to iterate through an individual device's history, causing the other views to update accordingly. The small multiples network visualization can quickly show how networks evolve and change between wardrives.

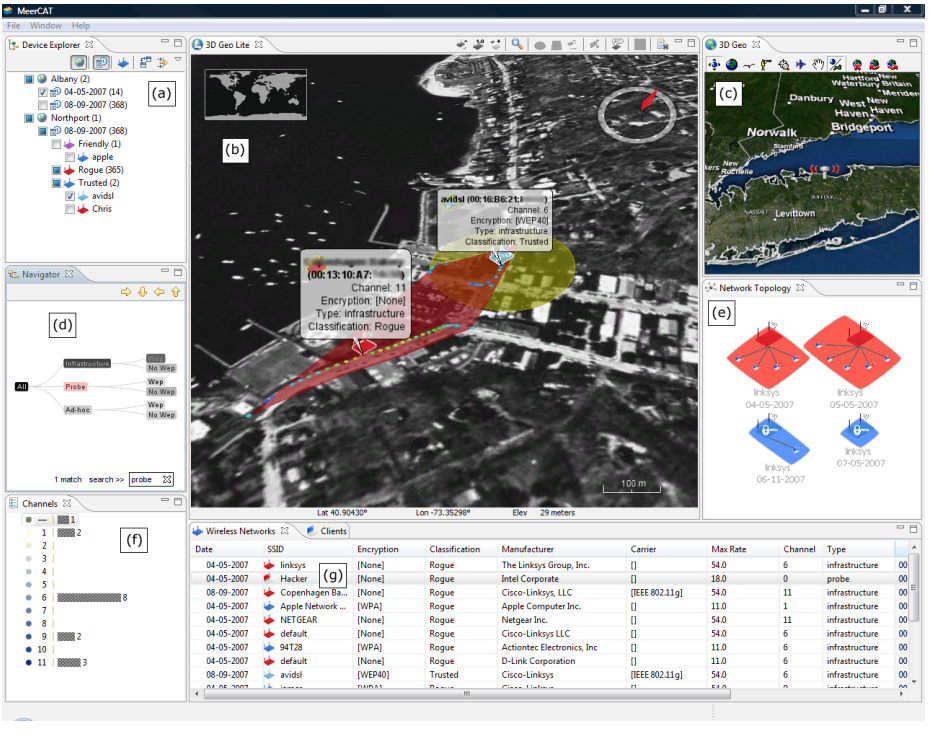

Fig. 2. MeerCAT wireless cyber asset discovery visualization prototype. (a) Device Tree list of detected devices; (b, c) Geographic Visualizations showing location of devices; (d) Device Visualization showing transmitters by type and encryption; (e) Network Visualization showing connections between transmitters; (f) Channel Visualization showing channel distributions; and (g) Details Table showing details of networks and clients.

5 Implementation

MeerCAT is implemented in Java using the Eclipse Rich Client Platform (RCP) [19] and Standard Widget Toolkit (SWT) [20] to provide cross-platform support with a native look-and-feel. A cross-platform solution was required as the users we interviewed depended on both Windows and Linux for their data collection and analysis.

We are currently using ESRI's ArcGIS [21] and NASA's WorldWind [22] for geographic visualizations and the open-source prefuse toolkit [23] for information visualizations. For data processing, we are currently using Oracle's TopLink Essentials [24] implementation of the Java Persistence API (JPA) and H2 [25] as our embedded database repository.

6 Conclusion and Future Work

The ability to discover, identify, and locate wireless transmitters is an increasingly crucial aspect of information security. To facilitate the analysis of wireless discovery data, we have developed a prototype visual analytic tool to enable security practitioners to easily understand the attributes, relationships, and locations of wireless transmitters. This prototype is intended to demonstrate the utility of the system and garner early feedback from security practitioners.

We plan to incorporate visualizations that depict communication patterns, derived from packet capture data collected by network discovery tools. We will also plan on incorporating reporting features, the ability to display wired network topology in addition to wireless, and in-building (floor plan) visualizations. Finally, we will be bringing our prototype to security practitioners to solicit feedback that will be incorporated into successive iterations.

Acknowledgments

This research and development effort is supported by DARPA Strategic Technologies Office through a Small Business Innovative Research grant, under contract number W31P4Q-07-C-0022.

References

1. Hole, K., Dyrnes, E., Thorsheim, P.: Securing Wi-Fi Networks. Computer 38(7), 28–34 (2005)
2. Pereira, J.: Breaking The Code: How Credit-Card Data Went Out Wireless Door. Wall Street Journal, 5/4/07 Issue (2007)
3. PCI Security Standards Council (Accessed 1 June 2008), https://www.pcisecuritystandards.org
4. NetStumbler (Accessed 1 June 2008), http://www.netstumbler.com
5. Kismet (Accessed 1 June 2008), http://www.kismetwireless.net
6. Hurley, C., Thornton, F., Rogers, R., Connelly, D., Baker, B.: WarDriving & Wireless Penetration Testing, pp. 219–246. Syngress Publishing, Inc. (2007)

7. StumbVerter (Accessed 1 June 2008), http://www.sonar-security.com/sv.html
8. KNSGEM (Accessed 1 June 2008), http://www.rjpi.com/knsgem.htm
9. Kismet Earth (Accessed 1 June 2008), http://www.niquille.com/kismet-earth
10. Bittau, A.: WiFi Exposed, Crossroads, vol. 11(1), p. 3. ACM Press, New York (2004)
11. Wireless Network Visualization Project (Accessed 1 June 2008), http://www.ittc.ku.edu/wlan
12. Lentz, C.: 802.11b Wireless Network Visualization and Radiowave Propagation Modeling, Dartmouth College Technical Report TR2003-451 (2003)
13. Connelly, C., Liu, Y., Bulwinkle, D., Miller, A., Bobbitt, I.: A Toolkit for Automatically Constructing Outdoor Radio Maps. In: International Conference on Information Technology: Coding and Computing (ITCC 2005), vol. II, pp. 248–253 (2005)
14. Zhou, L., Zygmunt, H.: Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security. Cornell University, Ithaca (1999)
15. Department of Defense Directive Number 8100.2 (Accessed 1 June 2008), http://www.dtic.mil/dticasd/sbir/sbir041/srch/n076.pdf
16. HIPAA Security Standard (Accessed 1 June 2008), http://www.cms.hhs.gov/SecurityStandard
17. ArcGIS Online (Accessed 1 June 2008), http://www.esri.com/software/arcgis/arcgisonline
18. Tufte, E.: Envisioning Information, pp. 67–79. Graphics Press (1990)
19. Eclipse Rich Client Platform (Accessed 1 June 2008), http://eclipse.org/rcp
20. The Standard Widget Toolkit (SWT) (Accessed 1 June 2008), http://eclipse.org/swt
21. ArcGIS (Accessed 1 June 2008), http://www.esri.com/software/arcgis
22. NASA World Wind (Accessed 1 June 2008), http://worldwind.arc.nasa.gov
23. Heer, J., Card, S.K., Landay, J.A.: Prefuse: A Toolkit For Interactive Information Visualization. In: ACM Conference on Human Factors in Computing Systems (CHI), pp. 421–430. ACM Press, New York (2005)
24. Oracle TopLink Essentials JPA (Accessed 1 June 2008), http://www.oracle.com/technology/products/ias/toplink/jpa/index.html
25. H2 Database Engine (Accessed 1 June 2008), http://www.h2database.com