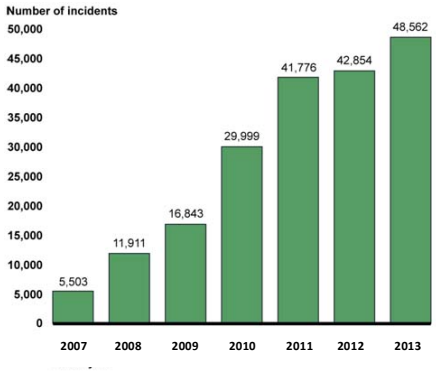
Location-Based Detection and Control

Eliminating Mobile Device Security Threats in Government Facilities.

Technical Brief

SENGEX
INGENUITY PRODUCING QUALITY INNOVATION
www.sengex.com

Government data breaches and cyber-attack incidents are increasingly prevalent. Unauthorized access to systems supporting critical infrastructure and government information systems are evolving and growing. These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives.



Over the past 6 years, the number of cyber incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (US-CERT) has increased from 5,503 in fiscal year 2007 to 48,562 in fiscal year 2013, an increase of 782 percent (see figure on right). In addition, reports of cyber incidents affecting national security, intellectual property, and individuals have been widespread, with reported incidents involving data loss or theft, economic loss, computer intrusions, and privacy breaches.

The capabilities of cellphones, smartphones and handheld wireless devices have made mobile wireless a "source" to cyber threats and have drastically altered how government entities implement policies to protect sensitive information and corporate intellectual property within their facilities. Today's mobile devices ability to rapidly perform large data transfers via 3G, 4G, LTE, and 5G technologies raises the stakes of how much data (and by definition) damage can be done quickly by wireless devices. The more time it takes to find a perpetrator, the more information they can compromise. The posting of signs that identify a facility as "No Wireless Allowed" location is not a strong enough deterrent from wireless threats that include:

- Devices are not using traditional vulnerability and compliance checks.
- Increased threat surfaces with users having two or more devices.
- Consumers are mixing personnel data with corporate/agency data.
- Mobile devices operate beyond agency boundaries, increasing their exposure to malware.
- The number of malicious apps and malware are on the rise.
- Hackers will find vulnerabilities.
- As the technology continues to evolve, so does the risk.

Unintentional and Intentional threats from mobile devices:

Wireless threats fall into two categories that include intentional and unintentional threats.

An intentional threat is categorized as a threat where someone plans to use their wireless device in a malicious cyber-attack manner to access, capture, copy, and steal government sensitive material. Regardless if this is an employee or visitor, or the motive for the action, wireless device's ability to take pictures, connect to internal networks, and communicate to external networks makes it a powerful tool for conducting malicious activities and an intentional threat will obviously ignore posted policies, and find ways to circumvent "entry-based" detection systems.

An example of the intentional threat devices is the Pineapple Mark V wireless attack platform that creates the illusion that it is an available access point with commonly used SSID like Starbucks or Marriott then connects to the device. Once connected the device is ready for hacking. Not only is it able to capture unsuspecting wireless clients, it can also mimic the address a known SSID at a facility and execute a de-authentication "deauth" attack by disconnecting the end user from their legitimate access point then reconnecting them to the Pineapple.

An unintentional threat consists of a threat where a wireless device enters a facility unknown to its owner that malicious code has been placed on the device. Toward the end of 2013, the U.S. government granted security approval for agencies to introduce bring-your-own-device (BYOD) policies, which allows their employees to use their smartphones and tablets at work. However, with so many devices within federal buildings and accessing networks means many new risks to their security. Smartphones are vulnerable to malware and, in particular, adware that tracks online behavior and harvests personal data. These vulnerabilities can then move to the wireless networks connected to the device.

As example, an unintentional threat may be an agency employee that has a Malware/adware on their smartphone without his/her knowledge. The malware could make the device act as an access point, or establish an adhoc connection to a network/device outside the facility perimeter, thus exposing a security gap without the user or government security and IT personnel even knowing about the gap. Without the awareness and control of all devices within the perimeter of a facility, there can be a significant threat to the security and integrity of the data. In either case, both introduce the opportunity for data breaches that can result in loss of sensitive material, intellectual property and increase the risk to national security. To combat these wireless threats, agencies need to implement solutions that address their policies needs as they pertain to the allowance of wireless devices within their facilities. In locations where “no wireless allowed” policy are established, the focus needs to be on solutions that can accurately and cost effectively detect mobile devices, regardless of intentional or unintentional attacks.

For agencies that participate in an employee/visitor owned device allowance, the security requirements become compounded where detection is not enough, and security practices need to include a “control” element that can work in conjunction with “detection” to create a complete wireless threat management ecosystem. The following sections will examine the needs for **detection** and **control** separately, and concludes with how a combined implementation provides for a homogeneous solution that allows agencies to establish an end-to-end wireless threat management policy.

“No Wireless Allowed”, Detection Requirements

Solutions for the detection of intentional and the unintentional threats from wireless devices within a restricted/controlled environment fall into three categories’ consisting of Entryway Scanners, Handheld Scanners/Wands, and Centralized Wireless Detection Systems. While each can provide organizations with some level of confidence in the discovery of unauthorized wireless devices within their facilities, the limitations of some of these solutions can result in undetected threats.

Entryway scanners:

The use of entryway scanners has been considered an adequate solution for mobile device discovery with the assumption that the detection at entry points of a facility will eliminate the risk of these devices entering restricted areas. However, powering off devices, or temporarily removing the battery can make them undetectable by the scanners. In addition, the size and construction of today’s mobile devices has also been proven to allow them to remain undetectable by many scanners.

A device circumventing an entry-based solution becomes invisible to the organization. Once past the facility access point, it can then be reactivated, and used within restricted spaces without any knowledge

of its location and usage, thus introducing a significant risk to the confidential data that an organization might have.

In some cases, an organization may allow visitors and employees to bring their wireless devices into a facility, but restrict their use to areas away from Sensitive Compartmented Information Facility (SCIF), at which point entry-based solutions are rendered useless.

Risk Level	Comment
Medium High to High	Easily defeated by the intentional threats

Handheld scanners/wands:

The practice of Technical Surveillance Counter Measures (TSCM) sweeps is a common exercise as a means to detect unauthorized devices. These may consist of the use of highly sophisticated and expensive handheld device operated by specially trained personnel, to the inexpensive handheld scanner solutions that have become popular on the web, but these solutions possess similar limitations as entry-based detection as it is only effective if the violating mobile device is within the scanners operating range. A further limitation to handheld detection is the need for a constant and time consuming practice to physically visit and scan all areas of 'concern' in the facility for threats. This results in a "hit or miss" scenario where an active unauthorized device could be in an area not currently under a TSCM sweep. The equipment cost and resources allocation of handheld solutions to produce "departmental" detection coverage makes this option the least efficient in wireless threat mitigation. Also handheld scanners are easily defeated by the intentional threats.

Risk Level	Comment
High to Very High	Easily defeated by the intentional threats

Centralized Wireless Detection Systems:

Where entry-based and handheld solutions focus on the detection of devices in a small targeted area, Centralized Wireless Detection Systems (CWDS) provide "location-aware" detection that can be implemented across a complete facility or multi-building campus to provide security personnel a centralized system to monitor, track, and be alerted of unauthorized wireless activity across the areas of concern or coverage.

Available solutions for CWDS vary that can include "detection" capabilities within wireless networking equipment. Depending on the solution provider, the level of accuracy can be limited to only telling users that there is a device in a certain perimeter. These types of solutions can be a challenge in the discovery of the violation when used in large facilities with a large amount of segmented areas such as cubical farms. In addition many available solutions only provide solutions for WiFi or cellular detection, thus requiring users to install and manage two systems for complete "wireless" threat management.

An efficient CWDS can not only detect rogue devices, but can also accurately pin-point their location, identify the device type (cell or WiFi), provide details associated with the device such as provide MAC address, SSIDs and association states of 802.11 WLAN devices, and track their movements on a graphical floor plan display. This enables personnel to immediately locate the violation and rapidly take measures to remove the threat.

Unlike handheld scanners, CWDS intuitive graphical interfaces eliminate the need for specialized trained users. A single PSO can monitor multi-campus environment for unauthorized wireless activity.

Options available for CWDS systems include both “fixed” installs where the system can be integrated into the organizations IT network and other security systems such as video surveillance, and physical access control systems, as well as portable systems that can be deployed and redeployed rapidly on an on an as-need basis.

In review of available CWDS solutions, ZoneDefense® from AirPatrol® meets agencies requirement for wireless detection in its ability to detect any mobile device in any government location, track its location, check for corporate policy compliance and provide immediate enforcement in accordance with our wireless security policy.

ZoneDefense continuously monitors for wireless devices through a network of fixed or portable RF sensors that detect and locate cellular and Wi-Fi endpoints. The sensors locate cell and smart phones prior to or during an active call, and can simultaneously detect all 802.11 or Wi-Fi activity. The ZoneDefense central console surveys movements and activities of these devices, sending alerts in real time while tracking those devices on a floor plan view.

Risk Level	Comment
Low	Location-based detection of both intentional and unintentional threats

Control Requirements

Government agencies that allow wireless devices to enter their facilities are seeing the value of Mobile Device Management (MDM) solutions that can bring to their security practices in the ability to secure, monitor, manage and support mobile devices – typically involving remote distribution of applications, data and configuration settings for all types of mobile devices such as smartphones, tablets and notebook computers.

Mobile device management also enables agencies to manage mobile apps that are on each “allowed” device, deploy, manage, block or remove rogue apps on individual or groups of devices, thus reducing the risk of dangerous mobile malware accessing government sensitive information.

For example, an agency may allow employees to enter a facility with their mobile devices, but invoke a policy on the unit that disables the camera and cellular-based communications as a means to ensure information cannot be collected and leave the facility (either by transmission or hand-carried).

While MDM does bring a “control” element to an agencies wireless threat management and mitigation practices, it does suffer limitations when an agency’s locations have areas within their facilities that require different levels of protection from wireless cyber threats. This introduces a need for a more granular level of control to standard MDM solutions to include “location-based control”

MDM deployment consists of an application/agent that is placed on the mobile devices that allows the MDM administrator to establish policies on the devices. The policies can be specific to the users capabilities to access/use applications/capabilities of the device (i.e. email, camera, web browser, etc), or force the user to only be able to see a menu of applications/capabilities that the MDM administrator allows them to use.

The implementation of a MDM solution is typically invoked on a global basis where all employees must have the MDM application on the device, and the policy(s) defined are pushed to all devices where they run on a fulltime basis, or are time sensitive to being active or not.

The "on or off" nature of MDM is a good control solution in situations where employees are provided *agency-issued* devices, however the allowance of personal owned devices within a secure facility adds complexity to MDM management as the users are going to want to have full access to their devices when outside the locations.

While some MDM's do provide for a "GPS" capability that can allow for an MDM administrator to invoke/remove policies based on users location, the accuracy, and potential of loss of GPS positioning once a user is within a facility introduces risk of the device being an uncontrolled and invisible threat.

This problem is compounded in locations where an agency might allow employees/visitors enter with their devices, but there are areas within the facility such as SCIF where no wireless devices are allowed.

Detection and Control Working in Harmony

Solutions for CWDS that provide "location-based" detection discussed earlier addresses the need for "no wireless allowed" locations, but can also provide valuable protection and enhanced security to locations that do allow employee/visitor owned devices into their facilities.

Through a CWDS's capability to integrate with industry standard MDM solutions, government agencies can achieve "location-based control" that allows them to not only detect unknown devices, but also detect and control known devices based on their location within a facility.

For example, employees may be allowed to have their phones in unclassified office areas, however if he/she enter a classified meeting room, a dynamic policy can be invoked that disables the users voice recorder and camera. Further, if the individual brings the device into a SCIF (intentionally or unintentionally), detection of the devices location by the CWDS would invoke a policy that completely disables the device.

An added value to location-based control is the ability to identify and detect known devices in addition to unknown devices. This is a process of registering a device in the CWDS system as being known to have the MDM profile that makes it a known device, at which point its icon display on the CWDS system identifies it as being known. The detection of a device that is not registered would then be identified as unknown or "rogue" that might have entered the facility to perform intentional or unintentional malicious intent. This enables personnel to immediately locate the violation and rapidly take measures to remove any threats.

Location-Based Control Features and Benefits:

- *Accurately detect and locate unknown/unregistered devices*
- *Dynamically apply/remove policies based on location*
- *Enable Mobile Enterprise Management*
- *Integration with other security systems*
- *Enable agency-owned/employee-owned device entry in government facilities*
- *Eliminate/minimize risk of malware/adware risks*
- *Use of intentional and unintentional data breach threats*

As a mobile device security platform, AirPatrol's ZoneDefense also offers connectors that allow it to integrate with mobile device management, application management, network security and policy

administration systems from leading firms such as MobileIron, AirWatch, Good, Appthority, ArcSight, BoxTone, Fiberlink, FireTide, McAfee, and many others. Connected to the ZoneDefense platform these 3rd party tools are enhanced with the ability to dynamically set and change policies, modify security and manage devices based on location as well as device.

Summary

Government agencies have begun to seek out best practices for mobile computing security, including developing a solid risk management framework for the use of mobile devices in government (which could be agency-issued, employee owned, or a combination of both). The convergence of mobile device management and mobile enterprise management software has enabled agencies into the realization of attaining full mobile enterprise management, but this cannot come with added risks to security.

When weighing the benefits of mobile enterprise management against risk of data breach government leaders remain leery of full commitment. Not only do operators have concerns of the potential loss of sensitive information as seen in the recent "Snowden" incident, but as seen in the corporate world, leaders are also being held personally accountable for data loss as in the recent example of the Target CEO.

Beyond abilities to detect unauthorized mobile devices within an agency facility, the use of mobile enterprise management solutions must include capabilities to ensure that "any" mobile device (under agency MDM control) be centrally accounted for within all the agencies restricted use locations/areas. Violations to agency policies for the use of mobile device must be identified and addressed in real-time, as conventional security means may be too late by the time the violation is discovered.

Whether executed via intentional or unintentional methods, threats to national security from wireless-based risks can result in significant loss of confidential information and possibly human life.

For agencies that have "no wireless allowed" policies, they need to closely examine the detection options available (and their associated limitations) to ensure they are not sacrificing accuracy for cost (where in some cases, costs may be higher when you factor in time and resources needed to manage the solution).

For agencies that allow employee/visitor owned devices, they must look beyond the basic "control" capabilities that MDM brings, to include the need for "location-based control" through MDM/CWDS integration that further protects the agency from devices within the 4 walls from intentional or unintentional threats.

About the Author:

Dave Boulos is Director of Technical Services and Marketing for Sengex. Dave has 25 years Product Management and Product Marketing experience in data networking, data security, IT infrastructure, and telecommunications industries. Dave holds a Bachelor's Degree in Electrical Engineering, along with Associate's Degrees in Business Management, Data Communications, and Telecommunications from Northeastern University.