

# Computing Without Wires (Or Even a Net): The Pitfalls, Potentials, and Practicality of Wireless Networking

## *Panel Moderator:*

Timothy J. Havighurst, National Security Agency, USA

## *Panelists:*

Anna Entrichel, Project Engineer, National Security Agency, USA  
James Bergman, Harris Government Communications Systems Division, USA  
Jason Willis, Project Engineer, National Security Agency, USA  
Herb Little, Research In Motion, Canada

## **Panel Theme**

Wireless Network Components (Wireless Local Area Networks, Bluetooth Radios, and Personal Digital Assistants) are presenting unparalleled convenience, potential gains in productivity, and huge security risks. Misunderstanding of capabilities, overstatement of security properties, and a fundamental lack of valid policies, can make for a very large risk in the workplace. Too often, "Management by Inflight Magazine" has led customers to embrace technologies that are not properly tested or even compatible with current or future system architectures or policies.

Customers are often forced, by their upper management, to shoehorn system components or technologies without benefit of a lot of security analysis or even the knowledge of the devices prior to their introduction to the network. Built in capabilities of network components such as Bluetooth radios, and wireless LANs will be seen as not only improvements in communications, but potential holes, backdoors, and points of entry to otherwise secure networks.

## **Panelists and Their Issues**

### **Anna Entrichel**

There are many potential problems with Commercial Off the Shelf Wireless LANs above and beyond the inherent loss of information due to the broadcast nature of the network radio card. We have been working for nearly 2 years to examine the potential vulnerabilities in WLANs that may result in a loss of information. Encryption weaknesses, MAC controls, network access, jamming,

and inter-brand interoperability have all been seen as weaknesses in this technology. Some of the areas have fixes, and some simply have precautions, but each should be known by the system administrator prior to purchase and set-up of a wireless network.

### **James Bergman**

Keeping in mind that there are customers that absolutely require SECRET level protection for their mobile data, what can be done to ensure that the WLAN is protected. Encryption, using the proper algorithms, can give the WLAN a great deal of protection against traffic analysis, spoofing, indiscrete network access, and confidentiality weaknesses. Incorporation at the network level gives the system a flexible and secure basis of protection for the WLAN user and the incorporation of PKI can give end-to-end protection of data, even over wired-to-wireless network connections.

### **Jason Willis**

Policies that protect systems from external threats are only part of the answer. The introduction of potential vulnerabilities that can be introduced by small, handheld devices (e.g., PDAs like PalmPilots, Blackberries, and other Personal Electronic Devices) are much larger than the previous threats of cellular phones and removable media, because they combine the capabilities of both. The use of these devices, even in unclassified areas, present such a potential loss of data, from both inside and outside attackers, that companies are being forced to either ban or ignore them. COTS systems that have the capability to transmit both short and long distances, interface with systems both physically and remotely, and even in spite of standard protection measures, present a plethora of vulnerabilities. Exploration of several policy

statements, and the (still) potential risks will be highlighted, and explained.

### **Herb Little**

Research In Motion (RIM) has been the only provider of constantly connected / constantly secure communications for the average user on the go. Providing additional security for a customer set that finds even FIPS 140-1 level 1 certification too low can be a real challenge for a commercial provider. Additional layers of protection, additional assets, and unique architecture requirements can make even minor modifications to COTS equipment send ripples through the entire product line. Balancing the security and marketing departments' expectations, and meeting the needs of the customer today and tomorrow can be very difficult. RIM has worked with the Government to change design criteria and process to meet these goals, and has begun their learning curve in the area of system security. Their lessons learned so far, and their expectations and applications towards the commercial market w.