



## Wireless Security: “The Best is yet to come!”

---

When reviewing the advances in technology, and how it empowers us to be more productive and accessible, there are some truths that are revealed. Wireless technology has stemmed from the need of portability and accessibility, at the expense of security. At first, it was accepted that this technology had limits, and if we were confined within the boundaries of the technology, we were just fine, however, as technology matured, so did the threats against them. For instance, we had seen advances in tools to locate unprotected access points, techniques to circumvent basic security measures, and even learned of employees who used “social engineering” to expand and extend the boundaries to areas left untested.

Today, wireless technology has advanced in addressing security concerns, not by choice, but by necessity to conform to management requirements, feature needs, compliance standards, to comply with policies, and to address security audits and auditor requirements. As this may be acceptable for today’s standards, it begs the question of “What will the future bring for wireless security?”, or more accurately, “What will the requirements be for a technology that traverses physical boundaries, is difficult to detect, and can be installed and maintained in obscure places on my enterprise?”. These are my predictions for wireless, as tire manufacturers state, “mileage may vary based on performance, and other considerations”.

### **Wireless Prediction 1: Build relevance and better enterprise management**

Relevant information can come in many different forms, however, it is important to realize that in the context of wireless security, it would have to be in understanding “what” is happening, “who” is trying to access my network, and “what is my response” to that event. Forensics are starting to appear with some professional grade wireless access devices, however, we must go deeper than that for this technology to measure up to management and compliance requirements.

Relevance is the ability to provide me pertinent information on an event, and with respect to compliance considerations, what is the appropriate response, and has it been executed successfully. As you may deduce, there has to be better reporting - relevant reporting, to provide answers to some of these questions, not because it is “nice” to have, but because it is mandated through either self regulation, or a governing body.

The wireless management system should provide more relevance and mature in the management area to provide enterprise caliber reporting, policy enforcement, and most importantly, providing actionable event coordination based on corporate policy and procedures. Event correlation needs to aggregate and collaborate with network systems to provide seamless prevention. It is no surprise on the need for manageability, but there is another facet with sometimes gets minimized, but has bearing with respect to relevance – compliance.

Compliance is a strong driver to enforce stronger security and show auditors that you a) understand your environment b) you can manage the changes in that environment, and c) demonstrate that the integrity of your environment has not been compromised throughout the

process of getting to a compliant state. Wireless security has yet to address this in its entirety to the satisfaction of auditors and governing bodies. Why?

First, wireless technology is difficult to confine in an area, and *theoretically*, signals can travel in many directions, with infinite range. More on that point in prediction number two (2), however there is much to be said about confining, or even defining what to do with these signals that are easy to sample.

Another point of relevance which we should see advancement is in the area of collaborative and coordinated assessment and response. The collaborative assessment would be in the ability to dialog with assessment tools such as SIMS, Risk Management consoles, and other such systems where threat feeds can be passed on to the head-end tools and aggregate data, and prescribe the appropriate countermeasure configuration – in short, DO something based on the information provided. Wireless equipment have already made strides in talking with these system types, but they are immature in an enterprise coordinated management and response. I foresee that further advancement will be coming in a compressed timeframe which will be able to talk to other protective platforms without intervention of a SIM type system. This will aid in expediting intelligence and response in preventing something, or someone from breaching the enterprise proactively in an orchestrated manner.

## **Wireless Prediction 2: Incorporate better obfuscation technology**

A large concern for wireless technology is *who* is listening to my communication. When sitting at a hotel, or public location, do we have confidence in the knowledge that no one is listening to my communication, or even more importantly, is someone trying to actively talk to my laptop?

Wireless technology ought to obfuscate the conversation and packet stream sufficiently so that no one with a wireless sniffer could replay and ultimately decrypt the stream and get important information. Secondly, there ought to be easier, but more robust security features embedded into laptops whereby there is some intelligence inserted onto the systems. An interesting feature that ought to be introduced is some default firewall-ish feature which senses a hard wired connection, and disables the wireless card. This would potentially prevent a split tunnel scenario. Another feature would be a wireless sensing technology which would act like passive radar. It scans quietly for access points and systems, and if it does not detect your friendly access points, or approved ones, would go into a “standby mode” where it won’t broadcast or acknowledge itself to anyone. Lastly, I think that in the future, encrypted burst mode type traffic will help keep the laptop from chattering too much, and allow for others to interrogate it. The military uses similar technology on equipment for forward spotters for artillery, and it might be cost effective in a few years to incorporate into commercial systems.

## **Wireless Prediction 3: More Features, Better Security, Cheaper Prices**

Wireless technology, like all technology, will incorporate more features, better security and ultimately, more cost friendly to the enterprise. There are some features that soon wireless equipment will embrace Network Access Control (NAC) standards where you can be proactive at the access point regardless if it is a managed system or unmanaged system. This is something which could help remediate (through the NAC remediation steps) a system before it gains access to network resources. This should be the next logical step for wireless technology in mass, to provide a proactive protection in conjunction with traditional infrastructure components. Being able to properly enforce your policies and procedures would aid considerably in plugging up holes in traditional network architecture retrofitted with wireless technology.

An interesting, albeit fantasy wish list for wireless technology, would be merging wireless technology with network detection technology which would educate my users to understanding which network am I trying to access. If I was at a coffee establishment, and wanted to check my

email through their wireless network, could my detection technology provide me authenticated access points to connect to? Is there some certificate which can be checked stating that this was a legitimate system or is it an ad hoc spoofed connection?.

## **Summary**

As eluded to, these are my personal predictions, however, what I expect is that throughout the next year, and into first half of next year, is major wireless technology vendors will have to face facts that if their technology is to enter into the enterprise, they will have to mature quickly and employ serious safeguards and provide means of proving compliance not just in the enterprise, but when mobile devices are away. There are some manufacturers who are making serious strides in the security space for wireless, and I predict that this will be a catalyst for many changes this year in their product lines. Failure to address these requirements, those vendors will risk being acquired in the security manufacturer game by some company who understands the enterprise needs, or will face losing their customer over time.