



PODCAST

To listen to the entire interview, log on to www.FutureHealthcareUS.com



Security Sans Wires

DR. AMIT SINHA, Fellow and Chief Technologist of Motorola's Enterprise Wireless LAN, clarifies wireless security in today's healthcare environment

Future Healthcare What are some of the wireless security implications for HIPAA Compliance?

DR. AMIT SINHA HIPAA is a broad set of requirements, and within the requirements for patient data confidentiality and security, you can distill a few specifics that are applicable to wireless networks. Overall, they can be broken up into a few brackets. You have requirements around encrypting your wireless network so data in transit cannot be sniffed by unauthorized people. That typically means that you use wireless encryption standards such as WPA2, which are known to be robust compared to some of the legacy standards like WEP.

Closely tied to that is the ability to detect unauthorized wireless devices. So if you have a hospital network where doctors and nurses are plugging in their own unauthorized wireless access points, those should be detected and weeded out to make sure that someone does not leverage these unauthorized wireless networks to gain access to patient data. You also have to make sure that peer-to-peer wireless communications and things like accidental wireless associations are monitored and prevented.

HIPAA further requires that you have a security management process and certification where you have explicit policies for wireless usage that are scrutinized, and then periodic testing or assessments are performed to make sure that those policies are being followed.

There are also certain requirements around security configuration management. You should have documented configurations; they should be applied globally, so you should have a

centralized system to enforce configuration and validate that those desired configurations form a wireless network perspective.

Finally, as with every compliance document, you should have an incident response procedure. Should an event happen in the healthcare environment where perhaps a patient's medical records have been compromised, you need to be able to have systems in place from a wireless perspective to detect these events; an alarm if, for instance, someone tries to break into your wireless network, or if internal users are trying to abuse the wireless network in ways that are not compliant with your usage policies. In the event that there is an incident on the wireless network, you should be able to generate an alarm and then take appropriate action. For example, if someone plugs in an unauthorized or rogue wireless device you should be able to detect it, find out where the device is, remove it from the network and then do another scan to make sure everything is in order.

FH What are rogue wireless devices and why are they dangerous in healthcare environments?

AS If you look at wireless security in general, apart from the encryption requirements that traditionally are applicable to networks, the other area of security stems from these rogue wireless devices. If you have a healthcare environment where doctors, nurses and others who work in these facilities are bringing in their own wireless networks and connecting it to the healthcare network in an unauthorized fashion, they can lead to gaping holes from a network security perspective. If a doctor brings in his home wireless router and connects it to an open

Ethernet port in his office (because he likes Wi-Fi access within his work environment) that's not acceptable. These unauthorized wireless devices, also known as rogue wireless devices, connected to the environment can be leveraged by hackers who might be in the parking garage of the hospital to gain access to the internal networks that might have patient data that needs to be protected.

In general, a rogue wireless device is an unauthorized wireless device that is connected to the authorized wired network and, in turn, is exposing the authorized wired network to hackers who might be in the vicinity of the facility. These rogue wireless devices typically are access points and can be things like:

- Wi-Fi routers that you install at home
- Embedded Wi-Fi devices and printers
- Wi-Fi devices in laptops that have been enabled while connected to the wired network and
- Any wireless network that is offering access to the authorized wired infrastructure and wasn't meant to do so.

FH How can wireless intrusion prevention solutions help in healthcare environments?

AS Wireless intrusion prevention solutions (Wireless IPS) have specifically been designed to monitor environments from a wireless perspective. In the healthcare scenario, they can provide value in three areas: the wireless security bucket, the wireless compliance bucket and troubleshooting related benefits.

If you look at it from a wireless security perspective, a wireless IPS system, such as the Motorola AirDefense Enterprise System, can very effectively detect rogue wireless devices. In a hospital scenario, if you have authorized wireless devices deployed, the system can discover which devices are authorized. If someone plugs in an



unauthorized wireless device, the wireless IPS can effectively detect that and neutralize it over the air.

The important point here is to make sure that you're not neutralizing your neighbor's network. If you have many hospital facilities scattered over a large geographical area, you can imagine that these hospitals might be in areas with a lot of neighboring Wi-Fi traffic. Being able to pinpoint what is unauthorized and connected to your network and not something simply coexisting in the airspace and belonging to a neighboring business or home user is key to the rogue detection problem.

An accurate wireless IPS system like Motorola AirDefense Enterprise can classify these rogue devices and automatically terminate them. Wireless IPS can detect wireless attacks in real time, so if someone is in a neighboring facility trying to break into your wireless network, those attacks can be detected and appropriate alarms can be generated so that the system administrator is aware and can take action in real time.

Another feature that Motorola AirDefense Enterprise has is vulnerability assessments. The system can perform automated penetration tests against all the wireless networks within a healthcare facility and produce an automatic report validating the security mechanisms that are in place.

Closely tied to security is compliance. A solution like Motorola AirDefense Enterprise can generate HIPAA compliance reports, so when an assessor or an auditor shows up, you have these wireless compliance reports ready. These reports can be generated on demand, and we maintain a full forensic database that can be leveraged should an audit happen and further investigation is necessary. In short, we are maintaining a full-blown "DVR" or "motion picture" of your entire RF environment which is logging every device on a minute-by-minute basis.

Coupled with compliance is detection of

configuration issues. For instance, HIPAA requires you to maintain a certain level of encryption. This typically translates to WPA or WPA2. Being able to guarantee that across the healthcare facility — that you have all wireless networks configured correctly — is something that the wireless monitoring system can do effectively.

The third bucket is troubleshooting. You can think of wireless IPS systems as a large distributed monitoring system for Wi-Fi networks, and what they can do then is help you with troubleshooting or support issues. If a doctor is experiencing problems connecting to the wireless network, or a nurse is having specific issues with a wireless handset, inventory tracking, point of care or patient bedside application, instead of having to send people on-site to debug these issues, a wireless IPS system like AirDefense Enterprise can very effectively help support and resolve these issues from a remote help desk.

FH What can hospitals do to reduce wireless support costs?

AS One of the benefits of Motorola AirDefense Enterprise, which is an industry-leading wireless IPS solution, is its capability to perform remote troubleshooting. If you look at wireless networks, particularly wireless LAN, people obsess about the upfront capital expenditure, which is rapidly going down. However, they tend to forget about the ongoing support and management and maintenance costs. In fact, over a three-to-five year lifespan, sometimes the support costs can exceed the upfront capital expenditure.

It is very important to make sure that you have the right tools in place to keep support costs down. Using some of the remote troubleshooting capabilities of Motorola AirDefense Enterprise, one can really bring down the support costs for wireless LAN.

Let's say you have a large healthcare facility

with many hospitals scattered everywhere in different locations and doctors' offices. If you have wireless networks in these facilities, supporting those distributed networks is a daunting task. A doctor may call in and say a particular wireless tablet is not connecting or seems to have intermittent connections to the wireless network or a patient wireless bedside application seems to be crashing all the time. The ability to look into these wireless problems without having to send experts on-site can dramatically cut your support costs.

With Motorola AirDefense Enterprise, you can leverage these remote monitoring sensors to effectively replicate the problem at a centralized help desk. So you can run a network operation center in a central facility and your help desk personnel could be on the phone and actually looking at the problem from a wireless network perspective at that remote facility.

Further, we can crank it up a notch and convert this into a more proactive troubleshooting system, so in a large healthcare facility you can run an automatic troubleshooting scenario where every morning the entire wireless network is tested using these remote sensors. The sensors then become the end-user client stations and actively connect to the wireless network, perform a diagnostic check to make sure the wireless network is healthy, various applications are accessible via the wireless network and produce an automatic report and have that report ready for the head of operations. That way, you're detecting and avoiding problems before they start impacting your healthcare users.

FH How can I increase the reliability and reduce the downtime for clinical applications that rely on wireless?

AS The first thing you have to do when you're going



“IMPROVEMENTS CAN COME WITH THE REMOTE TROUBLESHOOTING THAT WIRELESS MONITORING/IPS SYSTEMS CAN PROVIDE, WHICH CAN REALLY IMPROVE WIRELESS NETWORK PERFORMANCE.”

to an all, wireless enterprise is to make sure you've done a good job of planning. If you just hook up a few wireless access points and assume that everything is going to work, that might be OK for browsing type applications, but as you start scaling and running mission-critical healthcare applications via wireless, you run into bottlenecks.

You have to make sure you properly plan your wireless deployment, make sure you've accounted for all the applications you're going to run and do a site survey. Motorola has tools like LANPlanner that can help you very accurately plan your wireless network, determine the exact locations where wireless access points need to be deployed for guaranteed coverage as well as optimized capacity. If you look at the Motorola wireless LAN, it is designed to be self-optimizing and self-healing. What that means is that once you've deployed these APs, they can automatically detect reliability issues.

For example, if one access point goes down, the neighboring access point can rescue the failed neighbor. Similarly, if you have issues with your wired networking, wireless LAN APs from Motorola can set up a peer-to-peer mesh wireless connection to route around the wired point of failure. The Motorola wireless LAN also features things like SmartRF, where it can automatically optimize what channels your wireless network should operate on, it can automatically optimize the power levels that APs should be set to operate on, it can minimize co-channel interference and minimize the effects of other non-Wi-Fi sources of interference, such as microwave ovens or cordless phones, that might be interfering with your wireless network. Having

a robust wireless LAN that can self-optimize and self-heal is essential.

Finally, you have to have 24x7 monitoring system. Once you've planned properly and deployed, you still need the ability to remotely troubleshoot issues when they arrive. You need to be able to produce performance reports and produce historical context that can help you debug complex problems. That's what a wireless intrusion prevention system supplies you on top of your wireless LAN infrastructure.

FH How can wireless monitoring help companies improve wireless network performance?

AS The problem with wireless is that it tends to be very transient so you can plan for the best network, you can have a very robust system, and you still may run into issues. For instance, you might have a microwave oven directly next to an access point and it might start killing that AP with the enormous amount of power that it's pushing out in the 2.4 GHz band. You might have issues around reduced coverage, maybe the facilities have been changed or you may have roaming issues where clients may be dropping calls, particularly if they are using voice over wireless LAN.

In order to be able to detect what the source of the problem is, you need a wireless monitoring solution. With Motorola AirDefense Enterprise, for instance, you can generate automatic performance reports. These will tell you exactly where the problem areas are, and they can help you quantify the ROI that you're getting from your wireless LAN. And

if there are issues around capacity — for instance, you plan for 20 users per access point and suddenly there are 30 users hanging on from one access point that can bring down the user experience for that particular section of the building. Similarly, the Motorola AirDefense Enterprise system maintains detailed forensic records; we have 300-plus statistics that we maintain for every wireless device in the monitored perimeter, and that provides a very rich historical context, and you sometimes need that to ensure you detect complex problems. In the microwave example, it's possible that the wireless network performance goes down around lunchtime when the microwave oven is being used the most. When a tech shows up on-site in the morning or afternoon, that problem may not be there. So by leveraging the historical data that Motorola AirDefense Enterprise provides, you will be able to see those intermittent interference issues and resolve them.

Finally, improvements can come with the remote troubleshooting that wireless monitoring/IPS systems can provide, which can really improve wireless network performance. At the end of the day, if the wireless network is going down frequently and it takes a long time to get it back up because experts have to be sent on-site, the ROI is dramatically reduced. Having a remote monitoring solution that can help you troubleshoot wireless issues from a centralized help desk perspective is definitely going to cut the time that it takes to fix issues — they are being resolved remotely and in real time to help maximize the ROI. **FH**



DR. AMIT SINHA, serves as Fellow & Chief Technologist of Motorola's Enterprise Wireless LAN division. He was the Chief Technology Officer of AirDefense prior to its acquisition by Motorola. Dr. Sinha specializes in wireless communications and security and has authored over 25 journal/conference papers, contributed chapters to three books, and is the inventor of 16 U.S. patents. Prior to AirDefense, he served as Chief Technologist at Engim, a multi-channel 802.11 chipset company he co-founded. He received his S.M. and Ph.D. degrees in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology and his B.Tech. degree in Electrical Engineering from the Indian Institute of Technology.

Motorola AirDefense Solutions

MAKING WIRELESS WORK FOR HEALTHCARE

Motorola AirDefense Solutions bring secure, 'always-on' mobility to the point of care and beyond. They help your wireless networks meet HIPAA requirements, keeping patient data safe and secure. They make your mobile devices and clinical applications work better, faster, and with less downtime. What does this mean for you? Your staff will be more productive and spend more time focusing on patients, not technology. It's just another way Motorola puts Enterprise Mobility in the palm of your hand. HELLOMOTO™

Experience Enterprise Mobility at motorola.com/healthcare

MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.
© Motorola, Inc. 2008. All rights reserved.

