Communicating With Sam

Wireless Integration: Assessing the Risks

Sam Johnston

Question:

Currently our company has a standards-based wireless barcode system to support inventory scanning to our AS/400. The system has been in place for several years and is 900MHz technology with a dedicated proprietary wireless network. Due to the deployment of new ERP applications, and the client interface that is required, we could better leverage our new applications if we migrate to more current technology based on 2.4GHz standards, which means the introduction of a wireless LAN (WLAN) within our campus. Additionally, we currently have 900MHz wireless Companion phones, which are end of life. Consequently, we are assessing building a single 2.4GHz network to support both new barcode scanners and new wireless IP phones, as well as other applications and devices such as PDAs. However, based on published reports and the information made available in the media, our management team is concerned about security. We are trying to assess whether the business benefits of the change will justify the security risk and capital cost of the project.

Answer:

Wireless Wi-Fi 2.4GHz networks (WLANs) present perhaps the largest conundrum in the technology landscape. On one hand, the media bombards us daily with news on the growth of wireless hot spots and can't miss productivity benefits associated with staying connected to the enterprise regardless of where we are. However, this positive spin on Wi-Fi technology is always offset by a new report from some research group indicating how vulnerable corporate networks are due to poor wireless security. While your overall concerns about wireless security are valid, it is important to understand whether the issue is rooted in an inherently flawed technology, or is more a product of poor deployment practices.

Before you make your final decision, it is important for you to know and understand the advances and capabilities of wireless security. Once you translate these capabilities into a final solution design and implementation plan you will be better equipped to decide if the security profile of the technology is within the risk range that your company deems to be acceptable.

Aside from security issues, a key business decision is to determine whether it makes sense to integrate your wireless infrastructure to support multiple applications via a single network, or to maintain your existing approach of a separate and dedicated network for the barcode system and the phones, making the decision to upgrade each independent of one another. Overall, we would typically recommend moving to a single network infrastructure for the benefit of reduced support costs and consolidation of maintenance, configuration and support. While you may want to keep the two decisions independent, you may not be able to. The bad news is that to upgrade either your existing phones or bar code scanners, you will need to build a 2.4Ghz network. The good news is that the current technology standards for both the phones and bar code scanners use open standards, rather than proprietary networks, and hence, whatever network you need for one will also support the other, provided adequate capacity is built.

The technology that you have currently deployed for both the phones and bar code scanners is 900MHz and will not conflict in signal with the commonly deployed WLAN standard of 802.11b using 2.4GHz. This means that depending on the ROI associated with each decision, it is technically possible to migrate only one of the devices (either the bar code scanners or the phones), while leaving a legacy system in place for the other. However, given that a migration of either means a new network, and both your phones and bar code scanners are essentially at end of life, there is a good chance that you will be able to justify the additional capital of replacing both by improving the overall ROI of the project.

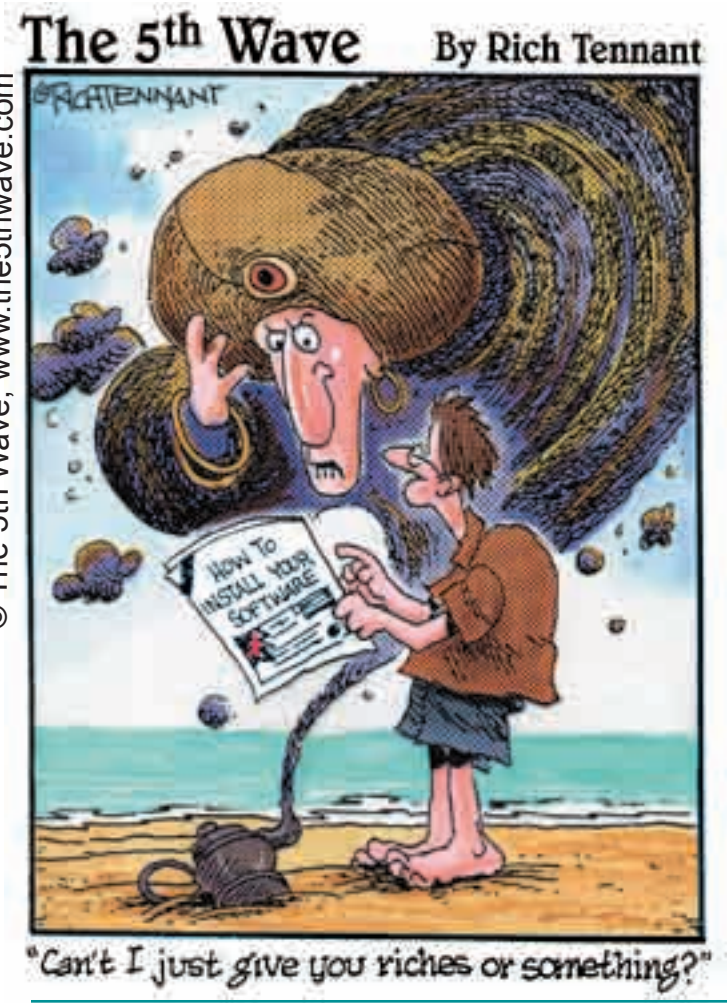
While technically the decisions can be kept independent, the ability to use a single network will likely make the two business decisions interdependent. Overall, the decision to replace either the wireless phones or bar codes scanners will be based upon the ROI associated with the cost of migration, which ultimately will be driven by the supported features associated with each device, and the potential to reduce the ongoing support costs by adopting more efficient new technology.

Assuming that you can justify replacing at least one or both of the devices, you will quickly be heading down the path of implementing a 2.4Ghz WLAN. An important step in the design process will be to review the security implications and the layers of security available for the WLAN.

While the technology can assist in providing a secure environment, it is also important to understand that security of any nature is always rooted in common sense prevention decisions. As a starting point, you can dramatically improve wireless security by ensuring physical security of your premise to make sure that unauthorized surfers of the network are kept out, and by designing your wireless cell coverage to cover only your premise, but not to extend unnecessarily beyond your business boundaries. This may mean that cell sizes are not optimized, leading to the increased cost of more access points, or that the odd dead zone is created in hard to reach corners, but this is a good alternative compared to letting your wireless network spill into the public domain for easy breach.

Securing a WLAN is similar to securing any other network, in that it involves layers of security and within each layer there are configuration options that will help customize the implementation path in order to meet your specific needs. Once we understand the overall security architecture that is possible, we can turn to recommendations for the implementation plan itself.

The security options we will review will be based upon the Cisco Aironet wireless LAN offering, which is the WLAN product with the most market share. Most other products available in the market should support most if not all of the same security features as many are industry standard.



The three main layers of WLAN security available are Authentication, Access Control, Encryption and Data Privacy.

1. Authentication

There are several options available for authentication, and it is important to review the applications that need to be supported by the wireless network, along with overall corporate security standards to determine which methodology best meets a specific need. Options available include:

- MAC authentication
- Open or Shared Authentication with SSID and matching WEP key and shared key.
- IEEE 802.1X:
  - Cisco LEAP (a.k.a. EAP-Cisco Wireless)
    - User authentication via user ID and password
  - PEAP
    - User authentication via One-Time Password (OTP) or static password (PAP or MS-CHAPv2)
    - Same CA certificate used to validate server to all users
  - EAP-TLS
    - User authentication with digital certificate (certificate installed Per User)
  - Wi-Fi Protected Access (WPA)
    - 802.1X is a required component of the WPA standard.
    - WPA is tested with EAP-TLS but works with all EAP types
  - Fast Secure Roaming as an extension to permit wireless client devices to roam between acess points.
- VPN- IPSec
  - Options to leverage IPSec as a secure framework for wired LAN access.

2. Access Control

Once authentication has been complete, access control can be used to limit where, within the wired space a wireless device is permitted to go. This can be effectively achieved by using Wireless VLANs to correspond with wired VLANs and limiting access to networks based upon assigned VLANs. Combining authentication with VLAN assignment is a powerful tool in providing levels of service to various network groups.

The following parameters are configurable on the SSID wireless VLAN:

- SSID Name
- Default VLAN ID
- Authentication types (Open, shared and network-Authentication Protocol (EAP) types
- MAC authentication under open, shared and network EAP
- EAP authentication under open and shared authentication types
- Maximum number of associations: Ability to limit maximum number of WLAN clients per SSID.

The following parameter is configurable on the wired VLAN side:

- Encryption key: Used for static WEP clients.

2. Encryption and Data Privacy

Authentication and Access Control will ensure that only authorized users will gain access to the network, and will be limited to reaching only the resources they need. This in itself will greatly reduce the security risks associated with rogue users, but will not protect the packets being transmitted by authorized users performing legitimate transactions. Even when your wireless signal is limited and contained within your own premise, you should consider the legitimate packets being transmitted over the wireless network to be as vulnerable as packets traversing a VPN link over the Internet.

Encryption technology will ensure that packets remain secure. Encryption options available are:

- WEP – static and dynamic
  - 40 bit
  - 128 bit
- Cisco –TKIP and WPA-TKIP (enhanced WEP)
  - Cisco standard and Wireless protected access TKIP
  - TKIP-MIC (message integrity check) to reduce replay attack vulnerability.
- Advanced Encryption Standard (AES) in near future
  - Stronger alternative to the WEP RC 4 algorithm.

One of the main challenges you will have in planning a security scheme is verifying that your end devices can support the level of security required. For example, wireless IP phones will not work when LEAP is deployed, and may need to be on a separate VLAN if LEAP is a part of your standard data security deployment. The flexibility of being able to tailor the security scheme on a per VLAN basis enables you to configure your security to maximize the end device capability, and to have a security scheme for each device that optimizes performance and adjusts to the security risk that is posed by that device. Lastly, remember to ensure that you match the WLANs to the appropriate VLANs and that you have adequate security on your LAN network. While wireless networks get most of the security attention in the media, it is not uncommon for organizations to have significant LAN issues that negate the value of any wireless security that may be implemented.

A good approach toward designing and managing wireless networks is to assume that they are security risks and integrate the highest levels of security you can manage. For example, ensure passwords or keys, if static, are long and complex to reduce the chance of dictionary attacks for cracking. Also, rotate and change your security values on a regular basis.

Finally, ensure that you inventory your end devices to know if an end device has gone missing and plan for reconfiguration as required.

Ultimately, wireless continues to travel the same path as other enabling technologies, such as VPN, have previously traveled. The potential power of the technology means that many have ignored the security risks in the short-term. However, as the technology reaches a mature state, wireless security continues to be a major concern for CIOs that needs to be addressed if the technology is to have a long-term viability. In part, this is justified, as the standards are still in the evolutionary stage, and many of the end point devices that have strong demand from early adopters are playing catch-up in adapting to what standards do exist.

However, remember that fundamentally good technology is always humbled by poor deployment practices, and poor deployment practices generally occur during the rapid expansion phase associated with early adoption where demand out strips the supply of expertise. While wireless security still needs to evolve to the state where it has the trust level that is equal to other enabling technologies such as VPN, many of the current security woes are largely perception due to poor implementation practices that gain notoriety, rather than weaknesses in the technology.

***Sam Johnston** is a partner and Chief Technology Officer of Intesys Network Communications Ltd., providing value-added networking and e-commerce solutions to the iSeries community. He can be reached at (416) 438-0002 or via e-mail at sjohnston@intesys-ncl.com. Any TUG member wishing to submit a question to Sam can forward their typewritten material to the TUG office, or to Intesys. The deadline for our next issue is Friday August 13, 2004.*

Take Advantage of your TUG membership...

TUG , in association with **COiN** (Central Ontario Information Network), and **MUGWNY** (Midrange Users Group of Western New York) will host **COMMON's Fall 2004 Conference and Expo in Toronto, Oct. 17-21.**

Some things you need to know...

► Your TUG membership automatically makes you a member of COMMON, so you can save the US$395 annual COMMON corporate membership fee.

► If you are a member of TUG, live in the Toronto area, and don't require a hotel for the conference – you still qualify for the CH (Conference Hotel) rate, a further savings of US$100 on the registration fee.

► Contact the TUG office for the COMMON membership number and the CH rate code.

► Go to www.common.org to register. Tell them TUG sent you!