Architecting a Secure Wireless Network

Ian Burke
MSIA678
Regis University
December 2, 2011

Abstract

When considering network architecture there are many things to consider. Use is among them. How you secure a network in a coffee shop would be different than how you would secure a back-end banking network in a PCI infrastructure. Integrating wireless into a network architecture will result in no less consideration. Likewise a public wireless implementation would be protected very differently than one implemented for wireless credit cared scanners.

When considering these dynamic situations it is clear that there is an array of situations in which you might secure wireless. This paper will explore some of these. It will also take a brief look at the way wireless access in a public environment might impact a corporate infrastructure and what safe guards might be implemented. This discussion is intended not to explore all of the technologies employed in wireless. Nor to be a comprehensive discussion of the advancements in wireless security. There is acknowledgment of new research into the WAP and iMode technologies. There is also acknowledgment that 802.11 in its design has flaws. Some of these exist in the encryption employed in the standard. These flaws will be acknowledged but they will not be explored in depth. The focus of this paper will be to look at what is involved in designing a secure architecture and what functional considerations must be considered in the process.

Discussion

Starting with the basic understanding that wireless, as with all networks have a varied set of

uses, it must be agreed that the type of implementations will also be dynamic. There are some basic considerations to look at when considering these types of implementations. These include things such as who needs access to the network and for which purpose is the network being used. For example a network that is required to allow access to both authenticated as well as guest users would be different than a network that is required to only all ow access to authenticated users. A network which is used to access only public data might be configured differently than data which is highly confidential. The following table outlines some of the considerations that should be looked at when looking at the different issues around wireless networks.

Authenticated Acces	Guest Access	Mixed Access	Confidential Da	Public Data	PCI Use
Internal Network Secured from Public Access	Isolated from internal network outside of firewalls	Access to internal network may depend on nature of data. Should employ technologies such as NAC and look at placing outside of firewall with VPN access to data.	Wireless should either deny public access or require VPN access to data	Public data should be distinct and isolated from internal data so that does guest or public access does not require special access	and PCI wireless should be hardened and isolated from the rest of the network so that the data can be send encrypted over the wireless and so that it is not in the same segment as other data.

Table1

Looking at some of the concerns around wireless might help to better understand some of the issues around these scenarios and allow for a better understanding of the complexity.

Miller (2001.) explores many of the wireless security issues today from the flaws in 802.11 to

the issues around the encryption and authentication methods employed. While WPA is more secure then the WEP standard he focuses on his premise is still valid. Wireless networks offer the sames vulnerabilities as wired infrastructure plus the weaknesses found in 802.11. This places the mandate on network administrators to implement appropriate safeguards to secure the wireless network. (Keygainnis, Owens. 2002.)

There is more to the security issue with wireless than simply these weaknesses though. Part of that keeps the success of wireless from moving forward is a successful standard and part of it is perception. Also, the current standard is no longer inclusive of all technologies. 802.11 looks at traditional wireless but what of cellular technologies and how do we account for other wireless technologies as they emerge. Ashley, Hinton and Vanderwauver (2001.) discuss some of these issues in their paper. They look at some of the new standards such as WAP and how these are looking at incorporating technologies such as SSL from end to end through the communication channel. They compare some of the WAP and iMode security features to the TCP/IP security feature.

So this raises some questions around how to architect a secure architecture to protect a wireless environment. Sherwood, Clark and Lynas (2005.) provide some insight into the impacts of different levels of architecture and how architecture complexity impacts and organization and its business processes both from an operational perspective as well as from a functional perspective. Integrating the right level of architecture into the information flow is critical to optimize the functional objectives of the business to enable security to function as a business enabler as opposed to a business constrictor.

In the wireless scenarios we began with we looked at authentication. In an ultra secure environment a security administrator may look at configuring their environment to suppress the advertisement of the SSID for their network and require authentication by pre-recorded MAC address of the end-client machine. While when coupled with encryption this would be a difficult network to compromise it would also be a difficult network to work with. Each client system would need to be

custom configured and would struggle to roam from access point to access point. There would also be potential for other complications such as lost packets due to communication issues. An alternative to this would be to require WPA2-Enterprise authentication with a radius table of MAC addresses to verify client systems. Advertise the SSID so that systems can roam from one access point to the next. This would still require a considerable amount of configuration but would make access and authentication secure. Neither of these situations would allow for guest access. In the event that you should need guest access in a secured environment they would need to be vetted and granted a one off situation. Conversely a non-secured guest network could be built that would only have Internet access. One common mistake made on secure or confidential networks is that guest networks are simply routed outside to the internet but are maintained on the same network as the secured wireless. As Keygainnis, Owens point out many o the common threats facing networks are much like viruses. Failure to truly segment a guest network from a secure network can lead to larger issues. Proper fire walling and monitoring is essential in securing your confidential data.

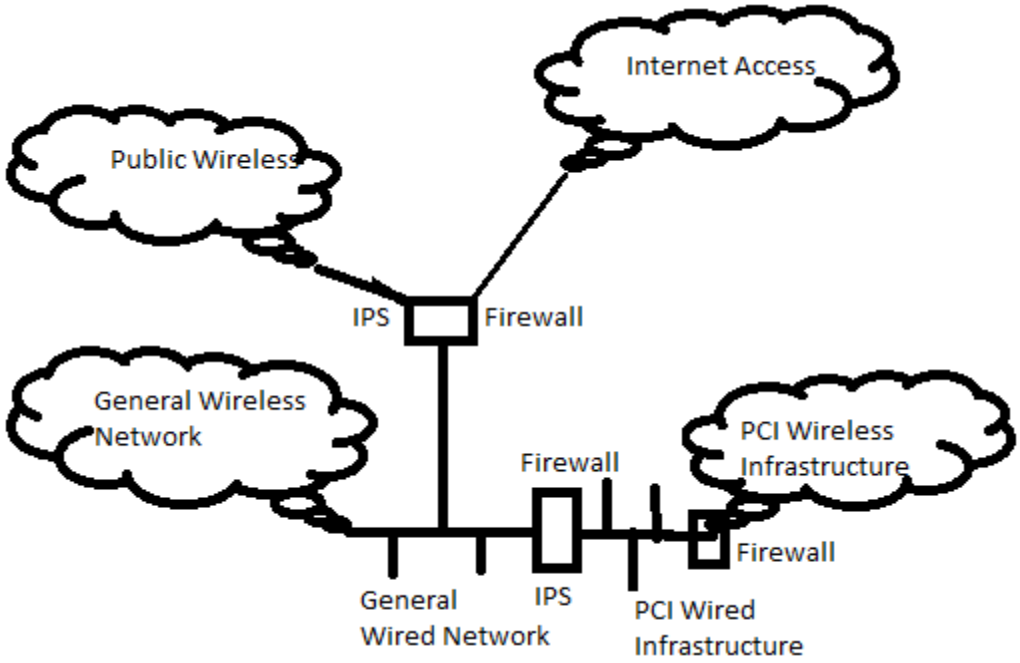
Many organizations employ network access control solutions for managing who has access to what network resources. Some of these can help to register and manage known and guest access to a wireless network. For example, a known employee system might simply be allowed access to the corporate wireless network while a guest system would be forced to a registration vlan and ultimately off to a guest vlan where they would be segmented off from the remainder of the network. These systems, while they help with access control also help with managing system configurations.

In our original scenario we also looked at the type of data, public or private, and how we might want to protect it in a wireless environment. As we look at the nature of the data we are exposing to the wireless network we need to consider the risk that we are willing to take with our network architecture. Is the data confidential but not protected by law or does the data fall under strict federal regulations? We need to look at whether the data is hosting personally identifiable information or simply business

confidential data. These types of details will help us identify both the regulatory constraints that our wireless solution must conform to and also the risk that we are willing to accept.

While the new WPA2 encryption standard is much stronger than the WEP standard employed prior it is still vulnerable to compromise. Haines (2010.) in the first two chapters of his book explore weaknesses in the 802.11 infrastructure both from the standard and the client side. He presents some of the commonly employed approaches to compromising the 802.11 standard from both through hardware and encryption weaknesses. If we acknowledge that there are known vulnerabilities in 802.11 than as security professionals we must implement appropriate safeguards to ensure that our data is protected to the level that is appropriate to the nature of its sensitivity.

As we identified that we would not choose to place public authorized guest accounts on the same wireless infrastructure as an authenticated secure user on the wireless network. We would not place sensitive or confidential information on a publicly accessible wireless network. For that matter we may chose to isolate the entire wireless network from the infrastructure containing the sensitive data depending on the nature of the data. By means of example lets look at a situation where one might have distinct and isolated wired and wireless infrastructures.



Iamge1

In this figure we see two distinct wireless environments. One for the PCI environment which is truly segmented off from the corporate network by two firewalls. This wireless network might be used for a mobile point of sales solution in the PCI architecture. In this situation it would be essential to enforce strong encryption such as WPA2 and at the same time limit access to both the nature of devices and the nature of data allowed on this network.

The other wireless environment is designed as a more typical corporate communication channel. Here this figure illustrated two SSIDs which have been split to two distinct vlans. One in the DMZ and the other internal to the corporate network. This type of situation would be indicative of a network supporting both guest and authenticated users. This situation might be supported by a network access control environment or some similar type of solution.

To this point we have been looking closely at the internal environments and how to support these dynamic situations. What is clear today is that many of our users are accessing our networks from

diverse and unique remote environments. With users coming across the internet from locations as public as restaurants, airports and hotels, it is safe to assume that these connections are unsafe and often compromised. This places yet another challenge on securing these wireless solutions. Unlike before where the conversation was focused on securing the connection to the wireless environment, here the conversation is on securing a connection from the internet. It may be assumed that the source connection is wireless but it may also be wired.

Here again there are options that should be considered but the focus is on how secure an environment is desired. The base in all of the solutions rests in a virtual private network (VPN). Establishing a VPN connection from the remote client to the corporate network will create a secure tunnel through which the communication between the client and the network is secured and confidentiality may be maintained. A consideration that organizations look at during configuring the development of a VPN solution include the use of a split tunnel which would allow for the VPN connection to access the internet through the local connection while accessing the corporate data through the VPN tunnel. While this may offer a benefit in the load placed on the VPN tunnel it is a large security risk in that any vulnerability the client is exposed to through the internet connection may potentially be passed along through the VPN tunnel.

A VPN should still be inspected for other types of vulnerabilities. It should not be assumed that simply because the connection from the client is over an encrypted VPN tunnel that the content is clean or free of malicious content. Enforcing checks such as virus protection and intrusion protection on the remote connection will help to mitigate these threats. Jiang, Kim, Shankaranarayanan and Henry (2003) look at the implications of integrating wireless and cellular into the network infrastructure. They emphasize the need for a VPN but explore some of the different protocols that would also come into play in the process of deploying the different technologies.

Conclusion

Wireless networks impact our organizations in many ways. It is important that we integrate them into our environments in an appropriate manor. Authentication and encryption mechanisms need to be taken into consideration so that the appropriate safeguards are taken for the appropriate data classifications. Failure to segment off a PCI wireless infrastructure could not only lead to the compromise of confidential data but also could result in the failure of a PCI audit which might result in fines or regulatory over site or the revocation of bank support for credit card processing.

A good wireless architecture is not simply about the removal of public access but rather the meeting of security and business objectives. A business that has a need for guest access may find that the implementation of a gues wireless network may be an ideal situation in that they can control the network appropriately. In contrast a network with a fairly mobile workforce will need to implement a wireless network to support their employees but may desire to segregate that corporate network from public access. These are the considerations that need to be measured when architecting the wireless network.

Likewise it is important to ensure that the connections to the network that generate from outside the corporate environment, such as the internet, are secured through a tunnel such as a VPN. This VPN must also be re-enforced with tools such as monitoring and anti-virus to ensure that that the client does not compromise the corporate network.

Wireless networks are useful advancements in a network design but must be architected carefully and thoughtfully.

References

Ashley, Hinton and Vanderwauver (2001). *Wired Versus Wireless Security: The Internet, WAP and iMode for E-Commerce.* IBM Software Group. Retrieved from: http://scholar.google.com.

Haines. (2010). Seven Deadliest Wireless Technology Attacks. Burlington, MA. Elsevier.

Jiang, Kim, Shankaranarayanan and Henry (2003). *Integrating Wireless Lan and Cellular Data for the Enterprise.* AT&T Labs Research. Retrieved from: http://wotan.liu.edu/docis/lib/goti/rclis/dbl/ieinco/(2003)7%253A2%253C25%253AIWLACD%253E/www.research.att.com%252Fareas%252Fwireless%252FMobile_Interdomain_Roaming%252FCellular_WLANs%252FInternetRoamingInternetComputingMagzineMar03.pdf

Keygainnis, Owens. (2002). *Wireless Security 802.11, Bluetooth, and Handheld Devices.* National Institute of Standards and Technology. Retrieved from: http://scholar.google.com.

Miller. (2001). *Facing the Challenge of Wireless Security.* IEEExplore.ieee.org. Retrieved from: http.scholar.google.com.

Sherwood, Clark, and Lynas (2005). *Enterprise Security Architecture.* Sabsa. Retrieved from: http://scholar.google.com.