



COA¹ Paper

Secure Protocols - Wireless

Problem

For mobile working, connectivity via wireless, whether inside the corporate environment or via publicly available hot-spots, Wi-Fi, Wi-Max or Cellular Data (GRPS, Edge, 3G) offers the ability to roam while remaining connected to your resources. The issue for most corporates is how they provide secure connectivity for their mobile workers, and end up with a trade-off of usability, cost, complexity and functionality.

For most mobile usage outside of the corporate WAN the use of IPSec VPN and 2-factor authentication is the most common standard, but whilst fine for static connectivity, say in a hotel room, it is restrictive for quick use “on-the-go”. The use of wireless inside the corporation is a known security risk and is generally implemented in a number of ways;

1. **Totally untrusted;** the users still need to use VPN and 2-factor authentication, this does not encourage “occasional” use, neither is it user friendly.
2. **Authenticated usage;** using WPA2 and Radius or similar AAA solution users can enter a password, or 2-factor authentication that permits access but secures the air interface.
3. **Background authentication;** the connection of the PC uses Active Directory to perform 802.1x authentication of the hardware and validate the user’s cached credentials. This is the most user friendly but is limited to a Microsoft only solution. Non-Microsoft authentication solutions are possible, but interoperability can still be an issue.

The flaw in all these solutions is that there are actually three separate problems:

1. Protection of the air-interface against unauthorised usage
 - In the public space the protection and generation of revenue
 - In the corporate space, the protection against intrusion inside the corporate boundary
2. Authorisation of the user to make a connection into the corporate WAN
3. Privacy and confidentiality of data transferred over the connection.

Why Should I care

The deployment of wireless within an enterprise exposes the corporate network outside the physical constraints of the building. Thus any mis-configuration or weakness effectively deperimeterises the whole organisation.

¹ The Collaboration Oriented Architectures (COA) paper and COA Framework paper are both available at <http://www.opengroup.org/jericho/publications.htm>

Current “secure” solutions are expensive and costly to manage and only work within a limited enterprise deployment. Conversely, systems that are secure (through employing inherently secure protocols) can utilise any wireless solution (corporate or public) without need for complex location awareness. With such a secure de-perimeterised solution, it is possible to implement a much simpler infrastructure; thus achieving significant cost savings. In this new environment, risk to the corporation of unauthorised use is substantially reduced, and while the business may choose to provide an open solution, they may still wish to implement some degree of connection authorisation thus guaranteeing their wireless users quality of service (QoS).

Recommended Solution/Response

By looking at these three problems both as separate problems and in a de-perimeterised manner reduces the complexity and provides an increase in security.

Background & Rationale

The need for inherently secure protocols

The protocols used by the end devices are all inherently secure protocols² (JFC#4³) and then all end-devices are thus capable of being deployed on the raw Internet (JFC#5).

If only such protocols are used it thus becomes irrelevant whether the end device is connected on a public network, public wireless of whatever type or a privately managed network, wireless or wired.

The need for quality of service (QoS)?

Operating in this environment, the question then arises; “why would a company need a private wireless network” to which the answer is; they may not any more.

The provision of a private network in a de-perimeterised world is now not driven by the need to provide (a false level of) security. Instead private networks (wired or wireless) are areas of network connectivity where a company can provide control over the traffic, ensuring that adequate bandwidth is available where they require it, and that performance meets the needs of the applications they are using over that network.

This is a Quality of Service issue and has little, if nothing, to do with security.

The need for connection control on Wireless and wired networks?

When implementing a wireless infrastructure for corporate use in a de-perimeterised environment then why can you not simply run an open network? This may be a viable option for a company that has non-corporate devices on its network every day.

The other option is to implement background connection control based on 802.1x or similar connection control mechanism. Authentication may be based on user or device or both (JFC#6). This will allow companies to implement QoS measures (rate limiting / bandwidth control) based on the device trying to connect. It could also require non-company devices (devices not inside the realm of your 802.1x credentials) to authenticate manually – for example via a redirected web page – similar to a hotel or public hot-spot.

² An inherently secure protocol is authenticated, protected against unauthorised reading/writing (probably encrypted) and has guaranteed integrity (is non-repudiatable).

³ The term JFC#n refers to the relevant Jericho Forum Commandment number.

Challenges to the industry

The numbering here provides for ease of reference and does not imply any priority.

1. Companies should regard wireless security on the air-interface as a stop-gap measure until inherently secure protocols are widely available.
2. The use of flexible interoperable 802.1x integration to corporate authentication mechanisms should be the out-of-the-box default for all Wi-Fi infrastructure.
3. Companies should adopt an “any-IP address, anytime, anywhere” (what Europeans refer to as a “Martini-model”) approach to remote and wireless connectivity.
4. Provision of full roaming mobility solutions that allow seamless transition between connection providers.

The way forward

The Jericho Forum believes that accelerating the use of inherently secure protocols will allow corporate to provide a simpler, yet more secure and holistic approach to remote and mobile and remote access.