Deploying a Secure and Scalable Wireless Infrastructure for use in Highly Sensitive Network Environments

Chris McNab, Matta Security
http://www.trustmatta.com

Gavin Leyfield, Ryzex Europe
http://www.ryzexeurope.com

Background & Rationale

Recently there has been a lot of public concern around the deployment of wireless networks, resulting in many organisations disowning the medium and its benefits. Wireless networks are already in use by hundreds of companies across the UK in warehouses and in other applications, including building maintenance and even restaurant ordering and table waiting systems. Wireless has been proven to improve efficiency within business, and will continue to do so into the future, offering high return on investment.

Traditional WEP (wired equivalent privacy) protocols including 802.11, 802.11b and even 802.1X provide defence against opportunistic attackers wanting to compromise wireless networks, many companies however, do not enable WEP encryption across their wireless networks, leaving them vulnerable to attack.

The 802.1X standard provides dynamic generation of WEP keys for each wireless user to then associate his devices with the network. 802.1X has been developed by Cisco and Microsoft, and uses a RADIUS-based authentication system, ensuring that users have to log onto the wireless network, before being able to access network resources. Other wireless vendors including Symbol Technologies, are embracing Kerberos authentication to ensure dynamic WEP key allocation. With larger network environments, a problem exists when users start to roam across sites and connect to different wireless access points, as they are continuously re-authenticating with the access points as they roam between them.

Matta was recently tasked with the design of a wireless network for deployment and use within a highly sensitive environment. Upon entering talks with Ryzex Europe (an established wireless network integrator), it was decided that the later 802.1X standards and other Kerberos-based infrastructures would not present the client with a scalable and secure single sign-on network.

Through using WEP encryption to provide a baseline level of network security, technologies including 3DES VPN tunnelling and token-based authentication were proposed to ensure a scalable, centrally managed, and secure network to be realised.

Introduction to the Model

When ensuring total security and control over a wireless network, it is important to not forget about the end users of the system, and authentication processes they must go through in order to use the applications at hand.

With key business drivers in mind, Matta has created its own best practice security model when talking about sensitive data being accessed by mobile wireless users across a series of company sites.

The following proven security technologies and systems form the components of our best practice wireless security model –

- RSA ACE Server
- RSA SecurID authentication tokens
- Checkpoint VPN-1 Gateway
- Checkpoint VPN-1 Secure Client

RSA ACE agents, and Keon technologies are not discussed due to the complex technical nature of PKI-based architectures and client requirements. Matta tackles single sign-on and specific requirements on a totally case-by-case basis.

Through openly admitting that WEP encryption does not provide adequate defence from determined attackers, it is important to put into place the right number of 'hurdles' that a potential attacker must jump over in order to compromise the sensitive network.

The first thing that we do is segment our infrastructure into 3 parts –

1. The non-trusted wireless segment

   The non-trusted wireless segment contains all wireless devices, access points, cabling, routing and switching infrastructure.

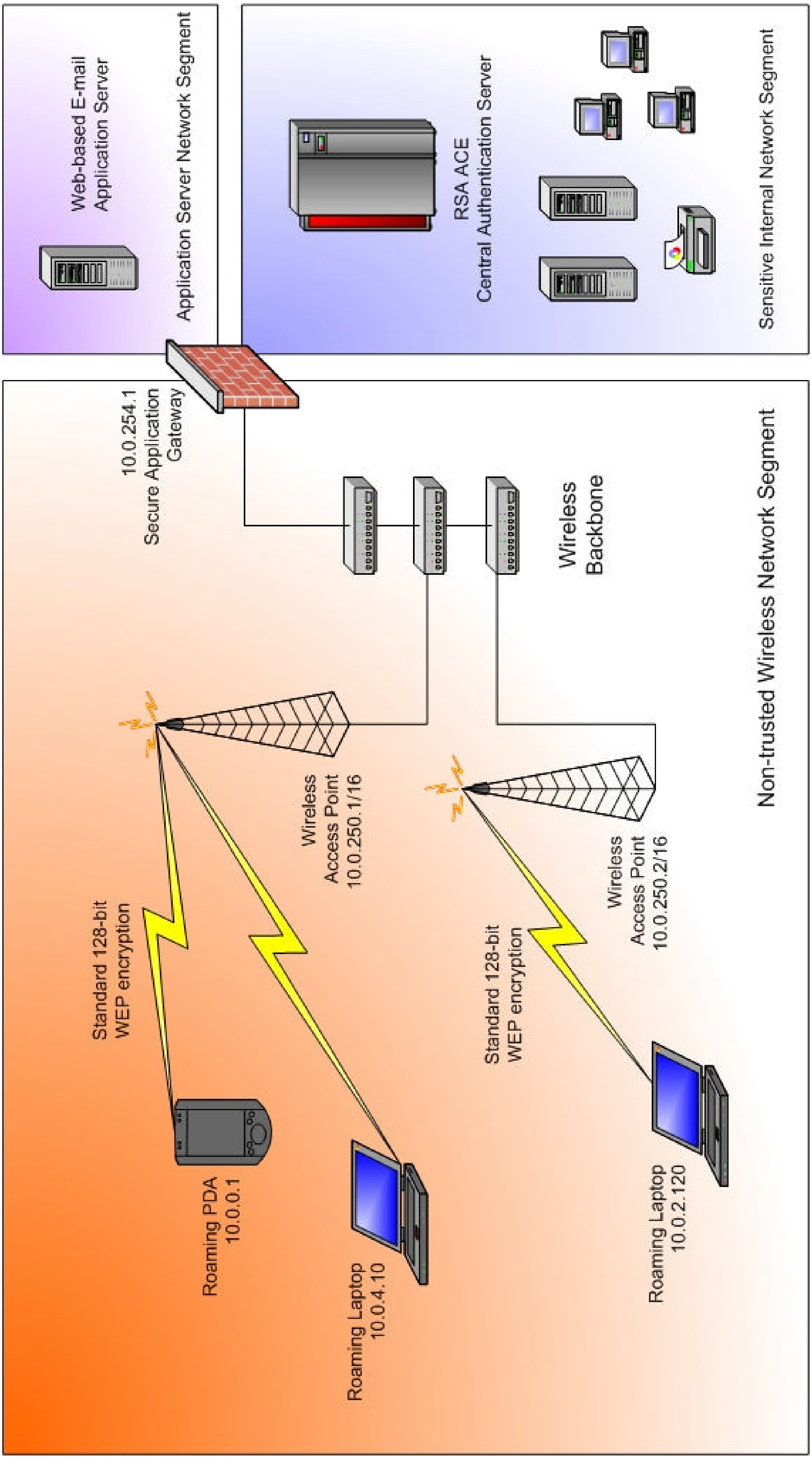
2. The application server segment

   The application server segment contains specific application servers that are to be accessed by the end user (for example, a web-based email application server, or Citrix terminal server).

3. The sensitive internal network segment

   The internal network space contains sensitive data is not directly accessible from the non-trusted wireless segment.

A logical diagram of the network follows on the next page..


Web-based E-mail
Application Server
Application Server Network Segment
RSA ACE
Central Authentication Server
Sensitive Internal Network Segment
10.0.254.1
Secure Application
Gateway
Wireless
Backbone
Non-trusted Wireless Network Segment
Wireless
Access Point
10.0.250.1/16
Wireless
Access Point
10.0.250.2/16
Standard 128-bit
WEP encryption
Standard 128-bit
WEP encryption
Roaming PDA
10.0.0.1
Roaming Laptop
10.0.4.10
Roaming Laptop
10.0.2.120

The model can be used to present content and serve applications securely using either a handful of roaming users, or thousands into the future. When Matta was tasked with designing a secure wireless infrastructure to protect sensitive information, a handful of different types of applications were being used across the wireless network (building maintenance, warehousing & stock control, e-mail collection and delivery, and Internet access), and so three secure application gateways were proposed.

The Secure Application Gateway

Each secure application gateway is a device responsible for the authentication of wireless users. Upon authenticating a wireless user, secure access to network resources is granted (using RSA technologies for authentication, and Checkpoint Hybrid IKE 3DES VPN tunnels to each roaming device). The roaming users associate with the wireless network when they power-up their wireless devices, and can then use an RSA-based single sign-on solution to access applications accordingly, through use of RSA Keon and x.509 digital certificates.

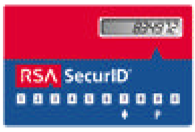
Each user's roaming device incorporates either Certicom's Movian VPN client (specifically designed for PDA and mobile phone VPN access), or Checkpoint VPN-1 Secure Client, which is configured along with other client software, to allow the user to easily access the applications he desires. Both VPN clients are capable of being used in conjunction with RSA two-factor authentication tokens, as outlined below.

Upon powering-up the roaming device, the user is prompted to authenticate with the secure application gateway using his RSA SecurID token. RSA SecurID tokens are available in three models, offering two levels of security –

- A keyfob token which generates a seemingly random number every 60 seconds, this random number is combined with the user's 4-8 digit PIN to form his passcode (SD600 model)

- A credit-card sized token which generates a seemingly random number every 60 seconds, this random number is combined with the user's 4-8 digit PIN to form his passcode (SD200 model)

- A credit-card sized PinPad™ token with a numeric keypad which generates the passcode by the user entering his 4-8 digit PIN number (SD520 model)



In environments where a high level of network security is required, an SD520 model PinPad™ token should always be used, as determined attackers could compromise user PIN details by sniffing authentication traffic. For the duration of this model, we will assume that PinPad™ tokens are being used.

Authentication from an end-user standpoint

Upon the user powering-up his wireless device, an authentication pop-up appears, prompting the user for the secure application gateway he wants to connect to, his username and SecurID passcode. Upon providing his passcode, a 3DES VPN tunnel is created between the end user's wireless device, and the secure application gateway.

The user can then launch a web browser or any other form of client to access the applications presented by the servers in the DMZ (de-militarised zone) behind the secure application gateway. Through using RSA Keon at desktop and application server level, single sign-on can be realised through using x.509 digital certificates throughout the architecture.

Matta has assisted in the design of Citrix Metaframe and Nfuse systems, allowing thin-client access to central resources to be realised through terminal emulation across wireless networks. The distinct benefits with using a terminal server such as Citrix Metaframe or Microsoft Terminal Services, is that data and access to resources can be strictly controlled.

Resilience of the Wireless Infrastructure

Through embracing strong two-factor authentication, coupled with 3DES encrypted VPN tunnels to each roaming user, a highly resilient and virtually impregnable wireless infrastructure can be realised. It would take an extremely determined and wealthy attacker in the order of 5 – 10 years with a supercomputer to break the encryption of a single 3DES tunnel. In real terms, roaming users will reconnect to the VPN on a daily basis, and so it will take hundreds of thousands of years for a determined attacker to completely compromise data flowing across the network segment between around 100 users and the VPN gateway.

Risk into the future can be managed by deploying IDS (intrusion detection system) sensors across the network infrastructure, allowing for a pro-active security stance to be taken. Network IDS sensor deployment on the non-trusted wireless network backbone will very quickly identify attackers and malicious users attempting to compromise protected networks.

Protection of the infrastructure is realised across the following levels –

- Wireless roaming user system security through platform hardening
- Wireless roaming user network security through personal firewall / VPN client deployment

- Environment password security and strong authentication through use of RSA SecurID
- Environment network security though dual-layer encryption
- Environment network security through IDS deployment

- DMZ network security through network filtering and control

- Internal network security through network filtering and control

- Application security and single sign-on through use of RSA Keon and digital x.509 certificates

Further Information & Considerations

Matta is a fiercely independent information risk management firm, in this instance, a Checkpoint / RSA solution was proposed from an ease of use and established interoperability standpoint. Plenty of other good two-factor authentication systems are available in the marketplace, most notably Secure Computing's Safeword system that is used by many large companies globally (http://www.securecomputing.com).

For more information, please contact us at –

Matta Security Limited
16 – 19 Southampton Place
London WC1A 2AX

+44 (0) 8700 77 11 00

info@trustmatta.com

http://www.trustmatta.com

Product brochures and implementation information regarding the technology tools discussed in this document are available from relevant vendor web sites –

RSA	http://www.rsasecurity.com
Checkpoint	http://www.checkpoint.com
Certicom	http://www.certicom.com