



White Paper

Security Management with iBurst Wireless Technology

Jonathan Withers
Chief Technology Officer, Personal Broadband Australia¹

Copyright © 2005 Personal Broadband Australia

PO Box 498, North Sydney, NSW 2059, Australia
info@pba.com.au www.iburst.com.au

¹ Personal Broadband Australia Pty. Ltd. ACN 123 456 789 www.pba.com.au

Introduction

The carriage of broadband services using wireless means is becoming commonplace. A legitimate concern of any diligent CIO or IT Manager is whether the introduction of a wireless technology could weaken the integrity of their IT networks, leaving it vulnerable to a new class of security attack.

This paper discusses the various aspects of wireless security management, the range of strategies applied to address the issues and some detail on the extensive security mechanisms used in the iBurst™² wireless broadband system operated by Personal Broadband Australia (PBA).

Background

Introducing a wireless technology to an enterprise IT environment presents a number of challenges not only from a technical perspective, but also due to its impact on operational procedures, the location and storage of information and, indeed, the way in which work practices become modified. The benefits of a wireless solution, be it within the office or providing fully ubiquitous coverage outside, are well demonstrated and will not be discussed further here.

To many, the use of wireless to carry sensitive data creates concern:

- “How can the carriage of data through the airwaves be as secure as using a wired solution? - surely it is easier to intercept?”
- “I’ve heard about WiFi - my neighbour’s got one and half the street ended up using it”
- And, from the better informed: “I’ve read about a successful attack mechanism on 802.11b (1st generation WiFi) - how do I protect myself against that?”

Putting Wireless Data Security into Perspective

The first point to address is the notion that wireless is an inherently less secure medium than wired solutions.

Any data transport mechanism must be assessed according to the sensitivity of the data to be carried and the required level of authentication of both the recipient and the originator. Wireless has the complication that the bearer signals can be received at more than one geographic location so it is necessary to ensure that any captured data is rendered unintelligible to anyone other than the intended recipient. On the other hand, wireless has the advantage that it is a shared medium, and that without the ‘inside knowledge’ it is very difficult to determine which recipient a particular captured packet of data was intended for.

Wired systems present their own challenges. There is often the presumption within the enterprise that physical security is the only mechanism necessary to protect system integrity - put everything in a locked room, have a good firewall in place and everything will be OK. More diligent system managers will create Private Network (PN) tunnels within the enterprise zone to prevent simple eavesdropping on the corporate traffic.

Irrespective of the internal solution, once the need arises to transport sensitive data beyond the enterprise zone - working from home would be a good example - most IT

² The iBurst™ system operated by PBA has been designed and developed by ArrayComm Inc. of San Jose, USA.

managers look to implement some form of *Virtual Private Network* (VPN) solution. VPNs are effective because they provide end-to-end (corporate server to client terminal) security without the need to have concern about the integrity of the transport networks in-between. The downside is that specific VPN software is required to be installed on each client PC and a degree of management and support by the enterprise IT staff is needed.

A note on 802.11 (WiFi) solutions:

WiFi solutions provide short-range data communications, typically in the home or office. However, they have received significant poor - and partially misguided - publicity regarding their lack of adequate security with headlines referring to networks being hacked into with ease, and therefore compromising the integrity of those networks. The fact is that 802.11 networks do now have encryption and authentication mechanisms which are adequate for the vast majority of networks. The difficulty is that these capabilities are SWITCHED OFF by default and it is up to the user/installer to enable them. Properly set up, 802.11 networks should be considered to be reasonably secure. A specific attack on the early 802.11b Wired Equivalent Privacy (WEP) cipher has been identified³ but these weaknesses are now being addressed in later version of the protocol.

From the above, it is clear that one solution to wireless security (which is also totally under the control of the enterprise) is to implement a VPN for all services to be run over the wireless bearer. However, such extensive measures are not necessary provided the chosen wireless solution has well thought out and properly implemented encryption and authentication mechanisms. The iBurst technology has all such capabilities and it can be demonstrated that it is quite possible to implement a secure PN solution if this is the preferred option whereby a session is terminated at the enterprise's servers. Indeed, it is possible to implement both this solution and VPNs if this is required.

The remainder of this paper will focus specifically on the security mechanisms implemented and supported in the iBurst wireless broadband solution.

Wireless Security using iBurst

Effective security has several essential elements:

- **Device Authentication:** Is the device being used to access the network legitimate and does it have the necessary access rights?
- **Network Authentication:** Is the network being accessed the correct one and not one 'pretending' to be the desired network? (spoofing)
- **Encryption:** Scrambling of the transported data using a cipher key to prevent interception of the data.
- **User Authentication:** Is the individual attempting to gain access legitimate and authorised to do so?
- **End-to-End Security:** The use of established techniques (SSL, VPN) to provide security between client and server.

³ Attacks that allowed the encryption key used by the RC4 algorithm in WEP to be extracted were first identified by renowned cryptographers Adi Shamir and Itsik Mantin of the Computer Science Department of the Weizmann Institute (Rehovot, Israel) and Scott Fluhrer of Cisco Systems Inc. (San Jose, USA) in a paper entitled "Weaknesses in the Key Scheduling Algorithm for RC4."

The PBA iBurst network is designed to support all of these elements. It should be noted that the first three measures are specifically architected within the iBurst protocol; the latter two measures are transparently supported by iBurst.

The iBurst security design is comprehensive, standards based, and has been specifically architected to be immune to known security attacks, including those used against WiFi networks.

iBurst security is based on the use of Digital Certificates which offer the following advantages:

- They provide a strong authentication method;
- Are scalable;
- Permit authentication verification to occur locally - no need for connectivity and latency associated with HLR/VLR-based schemes;
- Provide the ability to differentiate authentication and user authorization processes, and;
- Enable Public Key Infrastructure (PKI) implementation.

Each User Terminal (UT) has a unique certificate which in addition to the security function contains details of the class of service to be offered by the UT. In addition, each base station in the iBurst network has its own unique certificate. Certificates are managed centrally by a Certificate Authority (CA) and are updated on a periodic basis by the network operator (PBA).

Figure 1 provides an overview of the iBurst security architecture. Communication can only occur on the air interface between the User Terminal (UT) and Base Station (BS) and this supports both encryption and the UT and BS authentication processes. User authentication is provided using RADIUS, and the end-to-end link transparently supports network layer security (IPSec), transport layer security (SSL), and more advanced protocols at the higher application layers.

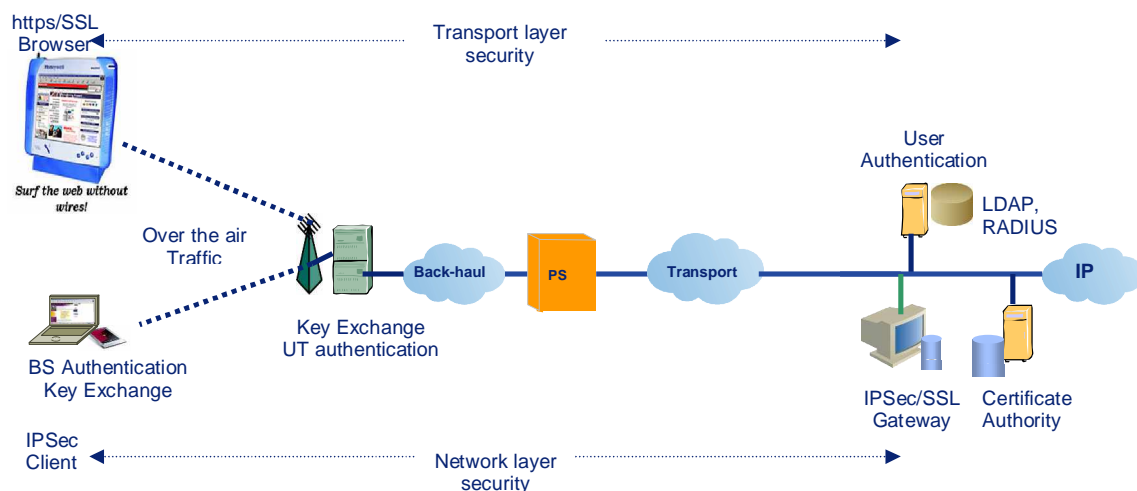


Figure 1 - Overview of iBurst Security Architecture

iBurst-specific Security Measures

iBurst has three protocol based security mechanisms; i-TAP for Device Authentication, i-HAP for Network Authentication, and i-SEC for over-the-air Encryption. All three protocols operate between the UTs and the BSs - this is illustrated in Figure 2 below.

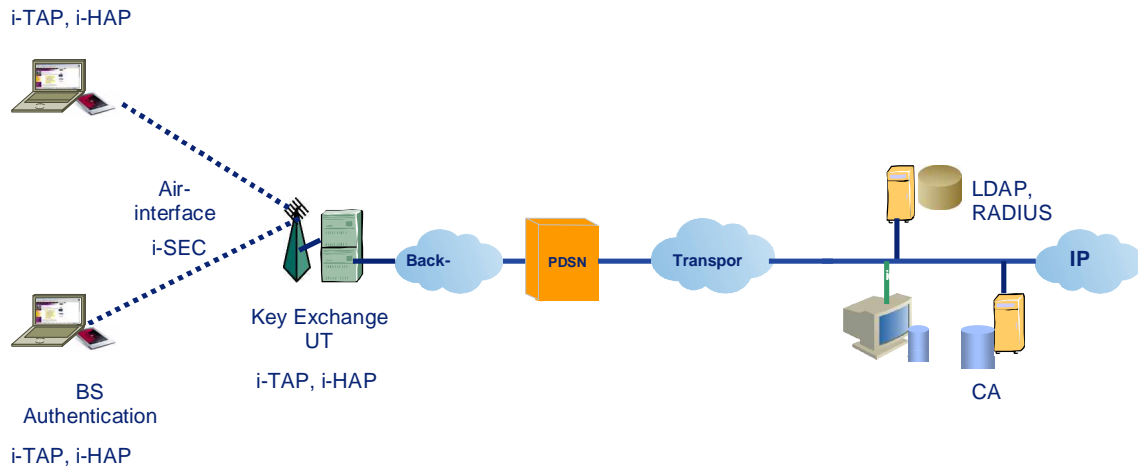


Figure 2 - Radio Interface Authentication and Encryption Protocols

Device Authentication (i-TAP)

The purpose of the Device Authentication process is to allow network access only to authorized UTs. The importance of this is that it prevents session theft on start-up and subsequently at any point where handover from one base station to another occurs.

iBurst Device Authentication is accomplished using the Terminal Authorization Protocol (i-TAP). i-TAP uses two different public key cryptography schemes; Elliptic Curve Cryptography (ECC) for secret key exchange and signed Digital Certificates using the RSA-1024 algorithm. Each UT has a public/private ECC key pair and the Certificate authority (CA) has a public/private RSA key pair. The CA signs digital certificates and keys using the RSA-1024 algorithm. The ECC complies with the FIPS-186-2 standard.

There are two principal certificate types; an Identity certificate that is assigned by the manufacturer and a Network Access certificate assigned by the operator (in this case, PBA).

In addition to its security functions, the i-TAP protocol also allows service profile information to be associated with each UT. Such information may include class-of-service and functional capabilities that the UT is entitled to use. This profile information is in addition to any user profile characteristics which are managed by the RADIUS server.

Network Authentication (i-HAP)

Network Authentication is the process by which the UT validates that it is communicating with an authorized iBurst Base Station (BS). This handshake mechanism is termed i-HAP and, as with the Device Authentication process, this is undertaken using Elliptic Curve Cryptography and RSA signatures. Each BS has a Digital Certificate containing a public/private ECC key pair.

In addition, i-HAP is the mechanism used for the exchange of the shared secret key which is employed for symmetric data encryption.

Radio Link Encryption (*i-SEC*)

The purpose of the i-SEC protocol is to secure over-the-air traffic between UTs and BSs providing the necessary confidentiality to user data. Further, it ensures that this information is shared only with UTs and BSs authorized by the Certificate Authority.

Confidentiality of data is assured by encrypting both the user data and control messages between the UT and BS using a function of the Secret Key. The Secret Key, which is set dynamically for each session, is based on RC4⁴ stream encryption and supports a shared secret up to 280 bits.

iBurst-transparent Security

The IP-centric nature of the iBurst architecture means that it can transparently support all of today's IP-based security mechanisms. Typical examples are User Authentication using a login/password combination and end-to-end network and transport layer mechanisms such as IPSec and SSL.

User Authentication

iBurst is designed to use Point-to-Point Protocol over Ethernet (PPPoE) to support PAP/CHAP user authentication mechanisms. During the session establishment phase, users specify a user name and password and this information is verified against a RADIUS database. This is illustrated in Figure 3 below.

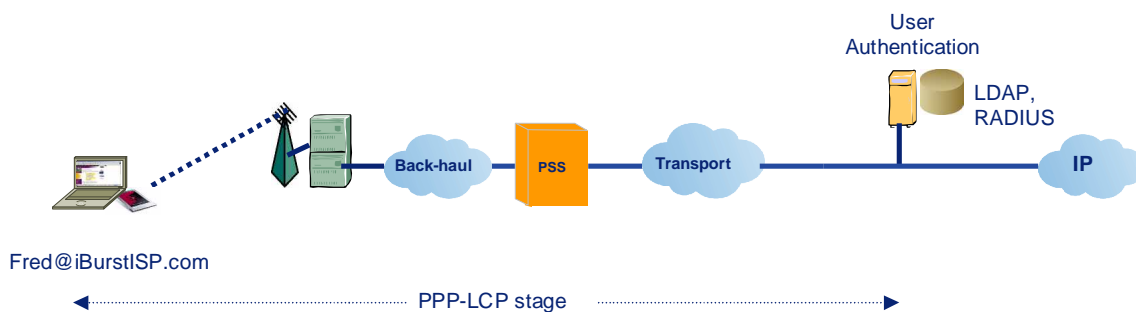


Figure 3 - PPPoE Supports Authentication at the ISP's RADIUS

End-to-End Security

Examples of end-to-end security protocols include Network Layer security using IPSec and Transport Layer security using https/SSL - see Figure 4, below.

⁴ Note that RC4 itself is unbroken - the WiFi attack discovers the key used by RC4. iBurst avoids the systemic errors used in WEP implementation in 802.11 systems through the use of key diffusion, long initialization vectors and key refresh.

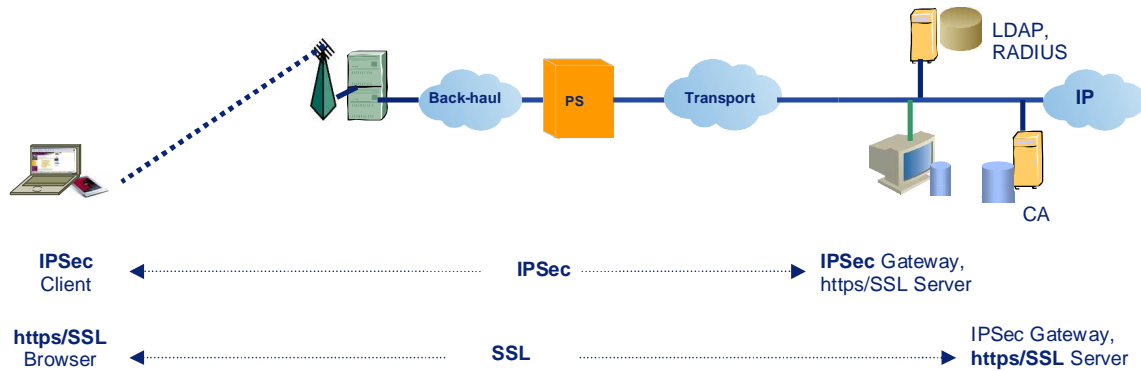


Figure 4 - IP Transparency Ensures Support for End-to-End Security Protocols

IPSec is used in a tunneled mode and requires an IPSec client on end user device and an IPSec gateway at the termination point (usually the operator/ISP). SSL/https are widely used commercial security mechanisms and are required to be supported by both endpoints of a user session. User data protected in this way cannot be intercepted at any intermediate point.

The IP transparency afforded by the iBurst system allows seamless operation of these and similar security protocols.

Summary

Personal Broadband Australia's iBurst network provides advanced security mechanisms which include mutual authentication of UTs and BSs on the radio link, privacy for user data on the radio link and support for end-to-end security solutions at Layers 3 and up. The solutions are standards based and have been architected to overcome known security attacks. Specifically, the architecture is immune to known WiFi attacks. Finally, the design has been implement to ensure low latency thus preserving the effectiveness of the communications channel.

PBA has an experienced team of IT professionals who are available to assist with the implementation of secure and cost effective iBurst solutions.