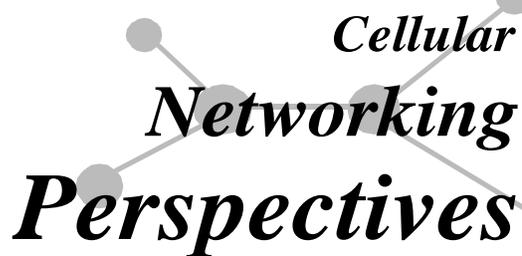


Wireless Security Perspectives



Cellular Networking Perspectives

Technical Editor: Les Owens, Managing Editor: David Crowe

Vol. 10, No. 2. February, 2001

CryptoNews: WEP Woes

Vulnerabilities Published for the 802.11b Wired Equivalency Protocol

It's not whether you have security in your goods; it's whether you have good security.

Introduction

We've all heard about the WAP (Wireless Application Protocol) woes associated with its slow growth. More important, however, is the news about the three security researchers who published some vulnerabilities in WEP (Wired Equivalency Protocol) — the security protocol for the IEEE 802.11b wireless LAN protocol. The IEEE's 802.11b, a recently adopted Ethernet-like wireless networking technology, operates in the 2.4GHz ISM band, which has become popular because of its world-wide availability. Pundits have predicted this technology, which is similar to the Bluetooth technology of which we have been writing, would take off because users like its range, reliability and security. The team of security researchers from UC Berkeley and Zero-Knowledge Systems may make some users re-think this motivation for 802.11b.

The 802.11b WLAN permits devices to establish either peer-to-peer networks or networks based on fixed access points which relay communications between mobile units. The researchers noted serious flaws “stemming from misapplica-

tion of cryptographic primitives” in the international IEEE standard. The team noted the flaws may lead to unauthorized disclosure and access security problems; they further noted that, because of these weaknesses, WEP doesn't meet its original design goals. The following four attacks were outlined:

- Ability to decrypt traffic based on statistical analysis (passive attack);
- Ability to inject traffic from an unauthorized mobile station (active attack);
- Ability to decrypt traffic based on tricking the access point (AP), and
- Ability to decrypt traffic in real-time follow analysis of captured (dictionary-building).

Nevertheless, the findings of the security researchers are no surprise. Many people have known about the 802.11b WEP security shortcomings. For example, in October 2000, a paper was published from Intel noting the problems with the WEP implementation. Also, efforts have been underway for months in the IEEE 802.11 standards body to “Kerberize” 802.11b — that is, add the Kerberos authentication capability. For more information, refer to:

[www.ietf.org/rfc/
rfc1510.txt?number=1510](http://www.ietf.org/rfc/rfc1510.txt?number=1510)

In any event, one thing is certain, it is not trivial to design a truly secure system — security is not a job for the uninitiated. A standards forum may say, “the technology has security.” That does not mean, however, the security is good. One of these days, we may stop repeating

About Wireless Security Perspectives

Price

The basic subscription price for *Wireless Security Perspectives* is \$300 for one year (12 issues) for delivery by emailed PDF file or by first class mail within the US or Canada. International subscriptions are US\$350 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees to allow more readers.

Current subscribers to *Cellular Networking Perspectives* receive a discounted price — only \$250 for delivery within the US and Canada or \$300 elsewhere.

Back issues are available individually, or in bulk at reduced prices.

Complete pricing information for both publications is available at:

[www.cnp-wireless.com/
prices.html](http://www.cnp-wireless.com/prices.html)

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due...

March 15th, 2001.

Future Topics

IP security • Public Keys & Wireless • Kerberos PKINIT • Public Key Infrastructure (PKI) • IKE • Wireless Data Security • IETF Security Standards • AES (Rijndael)

history, and we will use the right talent to build security right the first time.

Upcoming Security Events

The following are several upcoming fraud and security conferences that may be of interest to the wireless security practitioners.

VPNcon Spring 2001 (Virtual Private Network Conference)
19-22 February, 2001
San Jose

[www.vpncon.com/
2001events/spring/spring2001index.htm](http://www.vpncon.com/2001events/spring/spring2001index.htm)

Winter 2001 Biometrics Summit
26-28 February, 2001
Orlando

[www.aliconferences.com/
conferences/biometrics_feb01.htm](http://www.aliconferences.com/conferences/biometrics_feb01.htm)

InfoSec World Conference and Exposition
26 February - 1 March, 2001
Orlando

www.misti.com

CWTA Bluetooth™ Conference
6 March, 2001
Early registration by February 26
Toronto, ON

[www.cwta.ca/events/
bluetooth/index.htm](http://www.cwta.ca/events/bluetooth/index.htm)

eCoast SANS
23- 25 March ,2001
Portsmouth, NH

www.sans.org/eCoast/eCoast.htm

eSecurity Conference & Exposition
26-27 March, 2001
Boston

www.intmedgrp.com/security

Next Generation Fraud in Telecom
2 -4 April, 2001
London

www.iir-telecoms.com

Black Hat Briefings Win 2K Security
23-24 April, 2001
Hong Kong

www.blackhat.com

For more information on 802.11b, WEP and the recent vulnerabilities, visit the following sites:

[grouper.ieee.org/groups/802/11/
index.html](http://grouper.ieee.org/groups/802/11/index.html)

[www.nwfusion.com/newsletters/
wireless/2000/0717wire2.html](http://www.nwfusion.com/newsletters/wireless/2000/0717wire2.html)

[www.zdnet.com/zdnn/stories/
news/0,4586,2681947,00.html](http://www.zdnet.com/zdnn/stories/news/0,4586,2681947,00.html)

[www.wired.com/news/technology/
0,1282,41612,00.html](http://www.wired.com/news/technology/0,1282,41612,00.html)

[www.networkcomputing.com/
1006/1006r25.html](http://www.networkcomputing.com/1006/1006r25.html)

[www.isaac.cs.berkeley.edu/isaac/
wep-faq.html](http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html)

Wireless Security Perspectives will feature an article on the security (or insecurity) of WEP in a future issue.

Bluetooth, Part II: Applications

In the January, 2001 issue of *Wireless Security Perspectives*, we provided an overview of Bluetooth, with a particular focus on the security aspects.

If Bluetooth lives up to its promise, it will literally “cut the wires” for many applications. Some of the applications envisioned are:

- The Bluetooth Office – Workers will have personal computers with wireless connections to fax machines, printers and scanners. PC users will gain new freedom with Bluetooth-enabled mice and keyboards. This should also cleanup the office workspace immensely.
- The Bluetooth Business Traveller – Busy business executives can construct emails on an airplane and send them instantly upon landing. They will be able to “surf the net” from any location at an airport and at other common areas visited. At important business meetings abroad, they will be able to quickly upload business cards to a PDA. In the rental car back to the airport, they can drive safely while checking voicemail using a wireless cellphone headset. Last minute emails

can be sent automatically from carry-on bags while rushing to the gate. Back at the office, Bluetooth can be used to seamlessly synchronize the address books and calendar on their PDA with those on their PC.

- The Bluetooth Home – Bluetoothers at home can command home lighting and thermostats immediately from a wearable computer. Digital photographs taken at the zoo can be downloaded to a hard-disk. The kids can exchange saved games, and sit for hours on the couch with the joystick untethered from the TV. All will be able to enjoy BT-enabled cordless phones and have better command over the smart home appliances.
- The Bluetooth Store and Concession – A Bluetooth shopper can make a credit-card purchase of gasoline and a gallon of milk at the mini-mart quickly and nearly transparently from the Bluetooth-enabled e-wallet. While out-and-about later, he or she can dispense a diet coke from a vending machine with a simple account code entry from a PDA..

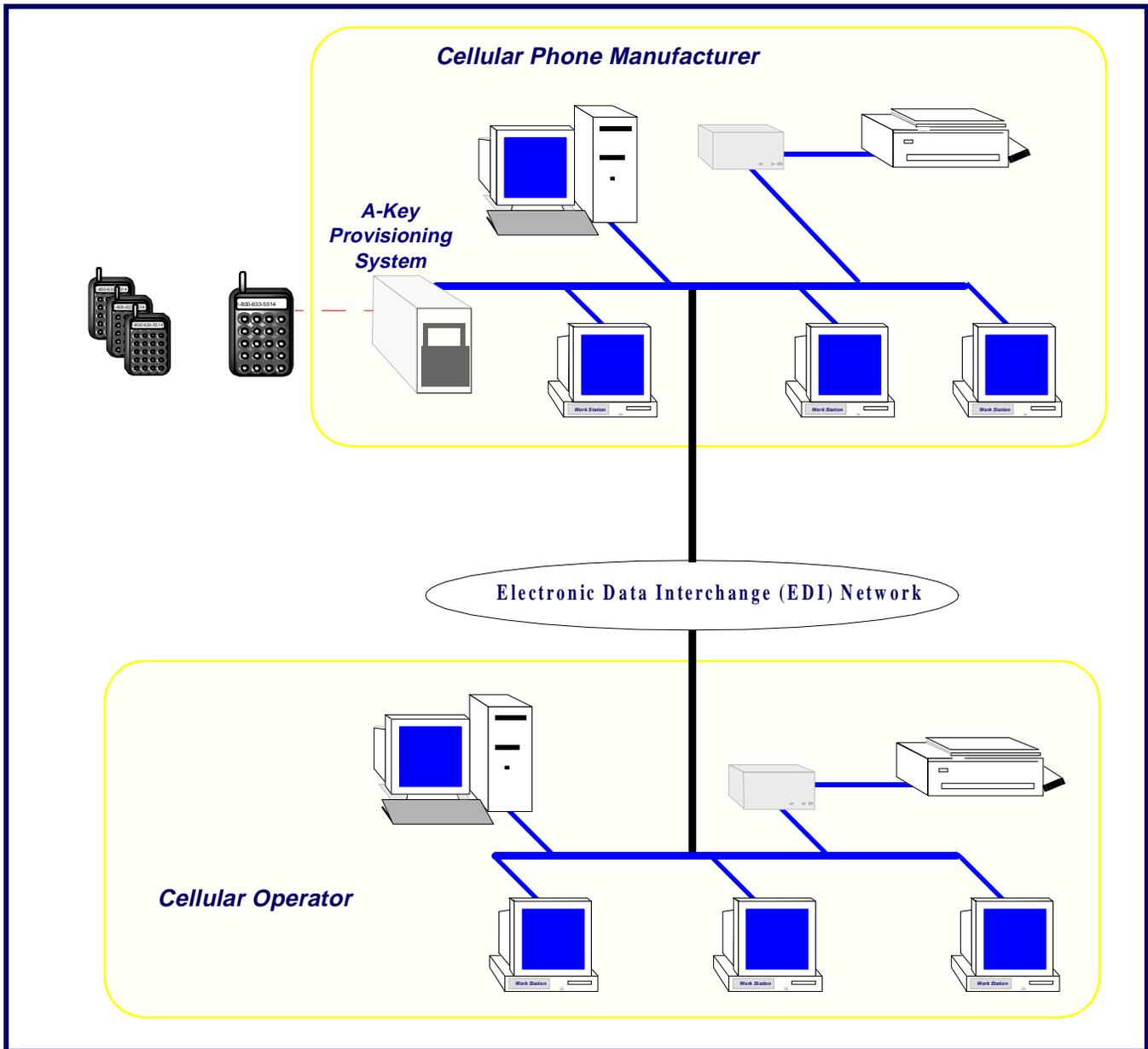
Applications are endless, although there will be competition from other technologies, particularly IEEE 802.11 for wireless LAN applications and HomeRF for management of appliances. Furthermore, only some applications will achieve consumer acceptance, no matter which protocol is used. Others will never make the transition from paper to product.

An Application: Cellphone Provisioning

For several years, North American cellular and PCS manufacturers have been provisioning authentication keys (A-keys) for the prevention of fraud. Typically this is performed in production facilities using various cumbersome and time-consuming cable connections to a dataport or “butt-plug.” With the emergence of Bluetooth, the A-keys can be rapidly, and perhaps more securely, inserted into cellphones. With a Bluetooth-enabled provisioning system

and with Bluetooth-enabled cellphones, this necessary and critical provisioning operation. as depicted in Figure 1, manufacturers may realize a significant cost savings for

Figure 1: A-Key Provisioning System that is Bluetooth-enabled



The North American cellular/PCS cryptographic key hierarchy is illustrated in Figure 2. This figure shows the keys used for authentication and other cellular security services. At the root of the hierarchy, is the seed secret cryptographic key, the A-key.

Current methods of A-key provisioning are the Over-the-air (using the cellular air-interface) method; manual A-key method (i.e. through the handset); and the data port method. The illustration

also depicts a fourth method – a new interface supporting Bluetooth enablement.

It is worth noting that this application of Bluetooth may also be used for the programming of the Number Assignment Module (NAM), subsidy lock codes, preferred-carrier lists, and other device-specific parameters. Such swift, hassle-free programming of cellphones could be of value to cellular service centers and cellular operators alike. The use of

Bluetooth for programming the A-key and other parameters is likely to appear this year, and it is expected to totally replace the use of the data port for this purpose in coming years.

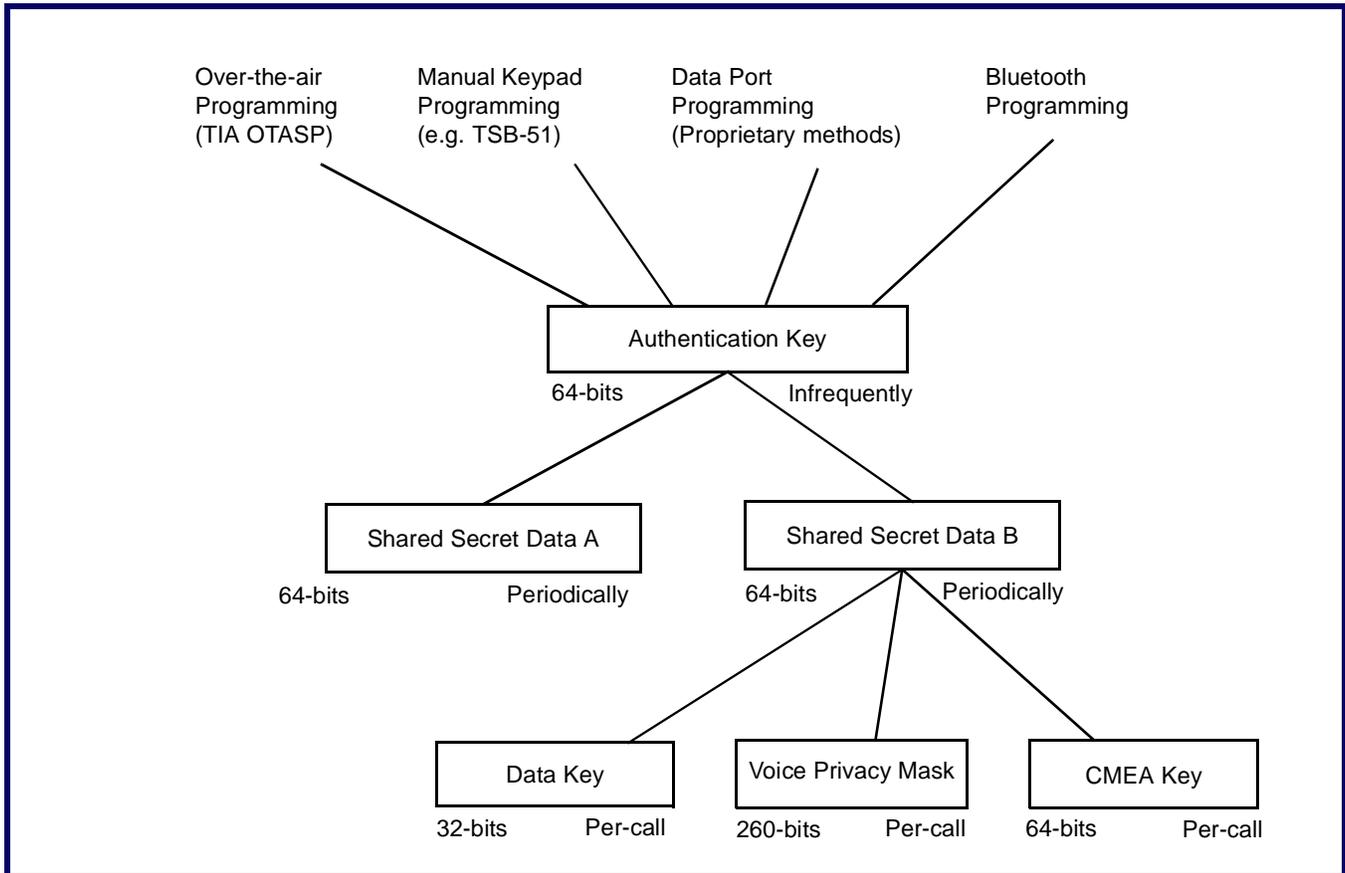
This method may not be necessary with GSM systems because encryption data for these phones is stored in a 'Smart Card' (aka UIM or SIM). Since phones never have any encryption data within them, phone manufacturers do not have to worry about provisioning of security

data. Smart card manufacturers have to program their product with a variety of information in any case, and they must sell their products directly to carriers or resellers; sometimes they must provide

programming tools. Smart card programming devices certainly could be Bluetooth-enabled, if mobility is a concern. Consumers and distributors of phones never have to worry about the

association of subscription and security data, because that is all neatly packaged on the "Smart Card."

Figure 2: Cellular Security Cryptographic Key Hierarchy



A Cautionary Note

One of the Bluetooth product areas described below is *Packet Analyzers*, more crudely known as *Sniffers*. While this equipment is useful, nay essential, for the development of Bluetooth systems, it is also the basis of any attack on Bluetooth users.

It is this kind of equipment, along with knowledge of the internals of cellular phones, that enabled cloners to so successfully attack analog cellular systems. It is worth remember that, as systems become more sophisticated and difficult to attack manually, automated test equipment and development kits become more and more sophisticated, giving fraudsters a head start in any attempt to penetrate the protective wall around any new technology.

Bluetooth, Part III: Information Resources

To obtain additional information on the Bluetooth specifications, visit: www.bluetooth.com

Conferences

To get in on the applications being developed, attend the Bluetooth Summit 2001. For additional information on this conference, visit:

www.it-telecomsolutions.com/pages/conferences/bluetooth2001.htm

For information on the 2001 Bluetooth congress meeting in Monaco, visit:

www.bluetoothcongress.com

Supranets

To read what this group has to say about Supranet, visit:

www.gartnergroup.com

Supranet refers to the wireless transmission of data and transactions between the hard-wired Internet, wireless devices (e.g., cellphones and PDAs), and the "papernet," meaning business cards and legal documents.

General Information

Below are three very useful web-sites for obtaining additional Bluetooth information:

- www.anywhereyougo.com
- www.palowireless.com
- www.thebluelink.com

The AnyWhereYouGo site provides several Bluetooth whitepapers which may be of interest. A very useful Bluetooth tutorial is available at the Palo Wireless site. TheBlueLink site is another great site to bookmark if you are working with or have interest in Bluetooth technology.

Bluetooth Equipment

Below are the URLs for several vendors offering Bluetooth-enabled equipment, PC cards, chip-sets or related products.

Chipsets

www.siliconwave.com

www.temic.com

Design Services

www.extendedsystems.com

www.wipro.com

Packet Analyzers

www.arca-technologies.com

www.digianswer.com

Other Manufacturers

www.3com.com

www.brainboxes.com

www.compaq.com

www.ericsson.com

www.hp.com

www.ibm.com

www.intel.com

www.motorola.com

www.nokia.com