Global Information Assurance Certification Paper

CDPD: A Look at a Secure Wireless Network

Introduction

The wireless revolution has pushed the current technologies to their limits. Today we have many devices connected around the world to wireless networks. Traditional telephony was granted years to address network security and reliability before customers started to rely on it for critical data transmission. The wireless medium has not been so lucky. Virtually a baby in the communications world, cellular networks now face their biggest challenge ever as they migrate from analog voice services to digital data delivery. Security has always been important with cellular but it is now essential. This paper focuses on one option called cellular digital packet data (CDPD) as a way to securely move data across wireless cellular networks.

CDPD Overview

CDPD was designed by the wireless industry to satisfy the need to push data across cellular networks. In 1992, carriers formed a group to conduct extensive research and development. They all needed to integrate data onto cellular networks to answer the demands of customers to be mobile. Their goal was to build a service that would address critical mobile data issues such as roaming, billing, security, and authentication. CDPD was the answer.

CDPD uses the OSI model like TCP/IP. That is why many experts refer to it as wireless IP. It is a true packet switched network that works as an overlay on top of an existing cellular network that uses 30 kHz channelization. In a simplified way this is the analog network that exists across North America.

CDPD is an efficient friend to voice transmission on a cell networks. It does not add overhead or interfere with voice traffic. It maximizes productivity of cellular channels by finding slack space in the analog communications to insert packets bursts containing data. It also waits for open channels and will hop across all channels when sending data.

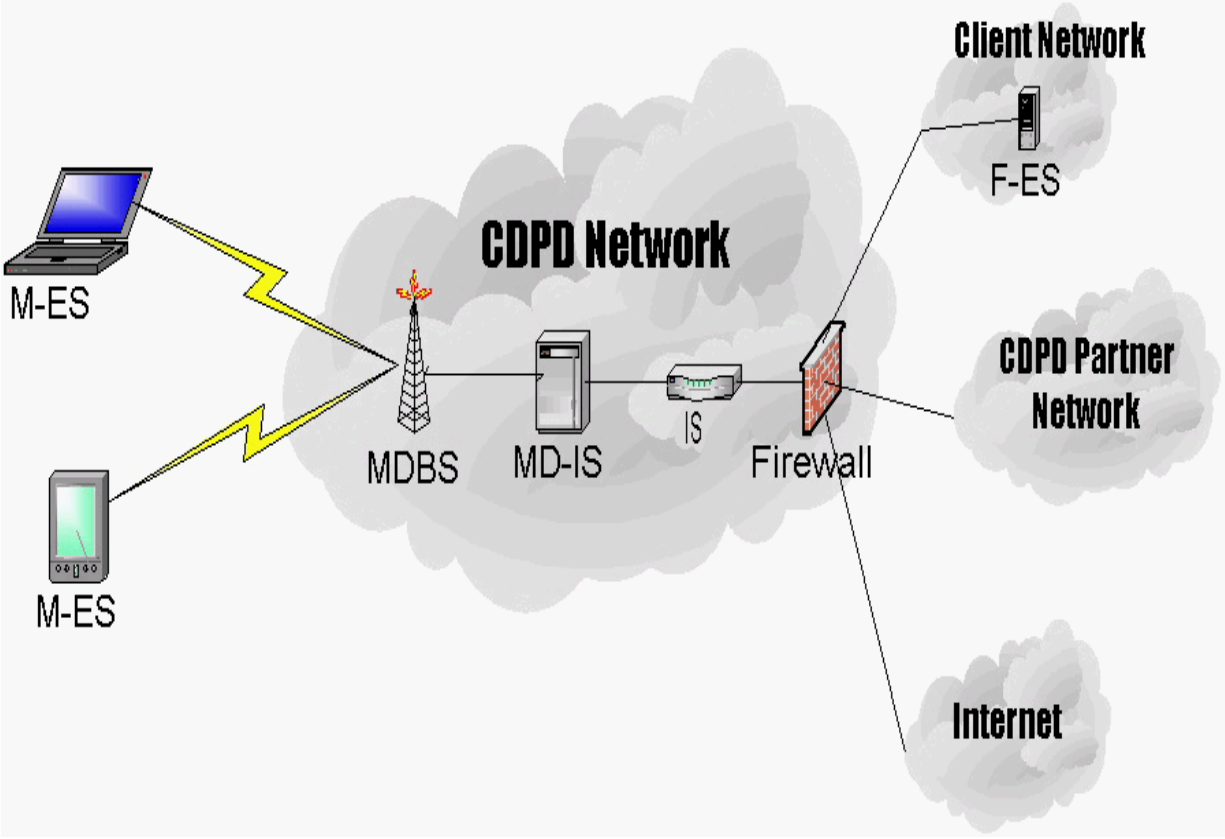
By it's design nature it does not require full control of the voice channel. Interestingly enough it doesn't have to establish a circuit or dial number. Hence it is a connectionless service. Once the device registers it is free to send and receive packets across the network.

Speeds are good for a wireless WAN. Raw transmission rates are listed as 19.2 kbps however real throughput is more like 10 kbps after the overhead for error control is factored in. CDPD also provides full-duplex communications. This permits wireless devices to transmit and receive at the same time. CDPD makes it possible to handle real-time interactive applications.

CDPD's most attractive feature is the security controls that are built in. The airlink is extremely secure. Your data transmission is virtually protected from all attempts to intercept of scan it. Device authentication is also excellent. Cloning an end device is extremely hard with CDPD registered devices. Security on customer data networks connected to the CDPD network remains the responsibility of the customer.

CDPD: An In-depth Look

The following diagram is an overview of some of the key pieces that you would find in an average CDPD installation:



This will prove useful when reading the remainder of this section.

The Devices

MES

Every client connected to the CDPD wireless network is considered a mobile end system or MES. These are traditionally PDA's or laptops with wireless modems. The connectivity provided by the wireless network can facilitate a variety of applications but because of the slower speeds involved usually involves limited web browsing. CDPD is very adaptive and has been incorporated into some areas that are unconventional. The following is a list of just a few key applications:

- Financial stock and new updates.
- Mobile workforces that track and dispatch technicians and vehicles.
- Law enforcement patrol radio and laptop access.
- Health care home patient monitoring and remote medical support.
- Telemetry uses such as remote control and monitoring devices.

Mobile Data Base Station (MDBS)

The MES connects to the mobile data base station also known as the MDBS. The connection is done across the airlink. Decisions on coverage really rely on this device. Having an MDBS in a cell site is an expensive move and implementation costs determine where carriers offer this service in their area. The MDBS does not make a contribution to the security of the CDPD network. It is a pass through device that facilitates sending and receiving packets to the MES.

Mobile Data Intermediate System (MDIS)

The MDBS serves as a relay between the MES and another component called the mobile data intermediate system or the MDIS. This box is really the heart of the system. The most important task that is carried about by the MDIS is managing the connections for all of the MES clients. It is really the only device that has any mobile intelligence. It does the mobile routing of MES data using a protocol called the mobile network location protocol or the MNLP. It determines the location the MES and then routes traffic to it via the correct path. It also performs critical management functions like data compression, encapsulated forwarding of packets to other CDPD carriers for roaming MES's, accounting, and multicast services. From a security perspective this is also the key piece. The MDIS is responsible for authentication and authorizing connections. It also provides the encryption services for the airlink communications.

Fixed End System (FES)

This whole system is designed to get back to some kind of end point where data or applications reside that the MES needs to access. This is referred to as the

fixed end system or the FES. It can be as complicated as systems or networks get or as simple as a desktop host. The key to this device is that it is fixed and not mobile like the MES. In most cases this is an email or application server but it can take other forms. In connecting the FES to the CDPD network appropriate security procedures must be in place at the customer's end.

Intermediate System (IS)

The final device that exists in a standard system is the intermediate system or IS. Is usually is a router but can take on other forms. The device is used to connect and route traffic from the MS-IS to some other sort of data network. That is most often the Internet or a corporate network but it can take on other forms.

The Interfaces

When looking at a CDPD network from a security perspective it is important to look at the devices and also their interfaces. There are four main interfaces deployed in a CDPD environment. They are:

- Airlink Interface
- Customer/External Network Interface
- Internet Interface
- Intercarrier Interface

Airlink Interface

By far the most important and security sensitive interface with CDPD is the airlink interface. That is the connection between the MES and the MDIS. The MDBS is not to be overlooked but it is more of a throughput device and not really an interface point. The airlink session is established when an MES contacts the MDIS with a "hello" request to create a secure tunnel between them. This is an SSL session that uses RC4 for encryption. RC4 is an RSA Data Security Inc. product available for use in 40 and 128-bit format.

Once the encrypted link is created a key exchange has to take place between the MES and MDIS. This key exchange competition rests totally on the ability of the MES to properly authenticate itself to the MDIS. The MES has an equipment identifier or EID and a network entity identifier or NEI. The EID on CDPD is traditionally the carrier assigned IP address. The NEI is comprised of two factors. One is the authentication sequence number (ASN) and the other is the authentication random number (ARN).

These ASN and ARN are credentials that take the role of shared secrets to positively authenticate the MES. They are different for every session. The ASN from the MES is sent across the encrypted link to the MDIS. If it is valid then the ARN is sent. It is important to note that they are not sent in the same payload

but are delivered as separate pieces of information to the MDIS authenticating server. Once both EID is verified as registered and the NEI information is certified correct two secret keys (Diffie Hellman) are created. One key is for sending encrypted data from the MES to the MDIS and the other for sending encrypted data from the MDIS to the MES.

The most important part of this is happens once the secret keys are in place. The MIS then updates the MES with credentials for the next logon session. The ASN is incremented by one and a new ARN is sent down. It is best to think of the ASN as the MDIS telling the MES how many times it has logged on. It is just an incremental counter. The ARN is the password issued by the MDIS. They are never really at risk of being compromised because they are never transmitted outside of the encrypted tunnel.

To contrast CDPD and regular cellular communications lets review the procedure an analog cellular phone uses to connect to the same carrier channels. The cell phone has two credentials it uses to access the network. It uses the manufacturer installed electronic serial number or ESN and a carrier assigned static mobile identification number or MIN. These credentials are passed unencrypted to the carrier. They are extremely susceptible to eavesdropping and that makes cloning very easy. Clearly CDPD has taken steps to secure against this risk.

If an MES in connecting to a carrier other than their home carrier the process is almost the same. The only difference is that the hosting MDIS routes all requests through to the home MDIS for authentication. Once the home MDIS authenticates a new ARN and ASN sent back down through the hosting MDIS to the MES.

Customer/External Network Interface

The customer interface is not all that complicated but it is essential that it be secured properly. Security on the network where the FES is located is usually the responsibility of the customer. The encryption of traffic on the airlink interface is not extended to the customer or external interface. The majority of these external connections use a frame relay network to build secure communications.

Traffic bound for an FES on the customers network would leave the MES and arrive at the MDIS. The MDIS would use the IS to route the traffic to the appropriate network. The connection from he CDPD network to the customer is usually a frame relay connection. Through frame relay a private virtual circuit or PVC is created. This relies on dedicated circuits between the customer and the CDPD network. That combination is much more secure than using the Internet. Today, VPN's across the Internet are being implemented to avoid some of the costs associated with this setup but for reliability and faster throughput many

customers prefer the PVC. VPN technology can be deployed through the PVC to offer end-to-end encryption through out the CDPD network in highly secure situations.

Depending on what type of security policies a customer has the traffic can be processed many ways once reaching their network. Usually a router screens the packets and sends then to the appropriate FES. A firewall can be implemented at this point in combination with the router when there is a security need for it.

Internet Interface

The Internet Interface is very straightforward. To fully understand the controls here you must go back to the authenticated MES's. The EID (IP address) that is assigned to the MES is critical throughout the network for routing traffic and restricting access. Usually carriers pool IP addresses into free IP's and restricted IP's. MES's with a free IP are free to send TCP and UDP packets through the firewall to the Internet. Likewise, any Internet host can send UDP and TCP packets to any MES with a free IP address. Restricted IP addresses are just opposite. They are restricted from hitting the Internet by the firewall on the CDPD network. Traffic is routed from the MES to the appropriate customer network via their PVC.

Intercarrier Interface

The final interface common to CDPD networks is the Inter-carrier Interface. It is the connection that brings together the CDPD networks developed by competing carriers. It allows MES's to roam and still have access to FES's attached to their home CDPD networks.

The inter-carrier interface is active during the authentication of a roaming MES. The MES contacts the serving MDIS which forwards the authentication credentials supplied across to the home MDIS. The home MDIS then checks the credentials and authenticates the MES. Now the MES is free to send packets to a FES on the home CDPD network. The only time the roaming MES doesn't have it's packets routed to the home MDIS from the serving MDIS is when they are Internet bound. The serving MDIS is permitted to the send those packets directly through it's firewall to the Internet without routing through the home CDPD network.

Once you familiar with all of the key devices and interfaces there are a couple of traffic rules that finalize the security and functionality of a CDPD network. A basic principle of the CDPD network is that only traffic passing through the airlink is allowed to ride on the IP network. (MES to FES, FES to MES, MES to MDIS, MDIS to MES, MES to MES) This traffic is not wide open. There are access control lists and firewall rules that further restrict this traffic to specific

destinations. Traffic from an FES to another FES is restricted. Also FES to Internet traffic is not permitted in either direction.

Summary

There are areas of the CDPD network security that can pose high risks. Any communication from the MDIS to the Internet or to an FES is not considered to be secure. Additional security elements, above and beyond CDPD, are required to offer reasonable security. VPN technologies seem to be leading the way here. Additionally most carriers adopted this technology when RC4 was the standard. Many have not taken advantage of the scalability of the CDPD infrastructure to advance to newer encryption packages than RC4.

The end devices themselves have problems. Even though the cell modems are a secure device they are not necessarily 'secured' in the MES that is using them. You don't need to clone the device if you can steal it. Access can easily be denied after the theft has been reported but it is the critical time between when it is taken and when the theft is discovered that poses the problem. Many devices and applications are password protected but those measures are usually easily defeated.

There is also some concern over the MES to MES communications. A vulnerable MES, such as a laptop with a cell modem, could be compromised if another device could remotely control it and use it's permissions. The big issue here is that customers are connecting their networks to an always-on service that hosts many clients. All of which are not necessarily trustworthy and reputable.

References

Verizon Wireless. "Verizon Wireless Data (CDPD) FAQ"
URL: http://www.gte.com/customersupport/howdoi/cdpd.html (April 3,2001)

Jim Geier. "CDPD Concepts"
URL: http://www.wireless-nets.com/whitepaper_cdpd.htm (March 29, 2001)

Gregory S. Smith. "CDPD: Does It Work Yet?"
URL: http://www.civic.com/civic/articles/1997/CIVIC_070197_48.asp (March 28, 2001)

Vasilis Koudounas. "Cellular Digital Packet Data (CDPD): What Makes It Reliable"
URL: http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol2/vk5/article2.html (March 30, 2001)

Wirless Ready Alliance. "CDPD Overview"

URL: http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol2/vk5/article2.html (March 29, 2001)

Sandra Wendelken, Radio Resource. "CDPD Hits the Streets"
URL: http://www.wirelessdata.org/atwork/pr%5Fstories/grotonpd.asp (April 3, 2001)

Rajarshi Gupta, "Cellular Digital Packet Data (DATA) Presentation"
URL: http://www.path.berkeley.edu/~guptar/wireless/CDPD/Default.htm (March 29, 2001)

Symphony Phone Inc., "Cellular Digital Packet Data"
URL: http://www.soloist.com/cdpd.htm (March 30, 2001)

Peter Rysavy, "Wireless IP : Ready to Lift Off?"
URL: http://www.networkmagazine.com/article/DCM20000503S0033 (March 30, 2001)

Lucent Technologies, "Wireless Networks – Cellular Digital Packet Data (CDPD)"
URL: http://www.lucent.com/wireless/products/networks/ai_cdpd.html (April 2, 2001)

Dorothy E. Denning. "Information Warfare and Security"
January 1999, Addison-Wesley Canada Ltd.

M Sreetharan & Rajiv Kumar. "Cellular Digital Packet Data"
January 1996, Artech House Inc.