



Financial Sector Discussion Paper

Mobile Risk Management: E-finance in the Wireless Environment

Tom Kellermann



Acknowledgements

The author would like to thank the following individuals who have spared their time and background material, for their valuable written and oral inputs: Chris Bateman, Tony Chew, Rick Fleming, Thomas Glaessner, Luc Laeven, Linda McCarthy, Valerie McNevin, Larry Promisel, Dr. Joseph Pelton, Cornelius Tate, and Dave Thomas.

- **The World Bank May 2002**

The findings, interpretations, and conclusions expressed in this paper are entirely those of the author and should not be attributed to the World Bank, to its affiliated organizations, or to the members of its Board of Directors or the countries they represent. The World Bank does not guarantee the accuracy of the data included in this publication and accepts no responsibility whatsoever for any consequence of their use.

Abstract

This paper documents the risks to electronic security via identity theft, hacking, etc. that wireless technologies may present in the context of delivery of financial services. Although the extent of security measures to be taken is not independent of the size of the transactions contemplated, this paper points out a variety of ways that interactions between technologies create points of vulnerability for security of financial transactions when wireless technology is employed. This paper lays out a variety of critical actions and measures that system administrators (particularly, in banks) can take in order to mitigate these risks to the largest possible extent and often without great increases in costs of security. The actions suggested in this paper for mitigating such risks reflect a concerted effort to address what many in the electronic security industry consider to be best practice in regard to electronic security arrangements in the case of use of wireless technologies in the delivery of financial services.

Foreword

The rapid growth of wireless technology in many emerging markets and the increasing use of such technologies in coordination with the internet or on a free standing basis to provide financial services in emerging markets will demand a very careful look at issues related to electronic security. Nowhere is this issue more prevalent in emerging markets than in the area of wireless technology given the extensive spread of cellular technology to many emerging markets. As more and more countries attempt to leapfrog via use of such technologies in the context of providing financial services, it is essential to recognize the potential electronic security breaches that can occur via use of wireless technologies and how market participants and systems administrators at banks or other key providers (e.g., hosting companies or ISPs) can better ensure that problems do not arise. Hence, this paper attempts to both illustrate how and why electronic security can become a concern and how to mitigate this risk via many actions that may **not** entail substantial additional costs for providers of financial services. Many of the recommended actions, noted in this paper related to layered security in the case of wireless applications to provide financial services, represent what can be considered to be best practice in the electronic security industry today. This comes with the important proviso that the rapid changes in technology make this a very difficult area in which to prescribe static guidelines for system administrators within financial service providers.

The paper is divided into the following sections. Section I introduces the reader to the widespread usage of e-finance and wireless technologies throughout the world. Section II illustrates the risks that are inherent to the wireless revolution. Section III depicts the vulnerabilities associated with WLANs and the appropriate risk mitigating procedures necessary to secure them. Section IV addresses the evolution of GSM networks and the vulnerabilities that are inherent to them. Section V details the appropriate methods of managing the risk found in GSM networks. Section VI illustrates the best practices for management of risk in the delivery of payment services. Section VII offers a conclusion with a perspective into the future (3G). The purpose of this document is to enunciate a set of security and risk management guidelines for banks and payment services. It aims to provide a framework for security risk assessment applicable to the wireless environment.

I. Background¹

Electronic financial services, whether delivered online or through remote mechanisms, have spread rapidly. Countries and consumers are increasingly getting connected. These new technologies not only allow countries to leapfrog in connectivity, they also open new channels for delivering e-financial services.² Since the mid-90s investment in banking technology has focused upon online banking and brokerage services to increase convenience. E-finance has lowered the costs of providing financial services. The

¹ For more detailed analysis of the e-security dilemma refer to "E-security Risk Mitigation for Financial Transactions" authored by Glaessner T., T. Kellermann, and V. McNevin, 2002.

² Glaessner, T., S. Claessens, and D. Klingebiel. 2001. "E-finance in Emerging Markets: Is Leapfrogging Possible?"

Internet eliminates many processing steps and labor costs, while avoiding the fixed costs of branch development and maintenance. A typical customer transaction through a branch or phone call costs about \$1 in the U.S., but that transaction costs just \$0.02 online.³ The lower costs for providing financial services have also allowed greater access to financial services. Internet-based services are sometimes as popular in emerging markets as industrialized ones. For example, online banking is nearly as widespread in Brazil as in the United States. Due to the apparent lack of fixed line infrastructure in many developing nations, most financial institutions have implemented wireless e-financial platforms to expand access to their services. Concurrent with these realities, four new technology related industry trends have occurred: outsourcing, open architecture, integrated strategies, and new methods of e-payment.⁴

E-finance is comprised of four primary channels. These are: electronic funds transfers, "EFT"; electronic data interchange, "EDI"; electronic benefits transfers, "EBT"; and electronic trade confirmations, "ETC". EFT is the oldest form of electronic money transmittal, beginning in the early 1960s. There is a huge amount of EFT world wide among and between banks. The U.S. Treasury estimates the figure to be \$2 trillion/day or \$700 trillion/year. A significant part of banking EFT via the SWIFT network is actually carried out via international satellite. Currently, half of the world's 200 countries obtain Internet and "Wide Area Intranet" connection via satellite links. Although these are typically the nations with the most developed economies, this involves a significant amount of digital traffic and E-finance operations. This is a major concern in terms of vulnerability.⁵

Figure 1 illustrates the projected rates of e-financial usage worldwide. By 2005, the share of online banking could rise from 8.5 percent to 50 percent in industrial countries, and from 1 to 10 percent in emerging markets. Online banking transactions with better connectivity in emerging markets could rise even further to 20 percent by 2005. There could be more than 6 trillion dollars of business to business (B2B) transactions online by 2005.⁶

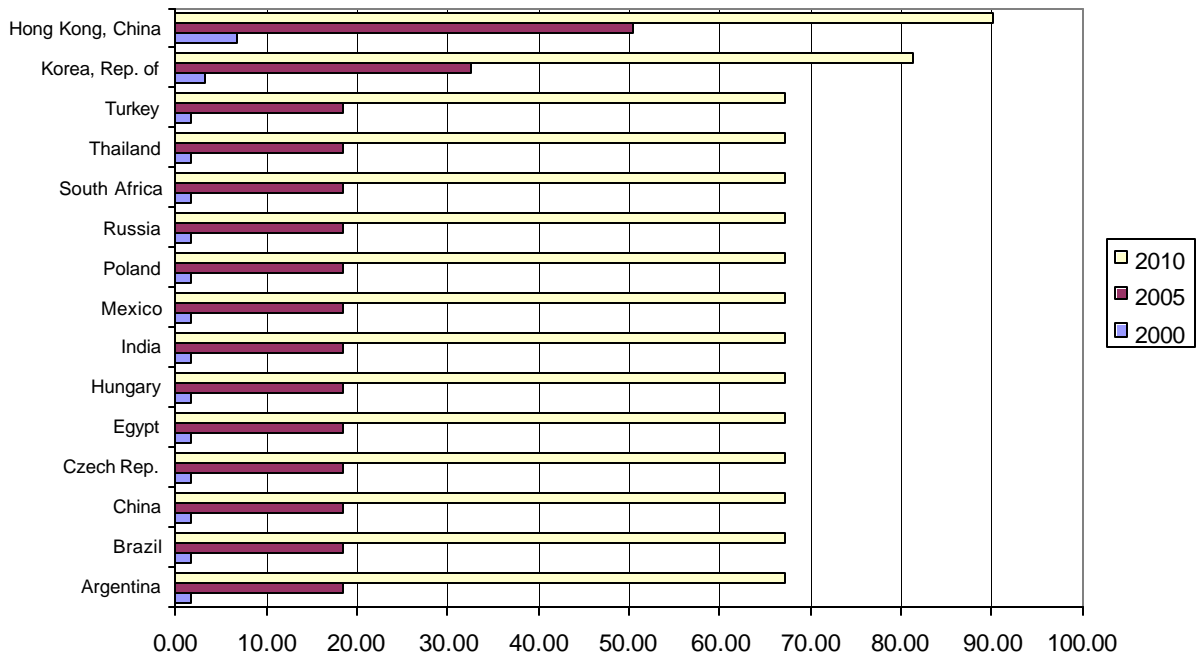
³ Goldman Sachs and Boston Consulting Group Statistics, 2000.

⁴ Gilbride, Edward. *Emerging Bank Technology and the Implications for E-crime Presentation*. September 3, 2001.

⁵ Dr. Joseph N. Pelton, "Satellite Communications 2001: The Transition to Mass-Consumer Markets, Technologies, and Systems".

⁶ Jupiter Communications, 2001.

Figure 1. E-finance Penetration: 2000 and Projected Rates for 2005 and 2010⁷



Source: E-finance in Emerging Markets: Is Leapfrogging Possible? Glaessner, T., S. Claessens, and D. Klingebiel. 2001.

Table 1. Global Mobile Phone Usage

Country	Number of mobile phone subscribers	Percentage of population who are mobile or cellular subscribers
Australia	8,562,000	45%
Brazil	23,188,170	14%
Cambodia	130,547	1%
China	85,260,000	7%
Egypt	1,359,900	2%
Finland	3,728,625	72%
France	29,052,360	49%
Guatemala	696,650	6%
India	3,577,095	< 1%
Indonesia	3,669,327	2%
Republic of Korea	26,816,400	57%
Mexico	14,077,880	14%
Philippines	6,454,359	8%
South Africa	8,308,000	19%
United Kingdom	43,452,000	73%
United States	109,000,000	40%

Source: International Telecommunication Union, *World Telecommunications Indicators Database 2000*.

⁷ The figures show projections based on take-off years with better connectivity. The projections assume in all emerging markets the same connectivity rating as in today's lowest-ranked industrial country, Portugal, 6 (or better if their current rating is already higher); thus the projections lead to the same, minimum level of penetration in each emerging market.

Table 1 illustrates the widespread usage of wireless communications technologies in the developing and developed countries of the world. This relatively new medium is quickly becoming the medium of choice for e-commerce and e-finance. The migration of business from paper-based systems of commerce to Internet-based platforms is profound. As services migrate from these “land lines” to more accessible wireless technologies, the subsequent negative externalities (e.g., war driving) of this phenomenon are beginning to proliferate as well.

Mobile devices are considered to be the developing world’s technological springboard. In 1990, there were just 11 million mobile phone subscribers worldwide. By 1999, the proliferation of wireless technologies had exploded to over 500 million.⁸ Now that number has almost doubled. One developing country typifies the possibilities of leapfrogging⁹ using mobile devices. With a fixed-line network, obliterated after more than 20 years of civil war, Cambodia became connected via the widespread adoption of wireless technology. Within one-year wireless penetration of mobile subscribers outnumbered fixed telephones.¹⁰ Cambodia with one of the world’s lowest per capita incomes surpasses 31 countries in overall telephone penetration, including countries with much higher incomes.¹¹ Rather than spending the vast amount of resources and time to establish fixed-line infrastructure to facilitate telecommunications, countries around the world are substituting hard-wired infrastructure for the relatively cheap and easy to develop cellular towers. There are, however, certain risks related to security associated with such leapfrogging.

Continued economic integration and the new delivery channels for financial services, such as the wireless protocols, will increase opportunities for banks to deliver financial services to remote areas. However, these opportunities are not limited to the formal economy. The underground (criminal) economy of the world have adopted technology as well. Integration of financial services across the wireless medium has created an opportunity for identity theft, fund transfer, and extortion.

II. E-finance on Wireless Networks: The Danger

With the benefits of new technology also come risks. Technology facilitates new methods of fraud and theft. Impersonation, remote access, high quality graphics and printing, and new multipurpose tools and platforms create this cornucopia of crime online.¹² With the spread of dial-up-ATMs that provide customer access to money in underdeveloped locations, criminals can manipulate the wireless connection between the dial-up-ATM and the parent bank, thus compromising all transactions that move in and out of the dial-up-ATM. The art of online penetrations (e.g., hacking) was once a very

⁸ Box 1 of “E-Finance in Emerging Markets: Is Leapfrogging Possible?” Claessens, S, T. Glaessner, D. Klingebiel, 2001.

⁹ Leapfrogging is defined as the phenomenon when developing countries build a hi-tech wireless communications infrastructure rather than undertaking the massive project of creating a fixed-line infrastructure within their borders.

¹⁰ Ibid.

¹¹ Ibid.

¹² Ibid.

skilled and sophisticated trade. The information age has cultivated a breeding ground for underground hacker websites that now supply dubious individuals with the multi-faceted tools necessary to break into financial platforms. Websites like www.astalavista.box.sk and www.attrition.org supply complex malicious code and viruses that allow novice users to penetrate banking systems. The Internet Data Corporation (IDC) recently reported that over 57 percent¹³ of all hack attacks last year were targeted in the financial sector. The traditional risks of yester-year have been reshaped. Historically, frauds were paper based or people based. In the electronic environment there are new opportunities for e-financial crime. In 2001, more than one fourth (27 percent) of banking and financial databases were breached.¹⁴ Table 2 highlights the most notable of electronic attacks in the case of e-financial services and the reported intrusions at various e-commerce and e-financial websites.. Eastern European organized hacker rings have penetrated hundreds of banks worldwide. Hacking has become a business model for organized crime. The FBI's computer crimes division notes that presently many banks are paying off extortion demands for fear of reputation risk and the potential loss of their customer base to competitors. The Egghead hacking incident of last year is a prime example of extortion. Hackers penetrated a database containing 10,000 credit card numbers and then demanded that the company pay them a large sum of cash, in order to protect those numbers from being posted in a chat room. In reality, on Christmas Eve, every one of those compromised cards was charged a minimal sum. Thus the threat goes beyond financial and reputational loss. One forecast suggests that reported incidents of identity theft in the U.S. will more than triple, from \$700,000¹⁵ last year to \$1.7 million in 2005, and the costs to financial institutions will increase 30 percent each year, to more than \$8 billion in 2005.¹⁶

¹³ www.idc.com.

¹⁴ Evans Data Corp. Survey.

¹⁵ This figure represents a yearly trend within the United States of America only.

¹⁶ Published in a 2001 report by Celent Communications. The projections were made using FTC data.

Table 2. Reported E-security Intrusions

<i>Date of Attack</i>	<i>Compromised financial and e-commerce entities</i>	<i>Name of hacker, group, or malicious tool</i>	<i>Various losses sustained due to the intrusion into the financial entity's networks</i>
September 18, 1995	Citibank ¹	Vladimir Levin	\$ 10,000,000 ²
March 1, 2000	UK, U.S., Thailand, and Canada's e-finance and e-commerce sites	Alias "CURADOR"	28,000 accounts compromised with total losses exceeding \$3.5 mln ³
March 15, 2000	Internet Trading Technologies	Abelkader Smires	Denial of Service Attacks which caused major disruption of trading on the NASDAQ
December 22, 2000	EggHead ⁴	Eastern European groups	Hackers compromise database of thousands of credit cards. On Christmas Eve many of the cards were "salami sliced". ⁵
March 8, 2001	40 domestic e-banking and e-commerce sites	Eastern European Criminal Syndicate	Intruders stole credit card account information and other data by exploiting a Windows NT security flaw. The NIPC labeled this attack as the "Largest internet attack to date." ⁶
August 10, 2000	Bloomberg ⁷	Oleg Zesev and Igor Yarimaka	These individuals broke into the Bloomberg computer system in Manhattan in an attempt to extort \$200,000.
April 12, 2001	VISA	Eastern European groups	Intruders gained access to its computer network in the UK and later demanded ransom for data obtained in the virtual break-in. The company received a ransom demand of £10 mln.
June 5, 2001	Central Texas Bank ⁸	Vasily Gorshov and Alexey Ivanov	They had access to the bank's system for six months before they were detected.
July 6, 2001	S1 ⁹	Investigation still ongoing	The compromise of over 300 banks and credit unions whose systems were hosted by S1. ¹⁰
July 14, 2001	Australia's Online Trading Systems	Black Orifice—Trojan Horse	Over 40,000 of their client's account data was compromised.
August 21, 2001	Riggs Bank, First Virginia Banks Inc., SunTrust, and Visa	Investigation still ongoing	Account information of over 4,000 account holders from these banks who utilized Visa Debit cards was compromised. Banks were forced to cancel all debit cards. ¹¹
September 3, 2001	Intrusions into banking and e-commerce sites	Eastern European groups	Various extortions. ¹²
September 20, 2001	Deutsche Bank ¹³	Nimda worm	Costs of breaches indeterminable.
February 7, 2002	U.S. Treasury Direct ¹⁴	Louis Lebaga	\$158 mln. Mr. Lebaga was apprehended only after attempting to steal \$1.3 Billion more five days later.
March 1, 2002	Prudential Insurance Company	Donald McNeese	He was arrested for the theft and credit card scam stemming from the hack of Prudential's database compromising 60,000 personal records of employees there. ¹⁵
April 12, 2002	Republic Bank	Investigation Ongoing	The hacker copied 3,600 bank customer account names and files thus making them vulnerable to ID theft. By exploiting S1's (the hosting company's) servers, he was able to compromise the accounts of these customers. ¹⁶

Notes:

1. "Bank's Security Chains rattled". The Financial Times. Sept. 20, 1995. www.ft.com .
2. Of the \$10 mln lost all but \$400,000 was recovered.
3. National Infrastructure Protection Center, Major Investigations website : www.nipc.gov/investigations/curador.htm
4. Bob Sullivan "Massive Credit Heist, Fraud Reported". Dec. 22, 2001. www.msnbc.com .
5. National Infrastructure Protection Center briefing. August 2001.
6. SANs Institute Alert. March 8, 2001.
7. National Infrastructure Protection Center, Major Investigations website : www.nipc.gov/investigations/bloomberg.htm
8. Predictive Systems "Global E-review". August 2001. www.chron.com/cs/cda/story.hts/metropolitan/929311 .
9. First reported by www.securityfocus.com.
10. A compromise is defined as the access to one's computer systems and databases without their explicit knowledge and consent. S1 had an impressive client list from E*Trade to FleetBoston Financial Corp.
11. Sara Goo of the Washington Post first broke this story. www.idg.net.
12. The FBI's National Infrastructure Protection Center. www.nipc.gov. These intrusions were perpetuated to steal proprietary databases, which were then sent to the heads of these banks with extortion demands.
13. The National Infrastructure Protection Center reported that the worm was distributed from unknown sources and is to have disrupted and infiltrated networks worldwide. www.zdnet.com.
14. John Frazzini, Special Agent, United States Secret Service, Financial Crimes Division.
15. U.S. Department of Justice Press Release. March 1, 2002. www.cybercrime.gov/mcneeseArrest.htm.
16. www.newsbytes.com/news/02/175977.html.

Box 1. Identity Thief

The most infamous of all identity thieves was Abraham Abdallah. In March, when police arrested Brooklyn busboy, Abraham Abdallah, he had Forbes magazine's issue on the 400 richest people in America, plus Social Security numbers, credit-card numbers, bank-account information, and mothers' maiden names of an A list of intended victims drawn from the issue, including Steven Spielberg, Oprah Winfrey, and Martha Stewart. Abdallah is accused of using websites, e-mail, and off-line methods to steal the celebrities' identities and make off with millions in assets. One of his schemes was caught in time. He allegedly sent an e-mail purporting to come from SiebelSystems founder Thomas Siebel to Merrill Lynch, directing that \$10 million be transferred to an off-shore account. In May of 2001, the United States Justice Department issued a statement to a Congressional panel on Internet fraud, that: "Identity theft is the nation's fastest-growing white-collar crime". John Huse Jr., the Social Security Administration's inspector general, testified that the misuse of Social Security numbers in fraudulent activity is a "national crisis. ...the Social Security number wields the power to engage in financial transactions, power to obtain personal information, power to create or commandeer identities which makes it a valuable asset and one that is subject to limitless abuse. About 1,400 times a day — or nearly once a minute — someone's identity is stolen. It's risk-free, why wouldn't criminals do this?"

Trends in cyber-crime reveal significant growth. Attacks on servers doubled in 2001 compared to 2000, and nearly 90 percent of companies surveyed have been infected with worms or viruses despite having anti-virus software installed, according to the Information Security Industry Survey.¹⁷ The 2001 CSI/FBI Computer Crime and Security Survey stated that over \$377 million in total annual losses occurred due to hacking in the U.S. last year.¹⁸

The issue of non-reporting is at the heart of why this serious issue has not been dealt with appropriately worldwide.¹⁹ Financial entities and corporations are fearful of reporting their losses due to the public image ramifications and thus remain complacent to the presence of the threat. If it becomes known that a financial provider has fallen victim to a computer crime or fraud, there is the assumption that their customers will lose confidence in them and their ability to protect information. It's essential for financial service providers to maintain control of their systems mitigate compromises to their security. The wireless medium, which is proliferating worldwide, is not a secure medium. The haste by which countries have adopted wireless platforms for the purposes of e-finance has created a significant quandary.

¹⁷ <http://www.infosecuritymag.com/articles/october01/images/survey.pdf>.

¹⁸ James Savage, Special Agent in Charge, Secret Service, Financial Crimes division, stated that: "This figure represents critical infrastructure losses that the business community is willing to admit having suffered." He suggested that this figure may represent only a minuscule fraction of the actual damage incurred to the U.S. business community. October 3, 2001.

¹⁹ Cornelius Tate, Special Agent, CERT depicted the lack of reporting: "I think the dollar loss is actually higher than what is being reported. In my experience, I see companies not reporting or downplaying their compromises or losses. I think, a lot of the reduced reporting comes down to the company attempting to reduce the "shock" to the stockholders and the public. I think, you will see noticeable increase in the dollar amount from year to year (although the number of respondents remain consistent) because companies are more aware of the fact that everyone is susceptible to being a victim, and to be a victim has become acceptable and does not equate to a loss of 'public confidence.'" (October 4, 2001).

Box 2. Hacker Methods: The Ramifications of a Successful Intrusion

If a hacker compromises an e-financial network, he or she can do the following:

Identity Theft: Once inside the internal network a hacker can copy the database that holds all account information per that bank's clientele. These customers can now have their identities stolen at will, which can be a potential goldmine for the establishment of fraudulent new credit accounts.

Extortion: The most common business model of all, extortion is usually done once a database of customer records has been copied, it is then sent to the banks management with a demand for funds. Most banks pay due to the fear of the reputational losses that would stem from the incident leaking to the media.

Salami Slice: Many hackers are cognizant that the transfer of a vast amount of funds will arise considerable suspicion. For example, once they compromise the customer database, they might charge twelve dollars to "each" account on a later date. With 100,000 charges for \$12, the reward is substantial.

Transfer of Funds: An expert hacker who can manipulate "root kits" and international servers can move money out of banks without leaving an electronic trail.

III. Wireless Local Area Networks (WLANs)

Wireless networks are currently available in three basic formats: wireless LANs (WLANs) using the 802.11b protocol; CDMA/TDMA/GSM (cellular and PCS) networks used for wireless phones and personal digital assistants (PDAs); and high powered microwave systems used by telephone companies for long haul, line-of-sight communications. While all of these are common throughout the world, they all suffer from the same basic security flaw; they use radio frequency (RF) technology to transmit their information. This can result in their transmissions being compromised.

Table 3. The Wide Range of Mobile Services²⁰

Cellular and PCS Services	GSM (TDMA), CDMA, digital cellular, and 3G.
WLANs	The 802.11a and b standards. As well as the new 5.7 GHz wireless LAN band. ²¹
Satellite Systems ²²	Ka-band desk-top services ²³ and the Astra satellite network. ²⁴

Wireless networks (WLANs) have seen explosive growth in their deployment. With cost savings at an all time high and with the simplicity of installation, WLANs have been deployed rapidly, especially by financial institutions. Wireless networks were supposed

²⁰ Provided by Dr. Joseph Pelton.

²¹ The new LAN is now being used for many new applications that involve financial transactions from toll highways in Europe to banking and B2B transactions.

²² These systems provide for both trunk-line Internet transmissions and Digital Video Broadcast services (video streaming and cache updating, as well as direct assess services).

²³ These systems began in Europe.

²⁴ Hughes Spaceway System.

to do what traditional Ethernet LANs do without cables. Convenience for the customer is paramount in the proliferation of wireless. Currently wireless technology is built around the 802.11b IEEE standard in the U.S. and the GSM standard in Europe.²⁵

802.11b Vulnerabilities: An American Phenomenon

Wireless LANs (WLANs) make use of the IEEE 802.11b technology. A system that transmits and receives in the 2.4GHz range and is capable of a maximum network capacity of 11Mbps. WLANs implement the Wireless Equivalent Protocol (WEP), which was designed to offer the same security features as a physical wire: confidentiality, access control, and data integrity. At last year's [Black Hat Briefing](#) (an annual conference for hackers) it became publicly known that there is a multitude of ways in which hackers can crack, intercept, or modify WEP messages on a wireless network. There is a particular problem with devices using the 802.11 wireless network standard. The encryption can be easily broken, and once broken can provide easy access to corporate networks for anyone listening in. Furthermore, if a wireless gateway is located on the corporate Ethernet network, then that network will broadcast all the data passing through it over the airwaves. If someone cracks the encryption, they can intercept everything. But the immediate points of vulnerability are the mobile devices themselves, including notebooks, which tend to be poorly protected and which often contain sensitive but unencrypted data. The danger to financial and corporate networks is very real. The 802.11b standard includes a provision for encryption called WEP (Wired Equivalent Privacy). Depending on the manufacturer and the model of the NIC card and access point, there are two levels of WEP commonly available. One is based on a 40-bit encryption key (also called 64-bit encryption because it uses a 24 bit initialization vector (IV) and considered very insecure), and the other uses a 104-bit key plus the 24-bit IV (also called 128-bit encryption).

A recent technical paper titled "Weakness in the Key Scheduling Algorithm of RC4"²⁶ laid out several fundamental flaws in how the RC4 encryption algorithm was used in the WEP encryption scheme. This paper proposed a method for determining the master WEP key that would allow a hacker to pose as a legitimate user of the network. Shortly after that, a program named AirSnort appeared on the Internet.²⁷ AirSnort takes advantage of the exploit outlined in the above paper and, after monitoring a wireless network for some time, can discover the WEP key. The essential problem with WEP is that the underlying clear text message used to frame the information in the 802.11 header is predictable and repeatable. Given enough cipher text couple with clear text, a cryptographer can find the key.

When designing a wireless network, there are important security concerns one should keep in mind. There are seven basic categories of wireless network security risks:²⁸

²⁵ To be discussed further towards the end of the paper.

²⁶ Scott Fluhrer, Istak Mantin, and Adi Shamir.

²⁷ Input provided by Rick Fleming, VP of Security Operations, Digital Defense, Inc.

²⁸ Chris Bateman of CERT Analysis Center contributed the seven wireless vulnerabilities.

1. **Insertion Attacks** – The intruder attempts to insert traffic into your network, typically through an unsecured mobile access point.
2. **Session Hijacking**—Also known as the man in the middle attack, it is possible to hijack a wireless session based upon the reality that the phone authenticates itself to the base station but not vice versa. It is possible to emulate the base station and thus hijack a phone's session.
3. **Jamming** – This is a DoS (Denial of Service) attack where the attacker tries to flood the radio frequency (RF) spectrum of your wireless network by broadcasting packets at the same frequency as your network.
4. **Encryption Attacks** – The IEEE 802.11b wireless network standard uses an WEP (Wired Equivalent Privacy) encryption method. This standard uses weak encryption and Initialization Vectors (IVs) and has been cracked successfully many times.
5. **Traffic Interception and Monitoring (War Driving)** – Wireless packets using the 802.11b standard have an approximate transmission distance of 300 feet. This means that anyone with the proper standard equipment can receive that signal if they are in transmission range. Equipment to further extend that range is easily available, so the area of interception can be quite large and hard to secure properly.
6. **Mobile Node to Mobile Node** – Most mobile nodes (laptops, PDA's) are able to communicate directly with each other if file sharing or other TCP/IP services are running. This means that any mobile node can transfer a malicious file or program rapidly throughout your network.
7. **Configuration Issues** – Any wireless device, service, or application that is not correctly configured before installation and use can leave an entire network at risk. Most wireless devices and applications are pre-configured to accept any request for services or access. This means any passing mobile client can request and receive telnet sessions or ftp.
8. **Brute Force Attacks** – Most wireless access points use a shared password or key for all devices on that network. This makes wireless access points vulnerable to brute force dictionary attacks against passwords.

War driving

Industrial espionage and white-collar crime has reached new heights with the advance of new technologies. War dialing, the hacking practice of phoning up every extension of a corporate phone network until the number associated with the firm's modem bank is hit upon, has been replaced by *war driving*. War driving involves motoring targeted financial institutions and corporate headquarters with a laptop fitted with a WLAN card and trying to record network traffic (sniffing). According to Dave Thomas, the Chief Investigator of the FBI Computer Crimes Division, war driving is a widespread phenomenon that jeopardizes the security of all institutions and corporations who implement WLANs.

When testing and deploying WLANs, a network administrator may find that their laptops can only connect to the access points within a certain distance and therefore assume that the signals don't travel beyond this point. This is a flawed assumption. In fact, these

signals may travel for a several thousand meters given there is nothing in the way to deflect or interrupt the signal. The reason for this misconception is that the small antennae in the laptops cannot detect the weaker signals. However, using external antennae, the range can be vastly extended. The wireless segment is usually omnidirectional so a potential adversary need not gain physical access to the segment to sniff (or record) the packet traffic. As a result WLANs are susceptible to message interception, alteration, and jamming.

The above considerations raise the issue of how to better secure wireless networks. This will be as critical as securing fixed-line Internet systems in the emerging markets as highlighted above. Each of these security breaches and associated risks can be minimized or negated with the proper use of security policy and practices, network design, system security applications, and the correct configuration of security controls.

15 Steps to Securing WLANs

Wireless network security is much like the physical security at the entrance of a building. Someone with enough interest, resources, and time is going to be able to gain access. First and foremost, it is important to treat your wireless network as though it were a publicly accessible network. A system administrator should not make any assumptions that his or her traffic on that network is private and secure.

The following security recommendations, compiled from a host of industry leaders, will provide some simple rules of thumb that can provide a foundation for securing a WLAN:

1. **Create an institution wide policy regarding wireless devices.** Tailor the corporate security policy to address network usage guidelines.
2. **Track how many employees have WLANs at home.** These remote access users need to be monitored, in order to eliminate unauthorized wireless access points.
3. **Define an account provisioning process to securely manage client's accounts which includes tokens.**
4. **Disable all unneeded services and applications on each client and server.** Typically, all services and applications that are not known or in use should *be disabled*.
5. **Change the default settings of your product.** Many administrators make the mistake of not changing any of the SSID or IP address information for their access points. Don't change the SSID to reflect your company's name, divisions, or products. Since this information is broadcast by the access point, once the hacker has broken WEP, they know exactly whose network they are accessing.
6. **Change the default password on your access point or wireless router.** Hackers often know the manufacturers' default passwords, and will try them first.
7. **Plan your coverage to radiate out to the windows, but not beyond.** As you do your site survey for access point deployment, think about locating the access points toward the center of your building rather than near the windows. If the access points are located near the windows, a stronger signal will be radiated outside your building making it easier for people to find you.

8. **Provide directional antennas for wireless devices.** Most wireless devices utilize omni-directional antennas, these antennae allow for systematic “sniffing” (recording) of all communications. Directional antennas coupled with a 2.4 Gig or higher frequency will lessen the propagation of the signal.
9. **Turn WEP on** and manage your WEP key by changing the default key and subsequently, changing the WEP key on a weekly basis.²⁹
10. **Use VPN tunneling between the network firewall and the wireless.** Though it would require a VPN server, the VPN client is already included in many operating systems such as Windows 98 Second Edition, Windows 2000, and Windows XP.
11. **Deploy a network based intrusion detection system (NIDS) on the wireless network.**³⁰
12. **Deploy enterprise-wide anti-virus software on all wireless clients.**
13. **Employ two-factor authentication.** There are two ways in which two-factor authentication is best employed. First, token-based smart cards that store a biometric record.³¹ The two-factor approach mitigates a tremendous amount of risk. Second, the use of Radius Servers, which authenticate the machine to the network. A Radius server permits association with your access points. A user connects to the radius server merely for authentication to the other servers. One can implement a biometric to initialize the server thus abiding by the two-factor authentication mantra. Radius servers³² act as a guard would in a lobby, authorizing passage to the rest of the building.
14. **Consider using a Wireless Firewall Gateway.**³³ This device operates as a standard dual-homed firewall with the wireless network on one side and the trusted network on the other. The firewall has security software such as IPSEC or some other VPN enabled and only after authenticating to that software can access be granted to the internal network. The firewall rules may also be used to limit where traffic originating from wireless networks may traverse. Make sure that the network firewall is between all wireless access points and the internal network or Internet.
15. **Disable DHCP and use static IP addresses for your wireless NICs.**³⁴ Also change the default IP address range for your wireless network from the manufacturers default.
16. **Purchase access points that have “flashable” firmware only.** There are a number of security enhancements that are being developed, and you want to be sure that you can upgrade your access point.

²⁹ Input provided by the NIPC <http://www.nipc.gov/publications/nipcpub/bestpract.html>.

³⁰ Input provided by Chris Bateman of CERT Analysis Center.

³¹ Bateman recommends the e-thenticator, which is a thumb print biometric scanner that stores the image on a smart card.

³² RADIUS or Remote Authentication Dial-In User Service is an authentication service that verifies user information and once verified, allows users to access certain network services. Part of what RADIUS can provide is encrypted communication between the remote client and the RADIUS server. Virtual Private Networks (VPNs) work in a similar manner but tend to operate on a network-to-network connection instead of the remote host to network method of RADIUS. Once the remote computer is authenticated and connected to the internal network via a RADIUS server, it operates as if it were physically located near and connected to the network. In other words, the encryption provided by the RADIUS server is only between the RADIUS server and the client machine, not over the network as a whole. Rick Fleming stated that: “Cisco’s Aeronet Tacacs Server is premier for this service.”

³³ Rick Fleming, VP of Security Operations, Digital Defense, Inc.

³⁴ Ibid.

Proper System Administration and Auditing

The proper administration of a wireless network is one of the main components of achieving reliable security. The system administrator should routinely perform the following tasks:

1. Reconfigure any wireless device from its factory settings before it is deployed on the network. Turn off all unnecessary services.
2. Obtain the latest security fixes from the vendor and install appropriately prior to deployment.
3. Review all firewall logs weekly, and scan critical host logs daily.
4. Review all ACLs and user accounts on a monthly basis. Systems Administrators should remove all access privileges for terminated employees.
5. Scan automatically all downloads, using enterprise anti-virus software.
6. Set password content and length policy to at least ten alpha/numeric characters.
7. Review all IDS logs weekly.
8. Maintain an inventory of all mobile devices.
9. Prohibit all unauthorized wireless devices should be allowed on the network
10. Develop a standard wireless access point configuration, and use it on all nodes.³⁵
11. Change all access point SSIDs (Server Set ID). These are the shared passwords that comes factory-installed on all wireless access points.³⁶
12. Disable SNMP community passwords on all access points.
13. Enable 128-bit WEP encryption.
14. Move or encrypt the SSID password and the WEP key. Most wireless clients store the SSID password and share a WEP key in the Windows registry file.

Also at least bi-annually, a penetration test or risk assessment should be performed. The results should be used to drive new policy, equipment, and network configuration changes. A wireless network is relatively easy to test for vulnerabilities, and a war driving system can identify key security risks cheaply and quickly. A more comprehensive risk assessment methodology named OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is available from the Software Engineering Institute at <http://www.cert.org/octave>. There are several freeware war-driving software packages available now (AirSNORT), and several made by wireless technology companies (e.g., IBM's WSA) that will provide the organization with a solid picture of the network's vulnerabilities.³⁷

IV. The European Cellular Standard: GSM

GSM is the world's most widely deployed and fastest growing digital cellular standard. Currently, there are nearly 600 million GSM subscribers worldwide, more than two thirds of the world's digital mobile population. And this figure is increasing by four new users

³⁵ Contributed by Chris Bateman of CERT.

³⁶ Ibid.

³⁷ Ibid.

per second. GSM covers every continent, being the technology of choice for 400 operators in over 170 countries.³⁸ But this is only the beginning of the wireless revolution. The industry predicts that there will be over 1.4 billion GSM customers by the end of 2005.³⁹

GSM phones have a small smart card inside them, which holds the identity of the cell phone. This small smart card is called Subscriber Identification Module (SIM). The SIM must keep the identity inside secret and uses cryptography to protect it.

The North American GSM system currently operates at 1900mhz in conjunction with digital PCS services. The data services associated with GSM are Short Message Service (SMS), Analog Cellular Switched Data (CSD), and General Packet Radio Service (GPRS).⁴⁰ Most of European Cellular Carriers use a form of GSM, in either 900mhz or 1800mhz.⁴¹ Europeans also have the option of using High Speed Circuit Switched Data (HSCSD), which combines several channels into a single channel capable of 38.4 KBPS. GPRS is also available in most countries.⁴²

GSM Vulnerabilities

The SIM Card Vulnerability

In both European and American GSM systems, the network access method is the same. Removable smart cards in the phone (SIM cards) are used to store phone numbers, account information, and additional software such as wireless web browsers. The data on the cards are encrypted, but the COMP128 algorithm that protects the information on the card has been compromised, thus making these cards susceptible to duplication. War driving is not a substantial issue for cellular subscribers utilizing GSM. Regardless of frequency, cellular signals can easily be jammed. There is a widely known method for recovering the key for an encrypted GSM conversation in less than a second using a PC with 128 MB of RAM and 73 GB of hard drive space.

The security of GSM phone technology is circumspect. It is possible to clone GSM SIM cards. The hack attack is possible because critical algorithms are flawed making it possible to dump the contents of the SIM cards and then emulate them using a PC.⁴³ This latest problem could render GSM phone conversations totally insecure. For a bank there are other issues. For example, a remote teller machine could be tricked into communicating with a fake mobile tower because it cannot reach a real one. This would allow the perpetrator to remotely control the transmissions of funds via the teller machine. (See Figure 2.)

³⁸ ETSI (European Telecommunications Standards Institute)
<http://www.etsi.org/search/frameset/home.htm?CiScope=%2F&CiMaxRecordsPerPage=10&TemplateName=query&CiSort=rank%5Bd%5D&HTMLQueryForm=search.htm&UserRestriction=GSM>

³⁹ Ibid.

⁴⁰ Input provided by Rick Fleming VP of Security Operations, Digital Defense, Inc.

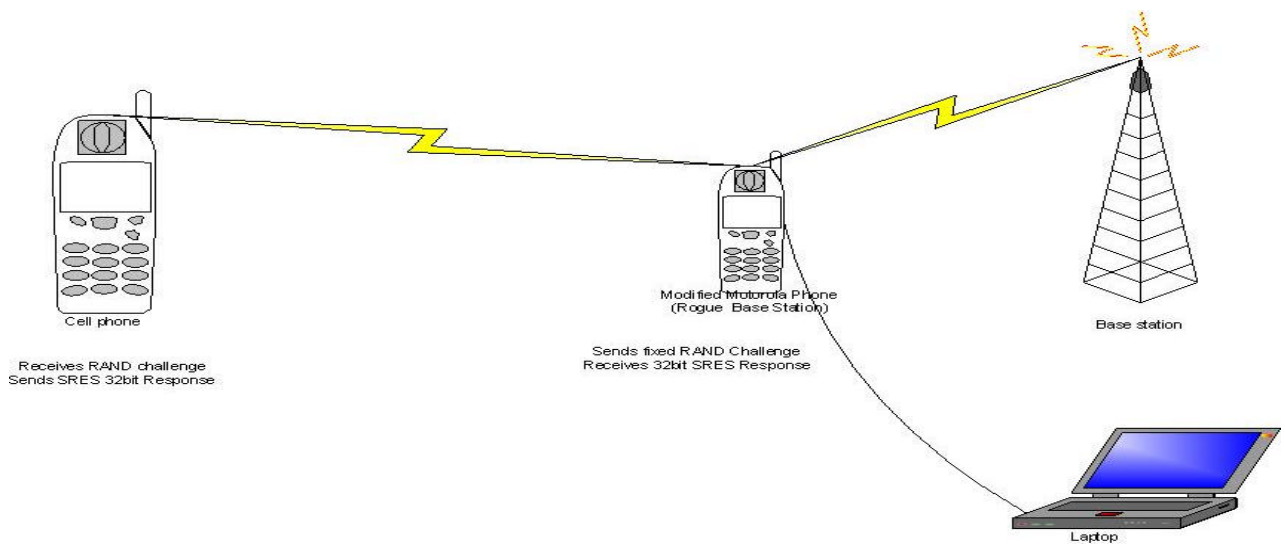
⁴¹ Ibid.

⁴² Ibid.

⁴³ Marc Briceno GSM Cloning <http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html>.

In Figure 2, below, a modified GSM cell phone and laptop are being made to act as a base station. All that is necessary is a few software and hardware modifications to the phone, and being within closer range than the actual tower. The mobile phone must authenticate itself to the base station, but the station doesn't have to authenticate to the phone at all. To eliminate the unknown variables, a fixed RAND challenge is sent out to all mobile phones in range. The received response(s) are the SRES and IMSI. These are recorded and used later, along with the COMP 128 algorithm, to derive the shared secret key K that is used. This key is then copied to a smart card and can be used to act as a person or to eavesdrop on a person.

Figure 2. A GSM Hack⁴⁴



The SMS Vulnerability⁴⁵

GSM offers Short Message Services (SMS). SMS is used in GSM systems for many reasons, such as voicemail notification, updating the subscriber's SIM, sending short text messages, and communicating with email gateways. Whereas these services are convenient, they pose an additional risk to the security of the network. SMS is a store and forward service that is inherently insecure because the messages that are transmitted in clear text and subsequently stored in clear text at the SMS center before being forwarded to their intended recipients. SMS also suffers from latency problems. Time critical transactions should not rely on this channel. There is freely available software that can spoof SMS messages, send SMS bombs both to handsets and SMS gateways (used to communicate between devices both on and off the network), and corrupt SMS packets that can crash the software on most handsets.

⁴⁴ Contributed by Rick Fleming, VP of Security Operations, Digital Defense, Inc.

⁴⁵ Ibid.

SIM Toolkit technology (STK) can be used to provide encryption security through the SMS channel. However, this is a transport layer security mechanism, and it does not provide end-to-end confidentiality for the customer PIN. Additional procedures for improving SMS security might include customers checking their personal assurance messages and the service provider, in turn, verifying the registered phone numbers of customers.⁴⁶

The GPRS Vulnerability

General Packet Radio Service (GPRS) is an IP packet-based service that allows an always-on connection to the Internet. The main problem with this is that it still relies on SMS for WAP push requests.⁴⁷ A spoofed (cloned) SMS packet can be sent to the phone requesting a redirected site and fooling users into entering their information into what they believe is a secure order form, but is really a fake site. Many GPRS enabled phones also support Bluetooth.⁴⁸ Each Bluetooth device has a unique address, allowing users to have some trust in the person at the other end of the transmission. Once this ID is associated with a person, by tracking the unscrambled address sent with each message, individuals can be traced and their activities easily logged. For Bluetooth devices to communicate, an initialization process uses a PIN for authentication. While some devices will allow you to punch in an ID number, you can also store a PIN in the device's memory or on a hard disk. This is highly problematic if the physical security of the device cannot be guaranteed. Also most PINs use four digits and half the time they are "0000."

The security of Bluetooth is based on keeping the encryption key a secret shared only between participants in the network. But imagine you and I are having a conversation using our Bluetooth cell phones. To keep the conversation secure, I use your secret key to encrypt his/her information. Later that day, a friend calls you again and you use your key. Knowing your key, I can use a faked device address, determine the encryption, and listen to your phone conversations. I could also masquerade as you or your friend. Bluetooth only authenticates devices, not users.

WAP Weaknesses

The common flaw in any of these devices, no matter what network, is the Wireless Application Protocol standard, which also includes Wireless Markup Language (WML) and Handheld Device Markup Language (HDML). For the sake of convenience, developers try to require the least amount of keystrokes when entering in credit card number, personal, or account information. This means that most of this information is still stored on a server, but the password to access that server is stored in a cookie on the handheld device, requiring only a PIN or sometimes nothing at all to shop online or transfer funds. This leaves the actual mechanism used to transport sensitive information

⁴⁶ Input provided by Tony Chew, Director, Technology Risk Supervision, Monetary Authority of Singapore.

⁴⁷ Ibid.

⁴⁸ IBM's wireless programming language.

end to end in these un-trusted public cellular networks, which is left to Wireless Transport Layer Security (WTLS).⁴⁹ Unless 128 bit SSL for mobile commerce or IPSEC for Enterprise access is being used (which most handsets can't support due to lack of processing power and bandwidth), there will be a weak link somewhere in the network that can be exploited. Even then, this only pushes the weakness out to the end devices that are communicating, and can be easily lost. GSM uses the Wired Application Protocol (WAP) and also the Wireless Transport Layer Security (WTLS). This is equal to Secure Socket Layer (SSL) but has weaker encryption algorithms. WTLS is not compatible with SSL, which is the industry standard. Wireless messages travel through a "gateway",⁵⁰ which channels them to a wired network for retransmission to their ultimate destination. At the gateway the WTLS message is converted to SSL. For a few seconds, the message is unencrypted inside the gateway, which in turn makes the communication vulnerable to interception.⁵¹

V. Security Solutions for GSM

The inherent problems affecting GSM are not easily corrected. The telephones and PDA's that utilize GSM technology typically cannot upload protective firmware and software. Users are at the mercy of the telephone developer. Whereas GSM is not vulnerable to war driving like its American counterpart, 802.11, it is suffering from four core vulnerabilities. The 802.11 standard is geared towards computers not hand-helds and thus security can be improved much more drastically for 802.11 than for the GSM protocol. Virtual Private Networks are the common thread between the two. The establishment of VPNs is commonly referred to as the solution for the existing vulnerabilities of GSM and 802.11. However when it comes to proper layered security there are no magic bullets.

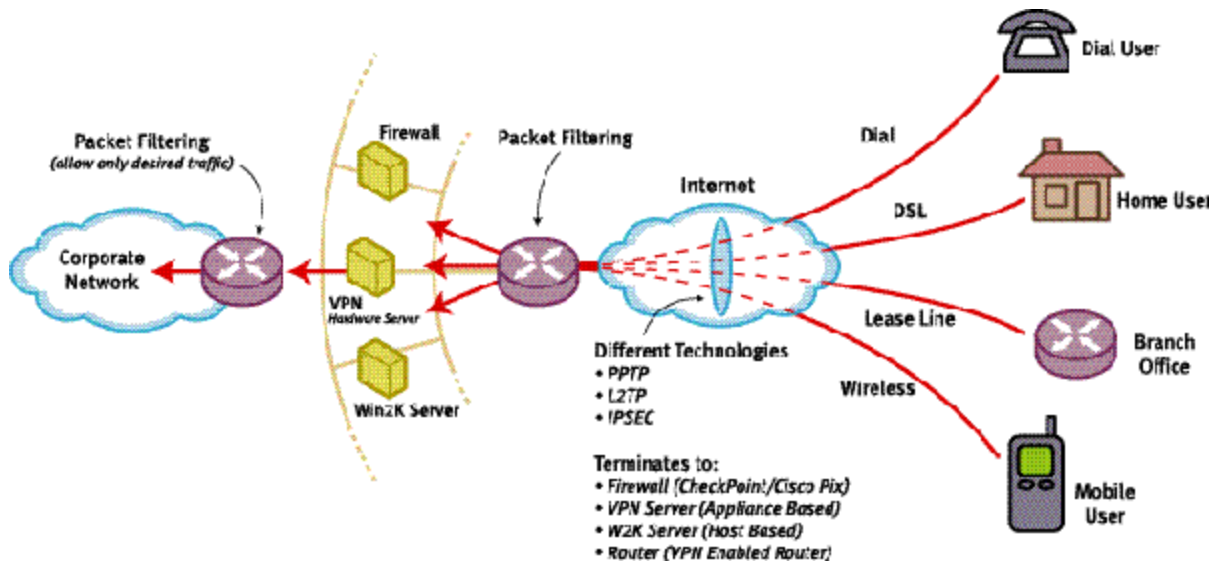
⁴⁹ In his paper *Attacks against the WAP WTLS Protocol* Saarinen describes in detail a number of security problems with WTLS. Although the WTLS protocol is closely modeled on the well-studied TLS protocol, a number of security problems have been identified with WTLS. These problems include: vulnerability to datagram truncation attack, message forgery attack, and a key-search shortcut for some exportable keys.

⁵⁰ A gateway is a device that translates the WAP to LAN, from wired to fixed-line communication. Hackers have cracked the security for gateways.

⁵¹ Input provided by Dave Thomas, Chief Investigator for the NIPC.

Virtual Private Networks

Figure 3. VPN Diagram



Source: Linda McCarthy, VP of Systems Engineering at Recourse Technologies.

To protect information systems that may use any of these technologies, users should deploy Virtual Private Network (VPN) technology at each and every trusted gateway into their networks and ensure that every user accessing the trusted network uses VPN technology. A virtual private network is essentially a private connection between two machines that sends private data traffic over a shared or public network, the Internet. VPN technology lets an organization securely extend its network services over the Internet to remote users, branch offices, and partner companies. In other words, VPNs turn the Internet into a simulated private wide area network (WAN). VPNs allow remote workers access their companies' servers.

To use the Internet as a private wide area network, organizations may have to overcome two main hurdles. First, networks often communicate using a variety of protocols; VPNs provide a way to pass non-IP protocols from one network to another. Second, data packets traveling the Internet are transported in clear text. Consequently, anyone who can see Internet traffic can also read the data contained in the packets. This is clearly a problem if banks desire to use the Internet to pass important, confidential business information. VPNs overcome these obstacles by using a strategy called tunneling. Instead of packets crossing the Internet out in the open, data packets are first encrypted for security, and then encapsulated in an IP package by the VPN and tunneled through the Internet.

Many vendors such as Nokia, Cisco, Nortel, Checkpoint, and Microsoft among others have viable, secure VPN technologies⁵² that can be deployed at multiple locations in a corporate network. While VPNs provide content protection for that information traversing the network, depending on how they are deployed, they may not provide any protection from extraneous users accessing the network itself. In other words, an unauthorized user may not be able to see the content because of the VPN, but they can still access the network resources and utilize the bandwidth causing network congestion and possibly denial of service to authorized users. Access control, authentication, and encryption are vital elements of a secure connection. The Point-to-Point Protocol (PPP) has long been used as the Internet's universal link layer for creating tunnel links between devices, but in more recent years, the Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) have prevailed.⁵³

VI. Banking Security Practices⁵⁴

As a result of the widespread usage of GSM for the delivery of e-financial services, there are certain control and security standards that financial providers should adhere to when providing wireless access to payment systems.

Payments through Third Parties

As a general rule, banks should directly authenticate their own customers in respect of the wireless payment transactions made. Customers may, however give their banks specific standing authorizations to accept payment debits from specified providers or third parties to charge the customers' accounts. Such arrangements could, for example, be made through Direct Debit Authorization agreements. However, when operating under these arrangements, third parties should neither obtain nor store the customers' personal banking IDs or PINs for the purpose of raising debit transactions against the customers' bank accounts.

Stored Value Accounts (SVA)

SVAs are utilized by customers who transfer funds into these accounts for the purpose of making periodic payments. SVAs may reside in mobile devices. No bank account should be accessed in making a payment. Bank accounts should be used only for replenishing SVAs at the customer's direction.

⁵² The standards for VPN are currently in revision by the IETF to make IP Sec more secure, but also make it compatible with satellite communications.

⁵³ Karen Bannan's article "Safe Passage" in PC Magazine reviews seven VPN providers for products that would suit a medium-size business with a budget of \$10,000 that needed a VPN for its central and branch offices.
http://www.pcmag.com/print_article/0,3048,a%3D12352,00.asp

⁵⁴ Section provided by Tony Chew, Director, Technology and Risk Supervision of the Monetary Authority of Singapore.

Close Proximity Wireless Payments

Close proximity wireless payment services are typically intended for over-the-counter retail payments. Such transactions should be completed only after customers have given explicit authorizations at points-of-sale. In the absence of such authorizations, it is possible that customer's funds may be involuntarily deducted from their SVA. Thus, explicit authorization should be mandatory for any payment request.

Interactive Voice Response (IVR)

Mobile IVR services are vulnerable to eavesdropping through the interception of calls. IVR systems should not be used for high-risk and/or value services. All IVR sessions should be recorded including the caller's phone number, the sequence of transactions made by a customer. Pin or authentication data should **not** be logged.

Customer Education

Banks should educate the consumer of mobile e-financial services in the following ways:

- Customers should be advised to use different PINs for different online services.
- Instructions should be provided to customers on how to configure their mobile devices to access mobile banking and payment applications in a safe manner.
- Customers should be advised as to the appropriate dispute handling, reporting procedures, and the expected time for resolution of complaints.

A View into the Future: 3G Technology

3G signifies third generation of wireless communication technology. It refers to pending improvements in wireless data and voice communications through any of a variety of proposed standards. The immediate goal is to raise transmission speeds from 9.5K to 2M bit/sec. In systems and communications security the goal is not to design a flawless system, but a system that can adapt to security enhancements as the need for them is identified. Several of the attacks that were possible on 2G and 2.5G networks have been addressed and eliminated in the 3G environment.

The Strengths of 3G's Security Structure

3G security was based on GSM security, with the following important changes:⁵⁵

- A change was made to defeat the false base station attack. The security mechanisms include a sequence number that ensures that the mobile can identify the network.
- Key lengths were increased to allow for the possibility of stronger algorithms for encryption and integrity.
- Mechanisms were included to support security within and between networks.

⁵⁵ The evaluation of relevant strengths and weaknesses associated with 3G technology was provided by Rick Fleming.

- Security is based within the switch rather than the base station as in GSM. Therefore, links are protected between the base station and switch.
- Integrity mechanisms for the terminal identity (IMEI) have been designed in from the start, rather than that introduced late into GSM.
- The authentication algorithm has not been defined, but guidance on choice will be given.
- When roaming between networks, such as between a GSM and 3GPP, only the level of protection supported by the smart card will apply. Therefore, a GSM smart card will not be protected against the false base station attack when in a 3GPP network.

The 3G system is far more secure than her GSM counterpart. That being said, the ingenuity of nefarious individuals should never be underestimated. Given this, there are certain attacks that are theoretically possible on a 3G network. They are described below.

Camping on a False Base Station

An attack that requires a modified Base Station / Mobile Station (BS/MS) and exploits the weakness that a user can be enticed to camp on a false base station. A false BS/MS can act as a repeater for some time and can relay some requests in between the network and the target user, but subsequently modify or ignore certain service requests and/or paging messages related to the target user.

The security architecture does not prevent a false BS/MS relaying messages between the network and the target user, neither does it prevent the false BS/MS ignoring certain service requests and/or paging requests. Integrity protection of critical message may however help to prevent some denial of service attacks, which are induced by modifying certain messages. Again, the denial of service in this case only persists for as long as the attacker is active unlike the above attacks, which persist beyond the moment where intervention by the attacker stops. These attacks are comparable to radio jamming which is very difficult to counteract effectively in any radio system.

Forcing Unencrypted Communications

This attack requires a modified BS/MS. While the target user camps on the false base station, the intruder pages the target user for an incoming call. The user then initiates the call set-up procedure, which the intruder allows to occur between the serving network and the target user, modifying the signaling elements such that for the serving network it appears as if the target user wants not enable encryption. After authentication the intruder cuts the connection with the target user, and subsequently uses the connection with the network to make fraudulent calls on the target user's subscription.

Integrity protection of critical signaling messages protects against this attack. More specifically, data authentication and replay inhibition of the connection set-up request allows the serving network to verify that the request is legitimate. In addition, periodic integrity protected messages during a connection helps protect against hijacking of

unenciphered connections after the initial connection establishment. However, hijacking the channel between periodic integrity protection messages is still possible, although this may be of limited use to attackers. In general, connections with ciphering disabled will always be vulnerable to some degree of channel hijacking.

Again it should be pointed out that these attack profiles are theoretical in nature based on an understanding of how the technology will be deployed. All in all, 3G systems have enhanced and improved security technology in place, but continued vigilance is necessary to maintain their security to set-up a mobile originated call.

VII. Conclusion

The most distributed networks are the most vulnerable to interception and unauthorized access. There is often maximum vulnerability to interception at the point where there is interconnection between fiber, coax, satellite, and terrestrial wireless systems. Air interface standards are but one example where modern telecommunications and IT systems are open to interception. The market has followed the trend of the so-called Pelton Merge⁵⁶ that calls for continued improvement of “seamless interface standards” that allows the smooth interconnection of fiber, coax, terrestrial wireless, satellites, and other new and evolving technologies, such as high altitude platforms. The challenge is to develop standards that allow easy and reliable interconnection and also protect security. One possible solution might be to re-examine the ISO seven layer model of telecommunications and, in particular, to consider the creation of a new layer that provides truly secure based on a 256 or even 1024 bit code that is constantly updateable.⁵⁷ Further study would need to be given to whether the ultimate solution is a separate layer or the re-engineering of part of an existing layer that could be devoted to this task. Nonetheless, the risks associated with e-finance are great.

The confidentiality and integrity threat posed by the GSM and 802.11 protocols can be mitigated to an extent. Beyond the use of VPNs, the protection of the gateway and the correspondent servers is essential. It is important for banking institutions to comprehend the various methods that may help to protect the network resources themselves while the VPN technology protects the authorized payload. Annex 1 of a forthcoming paper discusses the 10 essential layers of e-security in greater detail. Banks and their correspondent telecom partners should begin to institute proper layered security measures particularly at the “gateway” level. Mitigation of the risk associated with mobile communications will become more critical as commerce and finance increasingly are conducted over what amount to vulnerable, integrated technologies. The widespread adoption of WLANs and GSM technologies by financial institutions around the world has weakened the security of the payment system. These porous mediums were not developed for the movement of digital assets. As the apparent trends of e-finance continue, “mobile risk management” is going to become increasingly more important to the banking industry in the years ahead.

⁵⁶ Contributed by Dr. Pelton, Executive Director of the Clarke Institute.

⁵⁷ Contributed by Dr. Pelton, Executive Director of the Clarke Institute.

E-security Glossary

Access Control: A set of procedures performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access.

Audit: The independent collection of records to assess their veracity and completeness.

Audit Trail: An audit trail may be on paper or on disk. In computer security systems, a chronological record of when users log in, how long they are engaged in various activities, what they were doing, whether any actual or attempted security violations occurred.

Authenticate: In networking, to establish the validity of a user or an object (i.e., communications server).

Authentication: The process of establishing the legitimacy of a node or user before allowing access to requested information. During the process, the user enters a name or account number (identification) and password (authentication).

CERT: The Computer Emergency Response Team was established at Carnegie-Mellon University after the 1988 Internet worm attack named Morris.

Data Encryption Standard: An encryption standard developed by IBM and then tested and adopted by the National Bureau of Standards. Published in 1977, the DES standard has proven itself over nearly 20 years of use in both government and private sectors.

Decode: Conversion of encoded text to plain text through the use of a code.

Decrypt: Conversion of either encoded or enciphered text into plain text.

Dedicated: A special purpose device. Although it is capable of performing other duties, it is assigned to only one.

Encryption: The process of scrambling files or programs, changing one character string to another through an algorithm (such as the DES algorithm).

End-to-End Encryption: Encryption at the point of origin in a network, followed by decryption at the destination.

Extranet: Extranet refers to extending the LAN via remote or Internet access to partners outside your organization such as frequent suppliers and purchasers. Such relationships should be over authenticated link to authorized segments of the LAN and are frequently encrypted for privacy.

Firewall: A system or combination of systems that enforces a boundary between two or more networks.

Gateway: A bridge between two networks.

GSM: **G**lobal **S**ystem for **M**obile **C**ommunications. GSM is an open, non-proprietary system that is constantly evolving. GSM satellite roaming has extended service access to areas where terrestrial coverage is not available.

Hacker: Those nefarious individuals intent upon entering an environment to which they are not entitled entry for whatever purpose Utilizing advanced methodologies and devices to intercept the communications property of another.

Internet: A web of different, intercommunicating networks funded by both commercial and government organizations. The Internet had its roots in early 1969 when the ARPANET was formed. ARPA stands for Advanced Research Projects Agency (which was part of the U.S. Department of Defense). One of the goals of ARPANET was research in distributed computer systems for military purposes. The first configuration involved four computers and was designed to demonstrate the feasibility of building networks using computers dispersed over a wide area. The advent of open networks in the late 1980's required a new model of communications. The amalgamation of many types of systems into mixed environments demanded better translator between these operating systems and a non-proprietary approach to networking in general. Telecommunications Protocol/Internet Protocol (TCP/IP) provided the best solutions to this.

Intrusion Detection System: A system dedicated to the detection of break-ins or break-in attempts either manually via software expert systems that operate on logs or other information available on the network.

Key: In encryption, a key is a sequence of characters used to encode and decode a file. You can enter a key in two formats: alphanumeric and condensed (hexadecimal). In the network access security market, "key" often refers to the "token," or authentication tool, a device utilized to send and receive challenges and responses during the user authentication process. Keys may be small, hand-held hardware devices similar to pocket calculators or credit cards, or they may be loaded onto a PC as copy-protected software.

Local Area Network (LAN): An interconnected system of computers and peripherals, LAN users share data stored on hard disks and can share printers connected to the network.

Logging: The process of storing information about events that occurred on the firewall or network.

NIPC: National Infrastructure Protection Center brings together representatives from U.S. government agencies, state and local governments, and the private sector in a

partnership to protect the nation's critical infrastructures. The NIPC's mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our electronic critical infrastructures.

Policy: Organizational-level rules governing acceptable use of computing resources, security practices, and operational procedures.

Private Key: In encryption, one key (or password) is used to both lock and unlock data. Compare with public key.

Protocols: Agreed-upon methods of communications used by computers.

Remote Access: The hookup of a remote computing device via communications lines such as ordinary phone lines or wide area networks to access network applications and information.

Risk Analysis: The analysis of an organization's information resources, existing controls and computer system vulnerabilities. It establishes a potential level of damage in dollars and/or other assets.

Salami Slice: A hacker method for the acquisition of funds. A database of account information is copied. Then on a later date all accounts are charged a minimal amount, so as not to arouse suspicion.

Server: The control computer on a local area network that controls software access to workstations, printers and other parts of the network.

Two-Factor Authentication: Two-factor authentication is based on something a user knows (factor one) plus something the user has (factor two). In order to access a network, the user must have both "factors," just as he/she must have an ATM card and a Personal Identification Number (PIN) to retrieve money from a bank account. In order to be authenticated during the challenge/response process, users must have this specific (private) information.

VPN: A Virtual Private Network a private connection between two machines that sends private data traffic over a shared or public network, the Internet. VPN technology lets an organization securely extend its network services over the Internet to remote users, branch offices, and partner companies.

WEP: Wireless Equivalent Protocol. It was designed to be implemented over WLANs to offer the same security features as a physical wire: confidentiality, access control, and data integrity.

WLAN: Wireless Networks that correspond to wireless laptops.