11

Network Security

Security companies all over the world are locked in a race with malicious hackers to see who can react fastest to news of a new vulnerability. Increasingly, even the vandals are becoming more sophisticated. It is worth noting that net attacks are growing at the rate of 64 per cent per year. The year 2002 saw an enormous increase in such attacks. Every week, companies were attacked almost 32 times compared to 25 times per week in 2001. As if this was not enough, security companies hear about 400–500 new viruses every month and 250 vulnerabilities of computer programs. In fact, the losses suffered by these organizations are huge. The Computer Security Institute and the US Federal bureau of Investigation (FBI) computer crime and security survey shows that financial institutions are being continuously targeted and are not experiencing the scattergun approach. The survey also shows that more than 90 per cent of websites were attacked, 18 per cent suffered unauthorized access/abuse of their systems and 60 per cent had their sites vandalized. A further 80 per cent had suffered transaction thefts. The financial losses could well be in excess of US$265 million. Of those surveyed, 16 per cent did not even know that they had a problem. Many employees who are familiar with the latest technologies can easily bypass the office systems, effectively, opening the back doors of the organization.

A list of most frequently attacked companies has the power, energy and financial institutions as its major constituents. There is, unfortunately, a tendency on the part of financial institutions to push such attacks or break-ins under the carpet and to prevent any adverse publicity. While the need for not causing an undue panic is appreciated, customers remain vaguely uneasy about such matters. At the cost of repetition, it is maintained that customer anxiety on this point is a major stumbling block in the spread of e-banking. Banks and financial institutions must indicate exactly how they propose to tackle these problems and bring them to the notice of their clients. The time to plug holes is shrinking. In fact if they read the signs on the wall and move quickly, it would offer the Indian financial institutions a unique advantage.

The security concerns depend on the services offered. For the sake of analytical convenience these can be divided into three levels depending on the complexities of services offered. At level 1, the information provided could be tampered with and some data can be distorted. At level 2, the systems are interactive and they provide the ability to transmit sensitive messages, documents or files between users and financial institutions. At level 3, in addition to level 2 operations on the account, bill payments and other transaction services are included. These present a higher degree of risk. The use of an electronic channel to deliver products and services introduces unique risks due to the increased speed at which the systems operate and broad access in terms of geography, user groups and peripheral systems.

Types of Security Failures

The internet economy is built on information. In this economy, time is money and information is valuable. The value of e-finance is defined, in part, by technology's ability to move information and to affect markets quickly. The underlying assumption is that moving information is reliable. Reliability is based, in part, on constructing a system and a process that keeps the percentage of repudiated transactions to a minimum. In order to construct such a system, transactions must be appropriately authenticated, verified and authorized. A precursor to this is access controls. Access controls enable a dumb operating system to know whether an individual attempting to enter the system has been granted access. Authentication is the means used to assure the system that the party attempting to engage in an activity is, in fact, the party so designated. Verification is the means used to confirm that the party claiming a certain identity is the right party. Finally, authorization is the means used to determine that the party engaging in a transaction has the requisite authority to access that portion of the system or to engage in that type of activity. The value of information is based on its reliability and its integrity—whether the party was authorized to access or engage, whether the identity was authenticated, whether there is a risk of non-repudiation, whether there are any process restrictions for the particular transaction (specifically, whether the rules engine has any access controls) and whether there are any relationship constraints (specifically, whether privacy or confidentiality is protected). The process restriction is an internal risk, and the relationship constraint is a potential legal liability. However, the value of any information is directly related to the extent to which the information meets these criteria versus the extent to which it needs to meet this criterion. So, on a scale of 1–10, if the information should be a 10 but the system can only 'assure' a rating of five, it has lost at least 50 per cent of its value. Thus, security is a value-added proposition and is a major business consideration.

Customer interaction with financial institutions is migrating from in person, paper transactions to remote access and transaction initiation. This migration increases the risks of doing business with unauthorized or incorrectly identified parties that could result in financial loss or reputation damage to the institution. Secure electronic service delivery is a key to providing consumers with improved, more flexible and convenient access to financial services and to enhancing the efficiency of banking operations. One of the challenges in implementing secure electronic service delivery is building the appropriate non-repudiation mechanisms into the banking platform. Reliable customer authentication is imperative for financial institutions engaging in any form of electronic banking or commerce. The risks of doing business with unauthorized or incorrectly identified individuals in an e-banking environment could result in financial loss and reputational damage through fraud, corruption of data, unenforceable agreements and the disclosure of confidential information.

In a world where people increasingly do business with virtual parties they have never met and will likely never meet, authentication becomes as integral to the transaction as the exchange of goods and tender. Yet, authentication is the Achilles's heel of electronic finance. In fact, most computer intrusions are perpetuated as a result of insufficient access controls and weak authentication mechanisms. For example, in 1995, Citibank found itself in an ironic position: its technology was not as powerful as that of a group of hackers. Citibank's main weakness was the use of 'fixed passwords' to guard its computerized cash management system. There is widespread concern, especially among those in the law enforcement community that the financial sector is not keeping up with the security side of technological change. For example, overall industry-wide use of passwords is outdated. In fact, a 1999 General Accounting Office (GAO) report highlighted the reality of outdated access controls; it found access controls to be at the forefront of security weaknesses. Beyond the norm of gates and guards that were often inadequate, failures of logical controls—those access controls built into software—were pervasive. In the information age, there are hundreds of websites devoted to password cracking and/or interception. The most common programme used for password generation is Brute Force. This widely available application generates all alphanumeric combinations until the password is deciphered.

Control Devices

There are two issues here: access and authentication. Access allows those who should be able to get onto the system for the purpose for which they are authorized. Authentication is assuring the system that the person trying to gain access or engage in a certain activity is, in fact, the person he or she claims to be and that the person is authorized to engage in the act. Used together and diligently, these processes are the most cost-effective security devices available. Financial institutions can use a variety of access and authentication tools and methodologies to authenticate customers. Existing access control techniques and authentication methodologies involve three basic factors:

- Something the user knows (for example, password or Personal Identification Number [PIN]).
- Something the user possesses (for example, ATM card, smart card or token).
- Something the user is (for example, biometric characteristic, such as fingerprint or retinal pattern).

An effective access and authentication programme should be implemented across the organizational structure, including affiliate entities, which requires the appropriate use of controls and authentication tools. Authentication processes should also maximize interoperability and offer consistency with the financial institution's assessment of the e-finance system risks. Before it goes online, the financial institution should examine its business processes, undergo a data classification inventory as part of its risk management analysis and configure its rules engines and access controls to support the data classifications.

Access Control Using Password and PIN

The entry of a username or an ID and a secret string of characters such as a password or PIN is the most common and vulnerable of all single-factor authentication techniques. The effectiveness of password security depends on three characteristics: length and composition, secrecy and system controls.

Even with these precautions, the inherent weaknesses of passwords are technology and time. As a result of increased processor speeds, patient hackers can acquire an encrypted password file or session. A program named L0ftCrack is a random character generation program that, when used with a 1.8 giga processor, can run 1 million keyboard combinations per second.

The computer will execute L0ftCrack in logical progression, thus making it a matter of time before that terminal is compromised. Note that hackers with criminal intent are patient. It may take months to set-up an attack, but it takes seconds to execute a successful intrusion on a bank. Passwords can be compromised and thus provide no real level of non-repudiation.

Access Control Using Tokens and Smart Cards

A token is an authentication method that makes use of something the user possesses. Typically, a token is a two-factor authentication process, complemented by a password or a biometric as the other factor. The device itself may authenticate static passwords or biometric identifiers used to authenticate the user locally. This process avoids the transmission of shared secrets over an open network. Most so-called 'smart cards' are nothing more than a credit card sized device containing a microchip. The sophistication of the chips varies, but most commercially available implementations are far from being secure. In considering the threat posed by criminals, it is not enough to deter the casual criminal through the inconvenience of basic security. New measures must be able to withstand the continuous and repeated efforts of a determined and well-funded adversary. Standard smart cards usually contain account numbers, encryption keys and often additional stored information (such as biometric profiles), which can be extracted from the card and duplicated or altered. In doing so, the determined adversary can then present cloned or altered data smart cards as genuine, defeating the security and gaining access to critical infrastructure.

Cyoni™ technology is a core authentication system with a wide variety of applications. It is based on the use of mass-producible microchips that can be deployed in a variety of convenient consumer products. Each chip behaves uniquely in response to random or pseudo-random challenges. The system is fundamentally an authentication technology. The primary security advantage of Cyonic™ technology is that no system-level information is contained on the microchip. Thus, even a determined adversary, upon destructive analysis of the chip, will gain no insight into the system-level functions that authenticate system users. This prevents any adversary from achieving successful account cloning, regardless of the adversary's technical or financial resources.

Biometric authentication techniques can grant or deny access to networks by automatically verifying the identity of people through their distinctive physical or behavioural traits. A biometric identifier represents a physical characteristic of the user. The identifier is created from sources such as the user's face or hand geometry, voice, iris (or retina) or fingerprint. Once 'captured', a biometric is translated algorithmically into a complex string of numbers and stored in a database as a template. Later, this template is compared to any 'live' biometric presented as proof of identity. Introducing a biometric method of authentication requires physical contact with each customer to initially capture and validate the biometric information. This corresponds to the 'know thy customer' mantra of the financial action task force principles.

Biometrics is the future of access controls. Biometric devices fulfill the non-repudiation element of layered security by authenticating a user by his or her physical characteristics. Implementing biometric technologies virtually guarantees a system administrator that the person who initiated the communication or system access was who he or she should have been. The greatest obstacle that biometric technology faces lies in the acceptance of the public. Many people fear the ramifications of storing personal information in a vast database. There is an apprehension (fuelled no doubt by books such as *1984* and *Gattaca*) that this might lead to unacceptable centralized control or interference, etc. We must say that not having such controls could lead to far greater risks. The e-financial world must evolve past our fears of 'big brother', in order to face the security challenges that will face all 'virtual' industries in the years to come. Authentication is the gargantuan cyber-loophole that is exploited more often than not in order to gain access to others' computer systems.

Malicious Attacks

Worms, Trojans (the analogy is to the Trojan horse) and viruses are vehicles for deploying an attack. A virus is a program that can replicate itself by infecting other programmes on the same system with copies of itself. Trojans do not replicate or attach themselves to other files. Instead, they are malicious programs that are hidden within another program or file.

Once the Trojan file is executed, it can perform malicious activity at will. Virus scanners are critical in the mitigation of these attacks. Virus scanners should be updated every night. Beginning with an institution's email gateway, every inbound attachment should be scanned for viruses. File servers should be set to active scanning mode, where they scan every file copied onto them. Desktop scanners that protect the user's PC should also be updated. Data should be tested against standard loads if updates catch anything.

Worms, which are a relatively new phenomenon, use existing security vulnerabilities to gain access to the device. Worms replicate themselves onto other systems via a network connection. Typically, viruses and worms become malicious only when the infected files are accessed or deployed. Most of the time, these vulnerabilities can be eliminated by simply applying patches. The irony here is that someone who is not keeping up-to-date with patches most likely is not keeping up-to-date with virus software either. This human 'system' failure can have catastrophic implications for an institution's e-financial network.

Data Transmission Reliability

Cryptography and cryptographic tools sound complex and mysterious. The details of how these tools are constructed and work are intricate, laced both with mathematics and with provable and unprovable properties. The security of some tools can be based firmly upon some intractably difficult mathematical problem. The security of other tools cannot be proven formally, but is trusted as a result of the inability of experts to find and demonstrate any weaknesses in the tools over the years. However, what cryptographic tools do and how they are used are very easy to understand. There are only six basic types of cryptographic tools. They are:

- Symmetric (secret) key encryption.
- Asymmetric (public/private) key encryption.
- One way hash functions.
- Message authentication codes.
- Digital signatures.
- Random number generators.

By careful use of these cryptographic tools one seeks to design systems that can provide system security in the face of any of the attacks defined in an associated threat model.

Asymmetric Key Encryption

For asymmetric key encryption, the key used to encrypt data is a different key from that used to decrypt data. Unlike symmetric key encryption, which uses the same secret key both for encryption and decryption, asymmetric key encryption uses two different keys. Why is this important? It is important because only one of the keys needs to be kept private (or secret). The other key can be made public. It is for this reason that asymmetric key encryption popularly is called 'public/private' key encryption. Asymmetric ciphers greatly facilitate problems of key distribution.

One can appreciate the power of having two keys by considering how one orders items over the internet, such as books from Amazon.com. The ordering process used by such websites uses a protocol called Scare Socket Layer (SSL), to assure that a secure session is established between the customer's computer and the website. An SSL session begins with a 'handshake' protocol. The customer's computer sends a greeting to the Amazon web server, and web server's reply includes a certificate containing an Amazon public key. The customer's computer checks that the certificate is valid and then uses Amazon's public key to encrypt data that both the user's computer and the web server will use to construct a symmetric key for the session. Only the Amazon web server has the private key needed to construct the symmetric session key. After some further checking, the session continues using the symmetric key to encrypt/decrypt messages. The order information—credit card number, shipping address, gift-wrapping, greeting message and items ordered—then can be sent confidentially to Amazon.

The most widely used asymmetric cipher is called 'RSA', an acronym composed of the first letters of the last names of its inventors: Ron Rivest, Adi Shamir and Leonard Adleman, who first published their work in the summer of 1977. Patent protection for the algorithm expired in September 2000 and now it is in the public domain. RSA operates upon very large integers modulo, the product of two secret prime numbers. RSA public and private keys each are pairs of such large integers. For good security today, 1024 to 2048 bit integers are used, although some applications continue to use 512 bit integers. The cryptographic strength of RSA derives from the difficulty in finding the two secret primes given only their product.

Due to the relative strengths and weaknesses of symmetric and asymmetric cryptography, a common practice is to use asymmetric key cryptography for key distribution and symmetric key cryptography for the bulk of the transferred data. This is what is done within the SSL protocol— asymmetric cryptography is used to establish a newly created symmetric key, which then is used for the data transfers within the SSL session.

Use of Random Numbers

Random numbers are employed throughout cryptographic algorithms and protocols. They are used for keys, challenge values, pre-hashing appendages for passwords, and so on. Hardware devices based on some form of physical randomness are also beginning to appear. The problem with such hardware devices, of course, is testing them to assure they are operating correctly.

Sole computational means for generating truly random numbers do not exist. A favourite quote of John Von Neumann's, cited by Bruce Schneier, is: 'Anyone who considers arithmetic methods of producing random digits is, of course, in a state of sin.' Fortunately, computational means do exist for computing numbers that are sufficiently unpredictable that they can be used in lieu of truly random numbers. Such numbers are called 'Pseudo-Random Numbers' (PRNs). Some of the pseudo-random number generation methods employ values obtained by physical measurements of random events in a computer system, such as typing rates, arbitrary mouse motions, arrival times of I/O (an authentication software) interrupts. Others are based on symmetric cryptography or the difficulty of hard mathematical problems such as the factoring problem. Pseudo random number generators (PRNGs) that produce sufficiently unpredictable values are called 'Cryptographically Strong Pseudo Random Number Generators' (CSPRNGs).

It is not easy for banks and financial institutions to safeguard their networks because new vulnerabilities are discovered daily, and their fixes/patches must be diligently applied to all systems. New connections to the internet, modems, and virtual private networks (VPNs) create a multitude of new access points to a network whose risk is defined by its weakest link. Penetration testing entails obtaining knowledge of existing vulnerabilities of a computer system or network, and using that knowledge to attempt to gain access to resources on the computer or network while bypassing normal authentication barriers. It may also include exploiting vulnerabilities to gain increased authorization—for instance, to go from regular user to super-user. Penetration testing is good only on the day it was done (this is true for all security testing). Penetration testing is an excellent way of testing installed security measures, policies and procedures, and the effectiveness of a company's end-user security training programmes. First, a company will be able to tell if security measures such as firewall and

Intrusion Detection System (IDS) are functioning properly and what skill level is required to circumvent them. Second, a company will gain insight into whether established policies and procedures allow its staff to detect and react to an intrusion properly. And third, a company can determine if additional training is required for its end-users. Penetration testing should be performed at least annually and more often if the system is subject to frequent application or operating system updates. Once a penetration test has been performed, ongoing vulnerability assessment should be performed to address newly discovered exploits. The frequency of the vulnerability assessment should be determined on the level of risk an organization is willing to accept. Given the speed at which new vulnerabilities and exploits are discovered, a vulnerability assessment should be performed semiannually and in many cases quarterly no matter what level of risk one is willing to accept.

So far the causes and steps the organizations can take as damage control have been outlined. The next section points out the most frequent lapses which occur and which are within the category of 'controllable' items from an organizational perspective.

Managerial Checklist

Top 20 Red Flags

- Lack of training and expertise of administrators.
- No time for or interest in reviewing log files.
- No time for or interest in hardening machines.
- Deployment of new technology without security peer review.
- Failure to install software patches that fix security flaws.
- Lack of strict requirements to use strong passwords.
- Removal of security mechanisms because they cause user inconvenience. Restoration of systems from backups and failure to reload any patches that were previously installed.
- Failure to remove administrative-level accounts that were added temporarily for service personnel.
- Failure to install or use available security mechanisms such as password policy enforcement or system event logging.
- Lack of daily audit of network logs for suspicious activity.
- Setting up computer systems by using the default software. These default settings are designed to get the system booted up and run with the least interference; often these are very insecure.

- Failure to perform routine backups of systems and then test those backups for viability.
- Failure to properly install and update virus protection software.
- Sharing administrative accounts and passwords over multiple systems.
- Primary reliance on a firewall or public key infrastructure (PKI) system for security.
- Use of Simple Network Management Protocol (SNMP), telenet, file transfer protocol (ftp), mail, rpc, rservices or other unencrypted protocols for managing systems.
- Assignment of passwords to users over the phone.
- Failure to educate users about security problems and what to do when they see a potential problem.
- Poorly written and implemented policies and procedures.
- Improper documentation.

The following are some of the best practices prevalent in the industry.

Best Practices

- Network administrators should be responsible for installing and verifying patches and updates to operating systems weekly.
- On-site trained security staff should be present 24/7.
- Employees should be required to use robust passwords (long in length; mix of letters, numbers and symbols), which should be changed monthly.
- Computer monitors should not be visible to anyone who is not an employee of the institution.
- Network administrators should implement a profile procedure to process transfer of employees to another office in the bank, termination of employees and changing an employee's level of access within the bank's systems.
- Those who are responsible for large value transfers should utilize biometric identifiers as their password.
- Backups should be maintained of all critical material that is stored in a different location.
- An incident response capability and a plan that ensures continuity of operations and recovery from security breaches should be in place.
- Strong authentication—preferably biometrics, smart cards and cryptography—should be exercised for large value transfers.

- Firewalls and intrusion detection systems should be installed.
- Penetration testing/auditing should be performed on all of the institution's systems.
- A login banner should be displayed stating that the system is only for authorized use and is subject to monitoring.
- Patches must be updated weekly to both servers and remote access machines. See http://www.microsoft.com/technet/security/current.asp
- Critical operations should have two-person controls.
- A security policy should be developed that mandates training for non-IT staff vis-a-vis an incident response plan and that prohibits instant messaging, voice-over IP and wireless local area network (WLAN) installation without appropriate authorization and securitization.

Incident Response

The ability to react quickly to security incidents is an essential part of an overall security plan. An organization's ability to operate will depend on its ability to provide timely information to its clients in the form of electronic data. It is also essential to categorize information. Information from critical systems will certainly receive a more direct and focused response than, for example, electronic information stored for office supplies. An organization needs the ability to react to and recover from security incidents as they arise with an effective and coordinated response, which in turn will minimize the cost and damage to the organization's infrastructure and image within the banking industry. A security incident can be defined as an event that changes the security posture of an organization or circumvents security polices developed to prevent financial loss and destruction, theft, or loss of proprietary information. It is characterized by unusual activity that causes the organization to investigate because the activity cannot be explained through normal operations. Some possible classifications for security incidents are:

- Virus attacks (unable to clean, rename or delete).
- Denial of service attacks.
- IDS alert notifications (false positives possible).
- Automated scanning tools.

Banking organizations must share in the responsibility of coordinating their response efforts with those of other financial institutions. Networking in a trusted environment and sharing incident information and detection/response techniques can be important to all of these organizations in identifying and correcting weaknesses. Gathering intelligence information from all sources is a critical part of information infrastructure protection. Having an information-sharing network in place can also help government agencies alert other agencies to potential and/or actual threats directed at the critical information infrastructure of nations.

Incident response within any organization must begin with management. Management is responsible for providing the support, tools, personnel and financial backing needed to ensure the success of the incident response team. An incident response team must be perceived well by all concerned. Security awareness training and briefings for senior management are key components of a successful deployment of an incident response team.

Monitoring systems and reviewing security alert information submitted by vendors is an important part of an incident response team's proactive duty. IDS systems, however, do not provide a complete solution to identifying and responding to incidents. An overall security plan is needed to ensure overall protection that would include an incident response mechanism. An incident response team must also develop procedures. Clear definitions of each type of incident will enable members to react quickly and effectively. Procedures must detail the steps team members should take when alerted about an incident. Included within the procedures must be clearly defined investigative goals to be achieved before an incident can be closed. The team should also list and post contact information of key personnel and management to notify.

Survivable System Development

Survivability analysis or business continuity helps to identify the essential functions or assets in the institution that must survive in the event of an attack or system failure. The delivery of essential services and the preservation of essential assets during a compromise, and the timely recovery of full services and assets following attack are among these functions. The organizational integration phenomenon that typifies the modern banking community is accompanied by elevated risks of intrusion and compromise.

It is essential to determine what elements in the institution's IT infrastructure are absolutely mission-critical—that is, what elements must be up and running within a certain time in order for business to continue. One must envisage various compromises to the system so that contingency plans are there to cover all potential threats. The following sources on survivability will assist network architects in determining the impact of certain accepted risks.

The Carnegie Mellon Software Engineering Institute Network Systems Survivability Program uses incident data collected by the CERT (http://www.cert.org/nav/index_purple.html) as a basis for the institute's survivability research and for trend identification and the prediction of future problems.

The European Dependability Initiative (http://www.cordis.lu/esprit/src/stdepnd.htm) represents a major research effort within the European Union to address the critical infrastructure protection and survivability efforts of the member nations. There are plans for joint US/EU cooperation.

The National Infrastructure Protection Center (NIPC) is the US government's focal point for threat assessment, warning, investigations and response to attacks (http://www.nipc.gov).

E-SECURITY IN THE CASE OF WIRELESS NETWORKS

Wireless networks are available in three basic formats: high-powered microwave systems used by telephone companies for long-haul, line-of-sight communications; Code Division Multiple Access/Time Division Multiple Access/Global System for Mobile Communication (CDMA/TDMA/GSM) cellular and PCs networks used for wireless phones and personal digital assistants (PDAs); and wireless LANs that uses the 802.11b protocol. 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. The result can be compromising of their transmissions. 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. Wireless networks were supposed to do what traditional Ethernet LANs do without cables. Convenience for the customer is paramount in the proliferation of wireless. Wireless technology is built around the 802.11b IEEE standard in the US and the GSM standard in Europe. The next section discusses the security issues raised by both of these forms of cellular technology and provides a glimpse into the future of third generation wireless (3G).

Manager's Laptop—The Big Problem

Wireless LANs make use of the IEEE 802.11b technology, which is 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. 2001's Black Hat Briefing made public that hackers have a multitude of ways in which they can crack, interject 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 easily be broken, and once broken it can provide easy access to corporate networks for anyone listening in. Furthermore, if a wireless gateway is located on the corporate Ethernet network, that network will broadcast all the data passing through it over the airwaves. If someone cracks the encryption, that person 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.

When designing a wireless network, one should keep in mind a number of important security concerns. These are the six basic categories of wireless network security risks:

- **Insertion attacks**—The intruder attempts to insert traffic into your network, typically through an unsecured mobile access point.
- **Jamming**—This is a DoS (denial of service) attack, where the attacker tries to flood the radio frequency spectrum of your wireless network by broadcasting packets at the same frequency as your network.
- **Encryption attacks**—The IEEE 802.11b wireless network standard uses a WEP encryption method. This standard uses weak encryption and initialization vectors and has been cracked successfully many times.
- **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 he or she is in transmission range. Equipment to extend that range further is easily available, so the area of interception can be quite large and hard to secure properly.

- **Mobile node to mobile node**—Most mobile nodes (laptops, PDAs) 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.
- **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 preconfigured to accept any request for services or access. This means any passing mobile client can request and receive telnet sessions or ftp.

War Driving

Industrial espionage and white-collar crime have 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 between 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 that implement WLANs.

When testing and deploying WLANs, a network administrator may find that the institution's laptops can only connect to the access points within a certain distance and may, therefore, assume that the signals do not travel beyond this point. This is a flawed assumption. In fact, these signals may travel for several thousand metres if there is nothing in the way to deflect or interrupt the signal. The reason for this misconception is that the small antennas in the laptops cannot detect the weaker signals. But if external antennas are used, 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. These considerations raise the issue of how to secure wireless networks better. This will be as critical as securing fixed-line internet systems in the emerging markets, as highlighted previously.

Each of these security breaches and associated risks can be minimized or negated with the proper use of security policy and practices, network design and system security applications, and with the correct configuration of security controls.

The European Cellular Standard: GSM

In 1982, the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Groupe Spécial Mobile (GSM) to study and develop a pan-European public land mobile system. Today, GSM is the world's most widely deployed and fastest growing digital cellular standard. GSM subscribers worldwide number nearly 600 million, more than two-thirds of the world's digital mobile population. The numbers are increasing by four new users per second. GSM covers every continent, being the technology of choice for 400 operators in more than 170 countries. However, this is only the beginning of the wireless revolution. The industry predicts more than 1.4 billion GSM customers by the end of 2005. GSM phones have a small smart card inside them that holds the identity of the cell phone. This small smart card is called a Subscriber Identification Module (SIM). The SIM keeps the identity secret and uses cryptography to protect it.

GSM Vulnerabilities

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 is encrypted, but the COMP128 algorithm that protects the information on the card has been compromised, making these cards susceptible to duplication. War driving is not a substantial issue for cellular subscribers using 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 limited. 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.

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. Thus, a modified GSM cell phone and laptop can be made to act as a base station. All that is necessary is to make a few software and hardware modifications to the phone and to be within closer range than the actual tower. The mobile phone must authenticate itself to the base station, but the station does not have to authenticate to the phone at all.

The SMS Vulnerability

Short Message Services (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. Although these services are convenient, they pose an additional risk to the security of the network. There is freely available software that can spoof SMS messages, send SMS bombs to both 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.

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 Wireless Application Protocol (WAP) push requests. A spoofed (cloned) SMS packet can be sent to the phone requesting a redirected site and fooling users into entering their information into a fake site that they believe is a secure order form. Many GPRS-enabled phones also support Bluetooth, IBM's wireless programming language.

Each Bluetooth device has a unique address that allows 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 it is possible to trace individuals and easily log their activities. 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'.

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 credit card number or 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 means that the actual mechanism used to transport sensitive information end-to-end in these untrusted public cellular networks, is left to Wireless Transport Layer Security (WTLS). Unless 128-bit SSL for mobile commerce or IPSEC for Enterprise access is being used, which most handsets cannot support because they lack 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 it can be easily lost. GSM uses the Wired Application Protocol and also the Wireless Transport Layer Security. This is equal to Secure Socket Layer, but it has weaker encryption algorithms. WTLS is not compatible with SSL, which is the industry standard. Wireless messages travel through a 'gateway' that 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.

Security Solutions for GSM

The inherent problems affecting GSM are not easily corrected. The telephones and PDAs that use 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 several core vulnerabilities. The 802.11 standard is geared to computers, not handhelds 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.

To protect information systems that may use any of these technologies, users should deploy virtual private network technology at each and every trusted gateway into their networks and ensure that every user accessing the trusted network uses Virtual Private Network (VPN) technology. A VPN 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 to access their companies' servers.

Sound Practices for Managing Outsourced E-banking Systems and Services

- E-finance organizations should adopt appropriate processes for evaluating decisions to outsource e-finance systems or services.
    - Bank management should clearly identify the strategic purposes, benefits and costs associated with entering into outsourcing arrangements for e-banking with third parties.
    - The decision to outsource a key e-finance function or service should be consistent with the organization's business strategies, should be based on a clearly defined business need and should recognize the specific risks that outsourcing entails.
    - All affected areas of the bank need to understand how the service provider(s) will support the organization's e-finance strategy and fit into its operating structure.
- E-finance companies should conduct appropriate risk analysis and due diligence prior to selecting an e-finance service provider and should continue with it at appropriate intervals thereafter.
    - Organizations should consider developing processes for soliciting proposals from several e-finance service providers and should also develop a criteria for choosing among the various proposals.
    - Once a potential service provider has been identified, the bank should conduct an appropriate due diligence review, including a risk analysis of the service provider's financial strength, reputation, risk management policies and controls, and ability to fulfill its obligations.

  - Thereafter, banks should regularly monitor and, as appropriate, conduct due diligence reviews of the ability of the service provider to fulfill its service and associated risk management obligations throughout the duration of the contract.
  - Banks need to ensure that adequate resources are committed to overseeing outsourcing arrangements supporting e-banking.
  - Responsibilities for overseeing e-finance outsourcing arrangements should be clearly assigned.
  - An appropriate exit strategy for the organization to manage risks should a need to terminate the outsourcing relationship arise.

- Organizations should adopt appropriate procedures for ensuring the adequacy of contracts governing e-finance. Contracts governing outsourced e-finance activities should address, for example, the following:

  - The contractual liabilities of the respective parties as well as responsibilities for making decisions, including any subcontracting of material services are clearly defined.
  - Responsibilities for providing information to and receiving information from the service provider are clearly defined. Information from the service provider should be timely and comprehensive enough to allow the organization to adequately assess service levels and risks. Materiality thresholds and procedures to be used to notify the bank of service disruptions, security breaches and other events that pose a material risk to the bank should be spelt out.
  - Provisions that specifically address insurance coverage, the ownership of the data stored on the service provider's servers or databases and the right of the organization to recover its data upon expiration or termination of the contract, should be clearly defined.
  - Performance expectations, under both normal and contingency circumstances, are defined.
  - Adequate means and guarantees, for instance through audit clauses, are defined to insure that the service provider complies with the bank's policies.
  - Provisions are in place for timely and orderly intervention and rectification in the event of substandard performance by the service provider.

  - For cross-border outsourcing arrangements, determining which country laws and regulations, including those relating to privacy and other customer protections, are applicable.
  - The right of the organization to conduct independent reviews and/or audits of security, internal controls and business continuity and contingency plans, is explicitly defined.

- Organizations should ensure that periodic independent internal and/or external audits are conducted of outsourced operations to at least the same scope required if such operations were conducted in-house.

  - For outsourced relationships involving critical or technologically complex e-banking services/applications, organizations may need to arrange for other periodic reviews to be performed by independent third parties with sufficient technical expertise.

- Organizations should develop appropriate contingency plans for outsourced e-finance activities.

  - E-finance companies need to develop and periodically test their contingency plans for all critical e-banking systems and services that have been outsourced to third parties.
  - Contingency plans should address credible worst-case scenarios for providing continuity of e-banking services in the event of a disruption affecting outsourced operations.
  - Companies should have an identified team that is responsible for managing recovery and assessing the financial impact of a disruption in outsourced e-banking services.

- Companies that provide e-finance services to third parties should ensure that their operations, responsibilities and liabilities are sufficiently clear so that serviced institutions can adequately carry out their own effective due diligence reviews and ongoing oversight of the relationship.

- E-finance companies have a responsibility to provide serviced institutions with information necessary to identify, control and monitor any risks associated with the e-banking service arrangement.

There are many issues and alternatives associated with the best implementation method. It is hoped that over a period, a dominant industry-wide standard would appear. At the same time, even the most straight forward solutions available need to be monitored and maintained and patched on a regular basis to be effective. Ultimately organizations need to look at their own risk management issues and decide what level of vulnerability they can afford. It must be kept in mind that damage levels are rising to a point where security concern cannot be taken lightly. Further, banks must come out openly and make their clients aware about the occurrence of incidents. Information leaks through some sources within the organization would make matters worse. It would be better to come clean and advise the clients about the steps proposed. Agreements and the fine print therein may make it difficult for the clients to force the banks to make good the losses, but these are not helpful in building confidence levels. Ultimately the clients' trust is what matters in a highly leveraged industry.