

## Computer Security for 2004

With the emergence of better wireless technology government agencies and the military are becoming more and more dependant on information systems as a tool to perform their job.

It is as common now to see a cell phone or a Blackberry on a pistol belt as it is an ASP or handcuffs. With this new technology comes our responsibility to understand and use the technology responsibly and intelligently. Improper security of our information tools could have catastrophic affect from perpetrators becoming aware of pending searches or raids to loss of sensitive information on crime victims to the media prior to the next of kin being notified.

We have seen incidents in the Michael Jackson case where someone has bugged the flower pots outside the courthouse to listen to the deputies talking while on a smoke break and the President of Peru being monitored and broadcast live by the media during cabinet meetings. None of us are immune to prying eyes or ears. If your position was not important to someone, they would eliminate it. You could have information that could be vital to someone attempting to penetrate or destroy your facility or attack someone in or visiting your area of operation. The information that you transmit by email, telephone, pager, blackberry or just leave available could cost someone or even you to lose their life.

In the next pages and hours we are going to provide you with information on the risk and vulnerabilities or information systems as well as some things that you can do to assist your system administrators to insure that your system continues to be operating in a secure manner.

Taking information with you away from the secured facilities brings a new set of problems for information security practitioners.

As security professionals, our task of protecting our companies has expanded too much more than that of just Executive Protection or having our offices Swept for Bugs. With upper management, the media and politicians being more informed and Management less naive about their vulnerability to Hackers, Cyber Terrorist and Industrial Espionage, we must provide them with a complete Information Technology program. This includes securing our facilities, locating and mapping Wi-Fi hotspots within our facility, insuring that the hotspots are secured, conducting TSCM sweeps for illegal transmitters, providing Fire Walls, Computer Security Training and also protecting our employee's while they are in our facilities and their information while they travel.

We are responsible for Information Protection of our computers in the office as well as the notebooks, PDA's and Blackberry's used by our employee's while out of our facility. With the Executive out of your secured facility, our mission has become a much greater task. We not only have to protect our computers and communications inside of our

## Computer Security for Law Enforcement Officers

businesses, we also have to protect against someone compromising our business through the traveling Executive or through the Executives' home access to classified material.

We can no longer lock down a facility at night and not have to worry about it until the next morning. We can come under attack at any time from any where in the world from Hackers, Industrial Espionage Specialist, Competitive Intelligence Persons, Embezzlers and the old time thieves.

This session is designed to advise you of the vulnerabilities that you face while traveling, at home and while just out of the office. With the advancement of technology, we have found that criminals have also advanced their tactics for stealing from us. It is much easier for someone to hack into your computer and have you ship them 1,000 televisions than it is to get a crow bar and a truck and break into your warehouse to steal them.

There are four major concerns when it comes to Information and Computer Security:

- 1           Someone hacking into your system from outside or an unauthorized internal attack.
- 2           Someone intercepting your internal modem or communication traffic.
- 3           The penetration of your system through an employee's home computer that has access to your corporate system.
- 4           The actual theft and or copying of Executives' information while in hotels or while traveling.

These breaches in your communication security can be dealt with in a relatively easy manner with the proper support from your Senior Management. The problem is you have to have the Senior Management's support because they are the ones that are normally targeted.

There is a problem that all businesses and Agencies have to deal with. I am sure that most of you read where the head of the CIA lost his DOD Security clearance for leaving classified information on his personal computer.

The following is some basic information on computer security that I hope will assist you in the performance of your information security task.

The Internet connects to over 175 million computers in every continent, even Antarctica. Through these networks flows data through gateways, routers, dial-up connections, and Internet service providers. Individuals and organizations worldwide can connect to anyone without regard to location or nationalities.

This is also a two-way street. Not only can you reach out to others, they can reach out to you, and sometimes with out your knowledge. This creates a huge risk for businesses

## Computer Security for Law Enforcement Officers

especially if you are newsworthy or well known. Your firm is now vulnerable to new risks. Among them are the risks that valuable information will be lost, stolen, corrupted, or misused and that the computer systems will be corrupted.

Information that is recorded electronically on a networked computer, it is more vulnerable than if the same information is printed on paper and locked in a file cabinet.

This can be done from anywhere in the world without ever risking exposure by going to your facility.

*This session is* intended to help all stakeholders, security managers, and executives become more aware of the technical, and not so technical methods used by individuals in the business of obtaining your proprietary information and breaching your information security.

### Information Security Requirements for 2004

When we look at the concept of computer and information security, we find that we have three basic security concepts important to information security on the Internet. They are confidentiality, integrity, and availability. Concepts related to how that information is used are authentication, authorization, and nonrepudiation.

We have a loss of confidentiality when information is copied, read or transmitted to another that is not **authorized** to have access to the information. The importance of this can be seen in situations like research data, payroll or medical records, insurance records, new product specifications, and corporate investment strategies. In some locations, there may be a legal obligation to protect the privacy of individuals. If someone is attempting to assassinate someone, they always conduct surveillance on them and possibly their family before an attack. It is also much easier to intercept an email or phone conversation stating that they will be home at 6:30 than to have kidnapping or assassination teams waiting all day in the street to follow them. Other examples are organizations that use and collect credit information like banks and loan companies; debt collectors; or businesses that extend credit to their customers. Credit files are excellent sources of information from home addresses to types of credit cards and bank information.

Secondly we need to protect our information from being corrupted while it is available on an unsecured network. When information is modified in unexpected ways, the result is a loss of integrity. We are all familiar with defacing of Defense Department and White House web sites. What is worse than the blatant defacing is the very subtle thinks(--is thinks the right word???) like changing one number in a phone number or one of my favorites is the changing of "Links" on the contact us button. I have seen several sites where the "contact us" button takes the viewer to a competitors site. Unauthorized changes made to information, whether by human error or intentional tampering can destroy the network integrity. Integrity is particularly important for critical safety and financial data used for activities such as facility command, internal security systems, elevator controls, electronic funds transfers, air traffic control, and financial accounting.

J. Keith Flannigan, PhD, CAS  
Anti Terrorism Accreditation Board

Pedro L. Quinones PhD, CAS  
[www.goATAB.org](http://www.goATAB.org)

## Computer Security for Law Enforcement Officers

Another serious problem is the loss of data such as being erased or becoming inaccessible, resulting in loss of availability. At this point authorized users can not have access to get information that they need. Availability is critical when attempting to access criminal histories, building access authority or disaster recovery plans as well as in service-oriented businesses that depend on information (e.g., airline schedules and online inventory and delivery systems). Availability of the network itself is important to anyone whose business or education relies on a network connection. A denial of service occurs when a user cannot get access to the network or specific services provided on the network.

Authentication and authorization are the techniques used to determine what information will be made available to whom and if that person is a trusted user. Authentication is proving that a user is whom he or she claims to be. That proof may involve something the user knows such as a password, or they have like a “smartcard”, or something about the user that proves the person’s identity such as a fingerprint. Authorization is the act of determining whether a particular user has the right to carry out a certain activity, such as reading a file or running a program. Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Security is strong when the means of authentication cannot later be refuted—the user cannot later deny that he or she performed the activity. This is known as nonrepudiation.

“Information Assurance” is another term used in relation to information security. The basic concepts are the same. Internet users want to be assured that:

- they can trust the information they use,
- the information they are responsible for will be shared only in the manner that they expect,
- the information will be available when they need it, and
- the systems they use will process information in a timely and trustworthy manner.

The scope of information assurance extends to systems of all kinds, including large-scale distributed systems, control systems, and embedded systems, and it encompasses systems with hardware, software, and human components. The technologies of information assurance address system intrusions and compromises to information.

It is remarkably easy to gain unauthorized access to information in an unsecured networked environment, and it is hard to catch the intruders. Even if users have nothing stored on their computer that they consider important, that computer can be a “weak link,” allowing unauthorized access to the organization’s systems and information.

Seemingly innocuous information can expose a computer system to compromise. Information that intruders find useful includes which hardware and software are being used, system configuration, type of network connections, phone numbers, and access and authentication procedures. Security-related information can enable unauthorized

## Computer Security for Law Enforcement Officers

individuals to get access to important files and programs, thus compromising the security of the system. Examples of important information are passwords, access control files and keys, personnel information, and encryption algorithms.

From the latest research data on computer abuse reported in the media, no one on the Internet is immune. Those affected include banks and financial companies, insurance companies, brokerage houses, consultants, government contractors, government agencies, hospitals and medical laboratories, network service providers, utility companies, the textile business, universities, and wholesale and retail trades.

The consequences of a break-in cover a broad range of possibilities: a minor loss of time in recovering from the problem, a decrease in productivity, a significant loss of money or staff-hours, a devastating loss of credibility or market opportunity, a business no longer able to compete, legal liability, and the loss of life.

There are many new changes coming in the laws governing crimes committed using computers or over the Internet. We also have many new changes in the regulations that we have to comply with regarding the safe guarding of data such as HIPAA, GLB, SOX, Public Health Security and Bioterrorism Preparedness Response Act of 2002, USA Patriot act of 2001, H.R. 3448, CFR 42, CFR 49 and the Anti Terrorism and Effective Death Penalty Act of 1996. Violation of some of these acts have penalties of \$250,000 for the offender and \$500,000 fines for the organization. Federal computer crime legislation can be divided into three broad categories: encouraging information sharing; technical solutions; and enhanced law enforcement.

### **Many IT specialist are hesitant to discuss or report hacker attacks.**

Protecting corporate information from hackers and e-thieves may be tough; sharing information about corporate information security practices may be tougher still. Companies are loath to discuss cracks in the defense against hacks, particularly with outsiders or Federal Law Enforcement. And for several good business reasons. Trade secrets could wind up in the hands of competitors. If a case goes to court, the court transcripts may be obtained and the confidential information or patent information could become available to anyone. It could also be the cause for civil action by the shareholder in lawsuits against the company, to scare away customers or be used as the breadcrumb trail for still other hackers. Most civilians are also concerned that the law enforcement takes their information and does not supply the company with anything that they can use to either defend its self or to better their security.

Efforts are being made to change this perception and at least two industries, financial services and telecommunications, have actually set up an ISAC and others, including the information technology industry, are moving in this direction. The Financial Services Information Sharing and Analysis Center (FS/ISAC) is composed of 24 banks and financial services firms which share information on an anonymous basis. Not only the data provided but even the names of FS/ISAC members themselves is kept confidential.

### **Denial-of-Service Tools, and how to defeat them**

Distributed systems based on the client/server model have become increasingly common. In recent months, there has been an increase in the development and use of distributed network sniffers, scanners, and denial-of-service tools. Attacks using these tools can involve a large number of sites simultaneously and be focused to attack one or more victim hosts or networks.

Damaged systems include those used in the attack as well as the targeted victim. For the victim, the impact can be extensive. For example, in a denial-of-service attack using distributed technology, the attacked system observes simultaneous attacks from all the nodes at once—flooding the network normally used to communicate and trace the attacks and preventing any legitimate traffic from traversing the network.

The processes for discovering vulnerable sites, compromising them, installing daemons (programs used in the attack), and concealing the intrusion are largely automated, with each step being performed in “batch” mode against many machines in one “session.” Attack daemons have been discovered on a variety of operating systems with varying levels of security and system management.

Since the attack methodology is complex and there is no single-point solution or “silver bullet,” resolution and restoration of systems may be time-consuming. The bottom line is that an organization’s systems may be subject at any time to distributed attacks that are extremely difficult to trace or defend against. Only partial solutions are available.

An organization may be able to “harden” its own systems to help prevent having its systems used as part of a distributed attack. There is essentially nothing a site can do with currently available technology to prevent becoming a victim of, for example, a coordinated network flood. The impact upon the site and its operations is dictated by the security of other sites and the ability of a remote attacker to implant the tools and, subsequently, to control and direct multiple systems worldwide to launch an attack. The result may be reduced or unavailable network connectivity for extended periods of time, possibly days or even weeks depending upon the number of sites attacking and the number of possible attack networks that could be activated in parallel or sequentially.

Coordinated attacks across national boundaries have occurred. The tools and attacks demonstrate that a network which optimizes its technology for speed and reliability at the expense of security may experience neither speed nor reliability as intruders abuse the network or deny its services. The intruder technology is evolving, and future tools may be more difficult to defeat.

## Computer Security for Law Enforcement Officers

### Distributed Denial-of-Service Details

- Intruders compromise systems through other means and install distributed-denial-of-service (DDoS) tools. These tools often are equipped with a variety of different attack types.
- Computers that are compromised with DDoS tools are aggregated into networks. These networks act in unison to attack a single victim and can be activated remotely at a later date by a “master” computer.
- Communication between the master computer and the networks can be encrypted and obfuscated to make it very difficult to locate the master.
- Once activated, the tools typically proceed on their own. No further communication is necessary on the part of the intruder – it is not possible to discover the master by tracing an ongoing attack. However, there may be evidence on one or more of the machines in the DDoS network regarding the true location of the master.
- Attacks from the network to the victim typically employ techniques designed to obfuscate the true location of the machines in the DDoS network. This makes it difficult to recognize the traffic (and thus block it), to trace the traffic back from the victim to the nodes in the network, and to analyze an attack while it is in progress.
- The tools are rapidly evolving but have not reached their full potential by any means.
- The magnitude of the attacks can overwhelm even the largest networks.
- Intruders are building networks of machines used in these attacks ranging in size from tens to hundreds of machines. It is likely that some networks are much larger.
- The individual nodes in the network can be automatically updated by the master machines, enabling rapid evolution of tools on an existing base of compromised machines.
- Currently, there is a nearly inexhaustible supply of computers with well-known vulnerabilities that intruders can compromise and install DDoS tools on. Additionally, many networks are configured in a way that facilitates the obfuscation techniques used by intruders to conceal their identity.

The problem of distributed denial-of-service attacks is complex, and there are no easy answers.

Attackers often hide the identity of machines used to carry out an attack by falsifying the source address of the network communication. This makes it more difficult to identify the sources of attack traffic and sometimes shifts attention onto innocent third parties.

## Computer Security for Law Enforcement Officers

Limiting the ability of an attacker to spoof IP source addresses will not stop attacks, but will dramatically shorten the time needed to trace an attack back to its origins.

To lessen their exposure to such threats, user organizations and Internet service providers should consider the following suggestions:

- Ensure that traffic exiting an organization's site, or entering an ISP's network from a site, carries a source address consistent with the set of addresses for that site, and ensure that no traffic from "unroutable addresses" listed in Internet Engineering Task Force Request for Comments (RFC) 1918 are sent from their sites. This activity is often called egress filtering.
- ISPs can provide backup to pick up spoofed traffic that is not caught by user filters. ISPs may also be able to stop spoofing by accepting traffic (and passing it along) only if it comes from authorized sources. This activity is often called ingress filtering.
- Dial-up users are the source of some attacks. Putting an end to spoofing by these users is an important step. ISPs, universities, libraries and others that serve dial-up users should ensure that proper filters are in place to prevent dial-up connections using spoofed addresses.
- Network equipment vendors should ensure that no-IP-spoofing is a user setting, and the default setting, on their dial-up equipment.

In a common attack, the malicious user generates packets with a source address of the site he wishes to attack (site A) (using spoofing) and then sends a series of network packets to an organization with lots of computers (site B), using an address that broadcasts the packets to every machine at site B. Unless precautions have been taken, every machine at Site B will respond to the packets and send data to the organization (site A) that was the target of the attack. The target will be flooded and people at site A may blame the people at site B. Attacks of this type often are referred to as Smurf attacks. In addition, the echo and charged services can be used to create oscillation attacks similar in effect to Smurf. Solutions include the following:

- Unless an organization is aware of a legitimate need to support broadcast or multicast traffic within its environment, the forwarding of directed broadcasts should be turned off. Even when broadcast applications are legitimate, an organization should block certain types of traffic sent to "broadcast" addresses (should this be address ?)(e.g., ICMP Echo Reply) messages so that its systems cannot be used to effect these Smurf attacks.
- Network hardware vendors should ensure that routers can turn off the forwarding of IP directed broadcast packets as described in the Internet Engineering Task Force document RFC 2644 and that this is the default configuration of every router.

## Computer Security for Law Enforcement Officers

- Users should turn off echo and chargen services unless they have a specific need for those services. (This is good advice, in general, for all network services – they should be disabled unless known to be needed.)

### **Non Reporting can be a hazard**

Many organizations do not respond to complaints of attacks originating from their sites or to attacks against their sites, or respond in a haphazard manner. This makes containment and eradication of attacks difficult. Further, many organizations fail to share information about attacks; the attacker community has no such inhibitions and, as a result, enjoys much better information.

User organizations should establish incident response policies and teams with clearly defined responsibilities and procedures. ISPs should establish methods of responding quickly if they discover that their systems were used for attacks on other organizations. They must also have enough staffing to support these efforts. User organizations should encourage system administrators to participate in industry-wide early warning systems where their corporate identities can be protected (if necessary) to counter rapid dissemination of information among the attack community. Attacks and system flaws should be reported to appropriate authorities (e.g., vendors, response teams) so that the information can be applied to defenses for other users.

### **Repairs can be costly and difficult**

Many computers are vulnerable to take-over for distributed denial-of-service attacks because of inadequate implementation of well-known “best practices.” When those computers are used in attacks, the result can be major costs, headaches, and embarrassment for the owners of computers being attacked. Furthermore, once a computer has been compromised, the data may be copied, altered or destroyed, programs changed, and the system disabled. Solutions include the following:

- Organizations should check their systems periodically to determine whether they have had malicious software installed, including DDoS Trojan horse programs. If such software is found, the system must be restored to insure the security of the network.
- Organizations should reduce the vulnerability of their systems by installing firewalls with rule sets that tightly limit transmission across the site’s periphery (e.g. deny traffic, both incoming and outgoing, unless given specific instructions to allow it).
- All machines, routers, and other Internet-accessible equipment should be periodically checked to verify that all recommended security patches have been installed.
- You should turn off services that are not required and limit access to vulnerable management services (e.g., RPC-based services).

## Computer Security for Law Enforcement Officers

- Users and vendors should cooperate to create “system-hardening” scripts that can be used by less sophisticated users to close known holes and tighten settings to make their systems more secure. Users should employ these tools when they are available.
- System software vendors should consider shipping systems where security defaults are set to the highest level of security rather than the lowest level of security. These “secure out-of-the-box” configurations will greatly aid novice users and system administrators. They will furthermore save critically scarce time for even the most experienced security professionals.
- Tools including firewalls, intrusion detection systems, virus detection software, and software to detect unauthorized changes to files. Use of software to detect unauthorized changes may also be helpful in restoring compromised systems to normal function.
- Adequate time, support for training and enhancement of their skills. System administrators and auditors should be periodically certified to verify that their security knowledge and skills are current.

DDoS attacks require a long-term effort to define and implement effective solutions. The security of each system on the Internet depends on the security of all other systems on the network. The distributed denial-of-service attacks clearly demonstrate this interdependency and the responsibility of computer users to the larger Internet community.

- There are many tools available to detect DDoS attacks. All of them have some pros and cons. I have not found any one that does everything that I need to have done. There are several that can be found on the internet.

### Wireless Networks

One of the current threats in the business world today is with the wireless devices that are in use. War Driving or the scanning for wireless networks is pervasive. There is even a web site of subversive mapped sites around the world (Worldwidewardrive.com). More than half of the sites located by war drivers are either unsecured or under secured.

The hardware and software developers are doing all that they can to make the systems more secure. *Bluetooth* was conceived by Messrs. *Ericsson*, a multi-national technology company with about 80,000 employees worldwide, and with “Nordic ties”. Very quickly other global players like *Motorola*, *Nokia*, *Cisco*, *Agilent* – just to name a few – became aware of this revolutionary invention and joint the efforts to create a common product platform. Mainly to cut their piece of cake of this breathtaking approach, but also to ensure that from the very beginning manufactures would agree upon and support through their membership through **IEEE** (Institute of Electrical and Electronic Engineers) the

## Computer Security for Law Enforcement Officers

need for a universal data-transfer standard, applicable for all major appliances and applications.

### **Standard for Bluetooth and wireless applications**

Standards for data-transfer are defined by the **IEEE** (Institute of Electrical and Electronic Engineers) through their 802 committees. The digits behind the dot (.) specifies the type of the data-transfer.

- **IEEE 802.15** regulates **Bluetooth applications**.

### **Other wireless applications are governed by**

- **IEEE 802.11** deals with transfer rates from **1Mbps and 2Mbps**
  - defines standards for **WLAN's** (Wireless Local Area-Networks)
  - defines standards for infra-red, DSSS and FHSS with a data-rate of 1, 2 & 11 Mbps
  - defines power management implementation

More regulations are found in:

- **IEEE 802.11a**
- **IEEE 802.11b** (11Mbps)
- **HiPerLAN I und II**

Each device will be equipped with a **tiny and inexpensive radio chip** which converts the information to be transferred into radio signals. Both the **low cost** and the **low power consumption** for this data-transfer technology opens numerous applications.

**WLAN's** (Wireless Local Area Networks) is another favorite application for Bluetooth technology. The simple placement of transceivers in the area where a network needs to be established provides immediate coverage. Presently less than 8 nodes can be supported within a network.

**Wireless headsets** to communicate with **cellular telephones** are already standard features with the newest models of *Nokia*, *Motorola* and *Ericsson* phones. The world leader of handheld devices, *PALM*, has a blue chip card for the standard expansion slot in its final test phase. The new area of **PAN** (Personal Area Network) has already started.

Other applications are **Bluetooth**-chips in **freight containers**. A truck driving up to a storage depot will get its marked contents registered within seconds without any physical contact.

The applications are endless and reach into the privacy of our homes. **Refrigerators** will be able to communicate with a **Bluetooth**-enabled computer that the food supply is

## Computer Security for Law Enforcement Officers

getting low. Placing an order via the internet to refill the fridge by the retailer of the home-owners choice are less than a step away.

In days of rather heavy travel-restrictions and the desire by worried authorities to match airline-passengers with their luggage, another interested device undergoes its final testing. **Blue Tag**, a Danish company in Aalborg, specializing in wireless transmission technology, has created an **intelligent luggage tag**, which apparently will replace the conventional bar-coded paper tags on suitcases.

This type of **Bluetooth**-application is said to have a **range up to 60 feet**. Each tag will have a unique identification. Tags will be sold to airlines, airports, travel agents and insurance companies. Those travelers acquiring a blue tag will register one time their personal details in the blue tags memory. From before departure, and during the entire trip, the location of the suitcase will be known.

### Security features

There are 3 built-in security modes:

- Non-secure
- Service level enforced security
- Link level enforced security

Further to that, **Bluetooth**-access to service can be as a

- Trusted device or an
- Untrusted device

But it must be stated that the prime goal of the **Bluetooth**-technology is to get rid of cables. Most of the data transferred between 2 applications is not sensible. For personal- or delicate data other criteria apply. Generally speaking, the nature of transferring information is that of a “microwave link”, as opposed to a fixed cable connection, which means that it is especially vulnerable to attack.

### Disadvantage

- The allocated transmission medium in the 2,4 GHz band is already very crowded, With the very popular wireless CCTV. Some applications have already moved to a higher (and still available) band.
- Low data transfer rate if used in areas where more than 1 Mb/s is required.
- Although several security features have been implemented into the **Bluetooth** technology, it was primarily designed to transfer simple data and not sensitive information.
- Uneasiness about the continuous exposure to all kind of frequencies of a person for health reasons

## Computer Security for Law Enforcement Officers

The **Bluetooth** technology has been put to work in the Wi-Fi arena but there are a few security concerns. WEP or Wired Equivalent Privacy may not be the perfect encryption technique but it will help to discourage the average hacker or the person that is using “**Airsnort**” to locate a system to use to send out child porn or to hack some credit card sites.

“**Airsnort**” interception software needs to eavesdrop between 100MB and 1 gigabyte of data to crack a network’s WEP code. The more bits you use to encrypt the more data they need to intercept before they can get the code.

When you set up a wireless network access point, you may have missed one important security feature called MAC filtering. This is a list of network devices that are invited to use your network and the MAC filter stops unwanted users. Every network card has a unique code called a media access control or MAC address that looks something like this 00:60:85:23:1A:B2. MAC filtering uses these codes to identify who’s an authorized user and who’s not.

Insure that all the default IP addresses and passwords are changed. If you leave the access points SSID the same as the default, it could alert a good hacker as to your access points and who made them and what those default passwords and logins are. You should also insure not to name your SSID something that could draw attention like FBIHRFILES or DOJMedical.

You should change your WEP key often and most wireless networks let you store several passwords in your profile so all you have to do is go in and switch from key 1 to key 2. This is a very easy way to help insure that hackers have less chance to successfully attack your system.

Because WEP can be cracked wireless equipment makers have added an extra security layer called WPA. All new wireless products certified in the last year will support it. You will need to insure that all your wireless network card, access point, operating system, and client software all support WPA. If using Windows XP you will need to download a patch from Microsoft.

### References:

- Bluetooth revealed, ISBN 010902942
- Data Over Wireless Networks, ISBN 0072126213
- Bluetooth Group, an industry consortium, <http://www.bluetooth.com>
- Blue Tags, <http://www.bluetags.com>
- International Herald Tribune, Products and Concepts
- USA-Today, Technical Online
- ATAB IT Security in a modern world
- FBI Research files
- ICSI wireless study of 2003

J. Keith Flannigan, PhD, CAS  
Anti Terrorism Accreditation Board

Pedro L. Quinones PhD, CAS  
[www.goATAB.org](http://www.goATAB.org)

## Computer Security for Law Enforcement Officers

- SANS research files
- OFRAC IT Compliance <http://www.ofrac.com>
- Werner Preining Bluetooth Paper for ASIS

Prepared by J. Keith Flannigan PhD, CAS and Pedro L. Quinones PhD, CAS for the Anti Terrorism Accreditation Board and for ASIS International.

Mr. Flannigan has 28 years of experience in the Law Enforcement and Intelligence Fields. He has written and instructed Law Enforcement curriculum on Technical Surveillance, Crisis Response, Cyber Terrorism, Responding to a Terrorist Incident, and Managing a Bio Chemical Incident for county and state academies and Federal Law Enforcement Training Centers in Peru and Russia. For nine years he was an instructor at a police academy charged with developing and instructing training in all of the investigative areas from organized crime to crime scene investigations. Mr. Flannigan has instructed classes at Universities on Terrorism and Cyber Terrorism since 1995. Mr. Flannigan was named Counter Terrorism Professional of the Year in 1998 by the Counter Terrorism EXPO. He has completed 4 State and Federal academies, minored in Criminal Justice, earned a Ph.D. in Political Science and has completed over 3,400 hours of Law Enforcement Training.

Mr. Quinones has over 25 years of experience in the field of computer networks and network security and training. Mr. Quinones is the CEO of International Computer Solutions, Inc., a computer security firm that specialized in contract solutions to data recovery problems of Federal Law Enforcement Agencies in sensitive areas. Mr. Quinones specializes in deployment to Central and South American countries to obtain and recover electronic evidence from targeted information systems by overt or covert methods depending on the classification of the assignment. Mr. Quinones has developed computer security training programs for Narcotics Enforcement Agents from Peru, Chili, Columbia, Argentina, Ecuador and the Honduras held in Lima Peru.

Mr. Quinones has for the last 2 years conducted electronic evidence recovery operations for fortune 500 companies and law firms on some of the highest profile cases in the country. He Chairs the IT Security Committee for that Anti Terrorism Accreditation Board and sits on the advisory board for The Office of Regulatory Audit and Compliance. He has many years of advanced computer training and was awarded his PhD in Computer Science.