



▶ EDITOR'S COMMENTS.... 1

▶ Secondary Uses for Digital Surveillance 2



▶ Liability for Installed Surveillance Cameras 3

▶ Beyond the DVR... 4



▶ How Young is too Young for a Cell Phone 6

▶ Cell Phone Safety Tips..... 7

▶ Bluesnarfing..... 7

○ ISSUE 1 | ○ VOLUME 6 | ○ October 2007

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE.

Helping secure your world

Welcome to the sixth issue of **SECURITY SOLUTIONS**. As always our aim is on alerting you to security issues that can have a harmful impact, as well as providing you with practical implementable solutions for security issues in both your corporate and personal life.

This sixth issue is focused on CCTV and cell phones. While each of our previous issues has generally carried at least one article on CCTV, we were of the view that because of the central role that CCTV now plays as a security tool we should partially dedicate and issue to it. Our first article, [Secondary Uses for Digital Surveillance](#), highlights the fact that although CCTV is important as a security measure it also provides other operational benefits that have a financial impact.

To address legal concerns that some business people may have regarding the use of CCTV

on their premises, we have an article that deals with [Liability for Installed Surveillance Cameras](#).

In order, after the event, to use the imagery that CCTV provides it is necessary to attach the CCTV cameras to a recorder. The technology has definitely gone beyond tapes and into the digital realm. The third article looks at how the technology is already moving [Beyond the Digital Video Recorder](#).



Cell Phones are an almost indispensable part of everyday life. Throughout the Caribbean however there is discussion on cell phone use by children. The article, [How Young is Too Young for a Cell Phone](#) joins the debate on this subject.

We also provide some [Cell Phone Safety Tips](#). Our final article [Bluesnarfing](#), seeks to alert readers to a threat to their cell phone security.

If any additional persons in your organisation would like to receive this email newsletter, just send an email to newsletter@assl.com with the words "Subscribe Newsletter" in the subject line and the email address, name and organization in the body. To opt out of the mailing list send an email with the words "Unsubscribe Newsletter".

Brian Ramsey
Editor

Secondary Uses for Digital Surveillance Technology Grow



By Julie Ritzer Ross.

"Video surveillance in restaurants: Who's using what technology and why"

A desire to keep a tighter rein over day-to-day problems in the front-and back-of-the-house--not all of which are security related—is driving operators to adopt digital video surveillance technology that is light years ahead of the VCR-based sentries of the past.

Some restaurateurs, like airport feeder Hartsfield Hospitality of Atlanta, are using video surveillance to monitor food and cash handling procedures, employee conduct and more. That firm operates one Freshens Smoothie Co. unit and one Le Petit Bistro store at George Bush Intercontinental Airport in Houston, as well as four Freshens units and one Le Petit Bistro unit at Hartsfield-Jackson Atlanta International Airport in Atlanta.

Other operators using video recording, analysis, reviewing and reporting technology also augment the basic security and employee-theft prevention roles of their systems by using them to verify workers' compensation and guest incident claims. Service providers say such users include operators of IHOP and Steak n Shake restaurants and a number of Subway and McDonald's franchisees with multiple locations.

"With this [video] system, I can see basically everything that's going on, from how food is being

prepared, to how customers are handled, to whether employees are wearing their uniforms," Esau Sims of Hartsfield Hospitality said. "In fact, we've seen a big improvement in service efficiencies from using the system at Le Petit Bistro, where customers wait on line to pay for their food, because the recordings [revealed] that employees weren't calling the next [patrons] to the register fast enough when finished with the previous guest."

However, Sims, who is Hartsfield Hospitality's director of operations, indicated that his company's desire to improve its financial position was what prompted it to use technology by Coppel, Texas-based Digital Witness.

He had suspected that monitoring food preparation in the stores would bring expenditures "more in line with what they should be." Sims also had a hunch that putting a surveillance finger on the pulse of cash handling and customer service would benefit the bottom line. His suspicions proved correct, and Hartsfield has shaved about 2.5 percent off its annual food expenditures and increased profits by about \$100,000 since the system was deployed in February 2006.

The Digital Witness system consists of cameras placed in strategic areas around a restaurant, including near the front door, prep areas, cash registers and the back door. The cameras continuously record images on a digital video recorder, or DVR, and upload them to a password-protected Digital Witness website that operators can access from any computer. Sims logs in to the site daily to view images in real time, as well as to look at images that have been indexed by the system and are stored on Digital Witness' host computer.

Based on dashboards created for each operator, the cameras also generate and e-mail to management exception reports detailing any anomalies they have detected. In Hartsfield Hospitality's case, such anomalies include

instances in which employees are obviously deviating from prescribed food portioning guidelines and discarding or misappropriating ingredients. The system also has been programmed to let Sims and his colleagues know when an employee has made a cash-handling error, such as leaving a cash drawer open or failing to provide a receipt with a purchase.

Sims declined to quantify his company's investment in the system, noting only that the monitoring capabilities it affords have sparked an "excellent" return. Hartsfield Hospitality uses the technology on a subscription basis, as do 95 percent of Digital Witness' customers, whose ranks include operators of Outback Steakhouse, Benihana and Buffalo Wild Wings outlets.

Kelby Hagar, chief executive of Digital Witness, said the cost of an eight-camera system, such as the one in place at most Hartsfield Hospitality units, runs \$299 per store per month. That fee covers equipment, server and software licensing, maintenance, daily remote assessments to ensure that hardware is in working order and two annual software upgrades. System setup carries a one-time \$900 fee.

Two-unit coffeehouse operator Cafe Intermezzo in Atlanta acquired a video surveillance system to gain better control over workers' compensation and guest incident claims and employee conduct, said chief executive Brian Olson. The package, DTT OnSite from DTT Surveillance of Los Angeles, is already installed in one store and is being deployed in the other.

A third Atlanta store now under construction also will be fitted with the technology, as will all future units, management said.

Cafe Intermezzo purchased for each unit a 16-camera bundle that also included a DVR, CD burner, server and software. Sam Naficy, chief executive of DTT, said system purchase prices range from \$4,000

for a four-camera package to about \$11,000 for a 16-camera package. He declined to provide details about his company's monthly service fee. DTT also counts among its users some McDonald's and Subway franchisees, Naficy said, as well as those of IHOP, Steak n Shake and Moe's Southwest Grill.

The software can sort clips of images captured by the system by year, date and time, and footage can be played back on the hardware even as recording is occurring. Olson can set the playback function for single or multiple camera views, or he can view frame-by-frame thumbnail shots for quick identification of any incident.

Olson said the technology paid for itself within a year.

"On the first day we installed it, we recouped \$570 that had just gone missing from the petty cash in our locked cash room," he said. "We have cameras all over the store. One covers the cash room and another, the back office. When we realized the money had been taken, we reviewed the images and observed a dishwasher stealing the manager's keys and gleefully pocketing the cash."

Olson said the technology not only enabled Cafe Intermezzo to apprehend the thief and share a CD of the incident with police, but it also helped clear the manager of any wrongdoing.

In another instance, Olson recalled, a guest claimed her purse had been stolen from her chair while she was away from her table looking at the pastry selection, and she tried to pin the blame on the establishment. However, a look at the video indicated that she had taken the purse with her when leaving the table. In a third situation, an employee attempted to file a workers' compensation claim for a slip-and-fall incident, but the recording showed that she had caught herself before actually hitting the floor.

"Our workers' comp claims are way, way down because of the

system, and we don't worry nearly as much about bogus slip-and-fall claims by patrons," Olson said. "The technology has also been great in terms of [curtailing] employee pilferage. Once, we noticed that a lot of shrimp--which is very expensive--was disappearing. We reviewed images from the kitchen and found that a chef--who ran a catering business on the side--was responsible."

Reprinted from:

Nation's Restaurant News
August 2007

Liability for Installed Surveillance Cameras

By Ken Kirschenbau, Esq.



QUESTION:

One of our clients is reluctant to install cameras because they believe it increases liability. Our experience is a camera system decreases liability since the owner is taking steps to provide a secure facility.

But if the system is not monitored live does this give the occupant a false sense of security? Have you ever heard where an owner is liable for cameras that are not monitored live or liable for systems that do not have complete coverage of parking areas?

And does an owner legally have to post signs stating area has surveillance cameras and/or is being recorded?

MY ANSWER:

The issue of camera installation continues to plague property owners and security dealers because there is so little precedent to rely upon. There are, however, some principals of law which can be applied. One is that property owners do owe their tenants and others lawfully on the property some degree of reasonable protection. The level of duty has many variables.

A landlord of a residential property has a duty to provide reasonable security when the property is known to be in a high crime area and that tenants are likely to be at risk. Also, there are laws that affect the landlord's duty to provide some level of protection, such as front door locks and intercom systems. Of course fire protection/detection is another level of security and safety which is generally required.

Video surveillance, however, is rarely required by law. One that does come to mind is ATM facilities in New York City, which I believe must have CCTV coverage. But property owners are not required to install and supervise CCTV. More often than not CCTV is installed by property owners as a measure to reduce property damage or to record the damage for possible police investigation after the fact.

Some property complexes do have CCTV with on-site guard monitoring and certainly the presence of CCTV does raise the question of liability. One who assumes a duty is then required to perform that duty in a reasonable manner. Thus, creating a sense of security by installing cameras or taking other security measures designed to instill a sense of safety will create a duty to provide that reasonable measure of protection. Dummy cameras would be about as effective as dummy guards [I am talking about the inanimate stuffed ones].

Property owners would be wise to make it clear what cameras or other security is designed to do or detect. Signs just as conspicuous as the cameras would be a good start. A notice to commercial

tenants that cameras have been installed but are not supervised and are for the owners property protection would be a good idea.



In my office complex, for example, I see that the owner has installed cameras in the lobby of the buildings and outside the buildings viewing the parking lots. The cameras are visible, but the office tenants have never been notified why the cameras were installed or whether they are manned. This property management company could certainly avoid some issue, at least with the tenants, if it sent around a notice regarding the limitations of the cameras.

Another example that comes to mind is a landlord who installs cameras in a laundry room in a residential building. Especially if the landlord has a financial interest in the use of the washing machines, which they usually do, advising tenants of the true use and limitations of the cameras would be important if there were an incident.

The public's perception of CCTV coverage -- or for that matter guard coverage -- is probably not accurate with reality. Rarely is CCTV manned and more often than not security guards are instructed not to get involved in an incident other than to communicate with the police to report an incident. This is not to suggest that there are not buildings where CCTV is monitored live and where guards are armed and prepared to intervene.

A reasonable person on the premises should be able to figure out what kind of security exists on the premises, and an owner creating a false sense of security should expect to be held

responsible, not necessarily for the entire injury or loss, but contributing to it by the injured party not taking other security measures because of the false sense of security.

About the author: Ken Kirschenbaum, Esq., is a New York-licensed lawyer practicing with Kirschenbaum & Kirschenbaum PC, a Long Island legal firm with a rich history of assisting clients in security and alarm related matters. Ken can be contacted via email at ken@kirschenbaumesq.com. His website, www.kirschenbaumesq.com, features a great supply of legal information and court rulings relevant to the security industry. You can also sign up for Ken's discussion list from his homepage.

Reprinted from
SecurityInfoWatch.com

Beyond the DVR

By [Eduard L. Telders](#)

The security industry continues to be challenged by ever increasing requirements for surveillance applications. Comprehensive security and surveillance strategies are including digital video surveillance as a first option in ever increasing numbers. These strategies are designed to provide users with better threat detection and prevention, a low cost of ownership, streamlined security operations and decreased liability.

Along with this increasing need for surveillance systems is the increased need to effectively manage and use the massive amount of recorded images that must now be stored. Security directors who would manage from a few to hundreds of cameras just a few years ago, must now provide security surveillance services that include several hundred to even thousands of cameras — all of which produce recorded images that must be stored and available on demand.

Traditional Video Surveillance

The classic CCTV implementation that is still in use in many locations has not changed dramatically since the invention of the video recorder. These systems have been used successfully for many years. The typical installation included analog CCTV cameras which had separate wires pulled to them for power and for transmitting images over proprietary wired coaxial connections to VHS video recorders. Add a monitor and the security guard can watch live video or watch playback on the VHS.

Larger implementations of these systems would have security guards watching an ever increasing number of monitors — each of which would present either a continuous image of the area under surveillance or it would “cycle” between several camera fields of view in a predetermined sequence. Practical limitations for the number of monitors effectively screened by a security officer began to drive innovation towards enhancing these systems. Multiplexers were added to these systems to allow the recording of several streams of video onto the same tape, yet separated into discrete viewable streams on playback. Tapes only had a few hours of recordable surface, so multiplexers were used to drop frames in the stream to create the notion of the time-lapse VCR to permit longer recording time coverage on the same tape — although it would do so by reducing the number of actual recorded images.

Many environments still use these systems — even though by today's standards, analog camera and tape systems have a number of limitations. These implementations need manual tape storage and re-use procedures to ensure that retention of the images was available. The process was tedious and prone to human error leading to misplaced or lost information. Video tapes have a limited life span and would need to be replaced often to ensure the quality of the images remained within acceptable tolerances. Keeping the recorders cleaned and serviced meant taking them out of service. Finally, the

coaxial cables had limited effective distances which meant that these systems were deployed locally to the tape recorders and could not be transmitted between remote facilities.

The real bad news for users of these systems is that many of the manufacturers of tape systems have opted to discontinue making them as recently as 2005, which makes it imperative to consider alternatives as replacements, service and parts will soon become significantly more difficult to find.

The First Real Innovation: the DVR

Rapid development in video compression algorithms such as JPEG, MJPEG, MPEG and others coupled with lower data storage costs on digital media prompted the creation of the Digital Video Recorder, or DVR. DVR technology comes directly from the computer world using the same disk technology found in servers.

Conceptually the DVR is quite similar to the TiVo system you may have connected to your television set at home, and it has several advantages over traditional tape systems.

DVR systems are more reliable since there are no tapes to jam. They offer better video quality as they do not have tape wear problems. They have a low risk of degaussing or signal loss. They can store significantly more images — from weeks to years worth of data. They also eliminated the need for multiplexers as they provided that capability built into the DVR itself. The most important enhancement is that they are effectively automated so that you do not need a human resource to rotate tapes or remember to push the recording button.

The primary reasons for DVR implementations were to address the above issues; however they still have limitations. They still were primarily connected to analog cameras and were therefore still implemented local to the cameras themselves, making remote viewing problematic. They still were limited in the number of

camera ports available, as most of them allowed up to 16 channels or video ports. They also tended to be based on a proprietary analog-to-digital conversion capture cards which were not interchangeable with another manufacturer's DVR. Components and accessories were also proprietary. This also meant that the DVR manufacturer was your only real option for service and replacement — limiting the security director's options for consolidating service contracts. Backup and recovery of recorded images is typically not available — if you lose the device, you usually lose the images recorded on the disk.

The advent of the DVR provided advantages over tape-based systems, but more was needed to respond to security industry requirements.

The Impact of IP Based Systems: the NVR

The convergence of IT systems with physical security applications has been widely described. Suffice to say that the incredible growth of IP-based solutions is in parallel with the explosive growth of the Internet and browser technologies. Companies started to see the opportunities presented by using IT networks for more than business applications. Building management systems, fire control systems, HVAC, alarm and access controls, elevator controls, lighting controls, telecommunications, PA Systems, e-commerce applications, and many other previously siloed systems have joined this technological revolution. Physical security is no exception. The move to IP-based solutions on open architectures is under way. IP solutions open a wide variety of options and advantages to the security industry.

The advantages of using IP-based technology are a significant leap forward over previous systems. First and foremost is the simple ability to connect the IP-enabled camera systems to your IT network, eliminating the coax cables. It also means that the ability to transmit those images

across geographic areas is now only limited by your network's limitations. Local storage is no longer required. Getting power to an analog camera has always been a major obstacle and cost. The IEEE 802.3af standard for Power over Ethernet (PoE) was designed to address this problem, leading to significant cost savings in deployment of IP cameras. PoE means that networking devices get power from a PoE-enabled switch over the same kind of Category 5 cable that transmits data and video. It also means that cameras can get centralized backup power from the computer room backup power systems, so in the event of a power failure, they will continue to operate. Legacy analog cameras can be connected via a video server (which converts the analog to digital format) to the IP network to allow for migration plans and capital expenditures to be planned within budgets. IP digital cameras do not need to be converted.

One of the drivers in this industry is the sheer volume of video that is being captured. Security directors need to be sure that they record the information that is critical, and not capture information that is of little value. A camera watching an empty hallway is only valued when activity is presented. Intelligent video is one of the next big trends. Network cameras can have built-in motion detection and alarm management at the camera itself. The camera decides when to send video, at what frame rate and resolution, and when to alert a specific operator for monitoring or response. Intelligent algorithms for license plate recognition, people counting, facial recognition, etc., are being integrated into network cameras.

The next significant advantage is that you can base your video storage applications anywhere on the network. This generated the new term Network Video Recorder, or NVR, which has two types of implementations. The first is a "network aware" DVR developed on PC-based architecture, and the second simply uses a standard server which uses the same storage systems and disks as in

any other servers capable of storing video imaging. This allows for the centralization of video storage and management in a Security Operations Center (SOC). You can also choose to have distributed SOC controls as well. This also allows for ease of remote monitoring across the network using standard PCs and browser technology for controlling pan/tilt/zoom (PTZ) cameras and video surveillance. Gone are the 50-pound, standalone monitors.

Capacity and scalability have taken a significant leap ahead on NVR systems. Previous DVR systems could typically support 16 cameras, some higher-end systems could support up to 64 cameras. NVR systems can support camera counts from 50 up to 1,000 each. As your needs grow, you can simply add more capacity. Maximum resolution is also effectively unlimited. As digital cameras continue to provide increasing resolution, NVR technology can receive and decode without needing to be modified. NVRs can operate on almost any network topology, including wireless systems. You can install and configure effectively an unlimited number of servers for this purpose. Since the NVR is a server, it can be mirrored, providing you with backup and recovery capability of the stored images, thus preventing loss of the information in the event a server disk goes bad. Also, if the failure is in the server itself and not on the disk, the disk can be pulled and put into another server without losing the data. The typical cost to replace a failed DVR is the same as the unit cost, as they usually need to be replaced at a price that can be in the thousands. The same failure in a disk drive on an NVR server is only a couple of hundred dollars.

Computer industry leaders are making great strides in storage technology. The future of the NVR will be significantly impacted by these developments. Companies like CISCO and IBM, to name a few, are taking traditional IT storage ideas used in the data

network world and applying them to traditional video.

Reprinted from:
Security Technology & Design
August 2007

How Young Is Too Young For a Cell Phone

By Max Anderson



Are We Taking Cell Phone Usage Too Far?

The other day at the playground, I watched as what looked like a 5-year-old girl answered a cell phone call from her grandmother. No, it wasn't her mom or dad's cell phone she was using -- it was her own. Which raised the question -- are kindergartners too young to have their own cell phones? The answer may surprise you.

Practicality Counts

Listen, anyone who knows me knows that I'm not one for the overindulgence of children. In fact, I think the excess of spoiling our children is the reason why we have so many disrespectful irresponsible young adults running around today. That being said, however, I do honestly think that giving a cell phone to children of all ages isn't really a bad idea.

A Changing World

We have to admit the fact that we live in a changing world and the cell phone is a big part of that world. Years ago when I was little, I remember getting lost at an amusement park. What seemed like hours later, I was reunited with my mom. What if my mom and I had both had cell phones that day?

Think about it. You're at the mall with your 7-year-old and suddenly he's not next to you anymore. Instead of the panic attack most parents experience at this point, you simply call your son's cell phone. He answers, you find out exactly where he is and you go get him. No harm, no foul.

Or what about this... Your 12-year-old is at soccer practice and you're going to be about five minutes late picking him up due to an accident that slowed traffic. You call your son on his cell phone and tell him you're running late and to wait for you. Now your son doesn't worry when you don't show up right on time and you don't worry about your son having to worry.

Let's face it -- we all have enough stress in our lives when we're parents. If a cell phone can reduce that stress, I'm all for it.

Not All Cell Phones Are Created Equal

It is important to realize that not all cell phones are created equal. I do not advocate getting a flip phone with a camera and a mp3 player for a 1st grader. In their case, a Firefly or Migo will do. There are a number of age-appropriate cell phone options on the market. If you have kids, I suggest looking into them and getting them a cell phone that suits their needs and their age.

Reprinted from:
From Consumer Tips and Reports
July 2007

Cell Phone Safety Tips

August 24, 2007

As the technology improves, we increasingly rely on our cell phones for more than just making calls; we're using them to send e-mails, schedule meetings and surf the Internet. The Better Business Bureau (BBB) warns that the downside of having a little computer in your pocket is that, just like with the computer on your desk, there are people out there ready, willing and able to exploit it.



An estimated 600,000 cell phones will be reported lost or stolen this year. If your phone lands in the wrong hands, you're not only saying goodbye to all your contacts but you're potentially facing a very high phone bill. Some victims report having received bills for more than \$25,000 after their phone was stolen.

Even if your phone never leaves your side, it's still vulnerable to hackers -- or phreakers as they're called. Phreakers, by just walking past you, can hack into your cell phone and listen in on your calls or steal personal information without your knowledge. They do this by exploiting the short-range Bluetooth wireless connections between cell phones and hands-free headsets or PCs. Phreakers can also spread viruses through text messages, e-mails and memory cards.

- Don't lose it. Your best defense against thieves and hackers is to keep close tabs on your cell phone. If other people can't get their hands on it, they're going to have a much harder time trying to take advantage of it.

- Contact your cell phone provider as soon as your cell phone is lost or you think it's been hacked. If your cell phone is lost or stolen you'll want to discontinue service immediately before the thief can run up a big bill. Check your provider's policy because, while they may offer to cover charges if the phone is stolen, they are not required to and you could be held responsible.
- Password protect your phone. Locking and password protecting your phone is just as important as having passwords on your computer.
- Turn off your Bluetooth. Disabling your Bluetooth wireless connection when you're not using it will significantly decrease a phreaker's opportunity to wirelessly hack into your phone.
- Download anti-virus software and keep it updated. New viruses are created every day, so it's important to have anti-virus software on your cell phone—if it's available for your model—and update it regularly.
- Don't accept files and text messages from strangers. You wouldn't download an attachment to an e-mail you received from a stranger to your PC. For the same reason you want to be very careful about opening unsolicited files and text messages on your cell phone.



If you are interested in having First Aid Training or Defensive Driving Training for your staff, contact Amalgamated Security

Bluesnarfing



By: Brian Ramsey

Many individuals seem to be in love with their cell phones and immediately as a new model is released, they rush to get that model. Some of the features available on cell phones definitely make our lives easier and more productive. One of the extremely popular features is Bluetooth that allows cell phones and PDAs to connect and exchange information between each other and with devices such as PCs, printers and digital cameras. Bluetooth enables these devices to communicate with each other when they are in range. The devices use a radio communications system, so they do not have to be in line of sight of each other, and can even be in other rooms, as long as the received transmission is powerful enough. Most people take their Bluetooth devices for granted and the feature is left ON whether they use it or not. It has however been discovered that there are serious flaws in Bluetooth security that could lead to disclosure of personal data.

The weakness was discovered by Adam Laurie of The Bunker, who found that there are

serious flaws in the authentication and/or data transfer mechanisms on some Bluetooth enabled devices. The exploitation of this weakness has been given the name **Bluesnarfing** and is very popular in the United Kingdom and the United States and is now being done in Trinidad. It is being done on particular models of cell phones, PDAs and laptops and is usually done in crowded areas restaurants, bars, and popular internet hotspots. According to Laurie, "three vulnerabilities have been found:

Firstly, confidential data can be obtained, anonymously, and without the owner's knowledge or consent, from some Bluetooth enabled mobile phones. This data includes, at least, the entire phonebook and calendar, and the phone's IMEI. Secondly, it has been found that the complete memory contents of some mobile phones can be accessed by a previously trusted ("paired") device that has since been removed from the trusted list. This data includes not only the phonebook and calendar, but media files such as pictures and text messages. In essence, the entire device can be "backed up" to an attacker's own system. Thirdly, access can be gained to the AT command set of the device, giving full access to the higher level commands and channels, such as data, voice and messaging". Under this third vulnerability it is possible to use the **Bluesnarfed phone** to initiate calls to premium rate numbers, send sms messages, read sms messages, connect to data services such as the Internet, and even monitor conversations in the vicinity of the phone.

The manner in which these vulnerabilities are exploited are known as a Snarf Attack and a

Bluebug Attack. Laurie indicates that under a Snarf attack "it is possible, on some makes of device, to connect to the device without alerting the owner of the target device of the request, and gain access to restricted portions of the stored data therein, including the entire phonebook (and any images or other data associated with the entries), calendar, realtime clock, business card, properties, change log, IMEI (International Mobile Equipment Identity, which uniquely identifies the phone to the mobile network, and is used in illegal phone 'cloning'). This is normally only possible if the device is in "discoverable" or "visible" mode, but there are tools available on the Internet that allow even this safety net to be bypassed".

The Bluebug attack creates a serial profile connection to the device, thereby giving full access to the AT command set, which can then be exploited using standard off the shelf tools, such as PPP for networking and gnokii for messaging, contact management, diverts and initiating calls. With this facility, it is possible to use the phone to initiate calls to premium rate numbers, send sms messages, read sms messages, connect to data services such as the Internet, and even monitor conversations in the vicinity of the phone. This latter is done via a voice call over the GSM network, so the listening post can be anywhere in the world. Bluetooth access is only required for a few seconds in order to set up the call. Call forwarding diverts can be set up, allowing the owner's incoming calls to be intercepted, either to provide a channel for calls to more expensive destinations, or for

identity theft by impersonation of the victim.

Another exploitation of the Bluetooth weakness is known as Bluejacking and has become a popular mechanism for exchanging anonymous messages in public places. With Bluejacking the messages are passed between two individuals using a third person's phone.

The issue for most people will be how to stop their phones and PDAs from being Bluesnarfed and Bluejacked. The initial advice that was given was to set set your phone to 'Undiscoverable' in your Bluetooth menu. This "Undiscoverable" setting allows you to keep Bluetooth on so you can use compatible Bluetooth products, e.g. headsets, computer dongles, but other Bluetooth devices won't discover your device when they're searching for devices. There are however tools on the internet that allow the unscrupulous individuals to discover phones set on the "Undiscoverable" setting. It is now recommended that the Bluetooth feature should be turned Off until you are ready to use it and then turned OFF when you have finished using it.

About the Author:

Brian Ramsey is the Regional Development Director at Amalgamated Security Services

Amalgamated Security provides a full range of security services, which include:
Cash Services
Electronic Security
Access Control
Data Storage
Courier Services
Guarding Services
Alarm Monitoring
Response Services