

- ▶ EDITOR'S COMMENTS 1
- ▶ VoIP Wiretapping Widespread 1
- ▶ Insider Security Threats come in many forms 4
- ▶ Cover Your Assets 4
- ▶ Speaking Encode ..7
- ▶ What's inside your house9

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE.

Helping secure your world

As we publish our second issue of **SECURITY SOLUTIONS** one fact must be recognized, Crime is not going away. Some organizations recognized that fact early and invested in security systems that included CCTV. As technology changes and there are more capabilities with newer equipment, some companies are faced with a challenge of what to do with their older CCTV equipment. We have therefore included an article that points out how to integrate older legacy systems with newer IP devices.

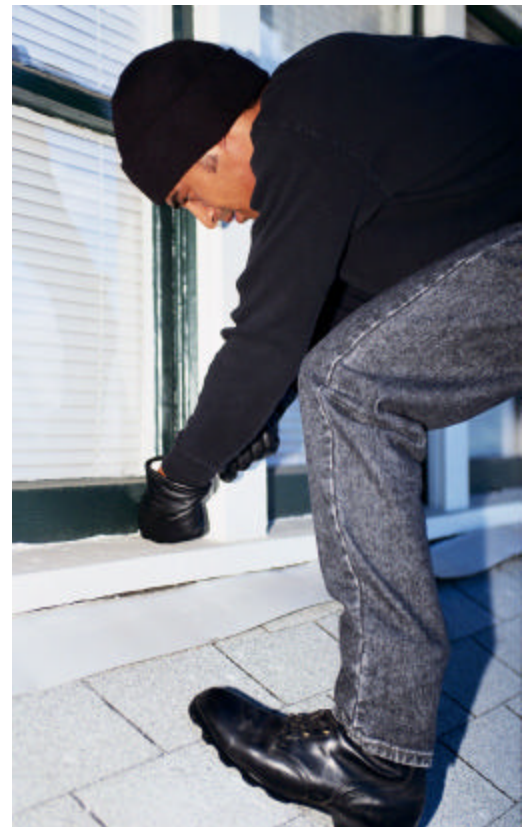
Even as companies grapple with security issues they must also contend with the cost of operating their business. In an effort to curtail rising telecommunication costs many companies have either switched to or are contemplating switching to VoIP systems.

Even in this arena however there are security issues to contend with and so we have included an article on the wiretapping risks with VoIP.

Unfortunately crime is not confined to the office environment and so in each issue we include a Personal Security section. In this issue we look at the risks associated with the persons who come to your home.

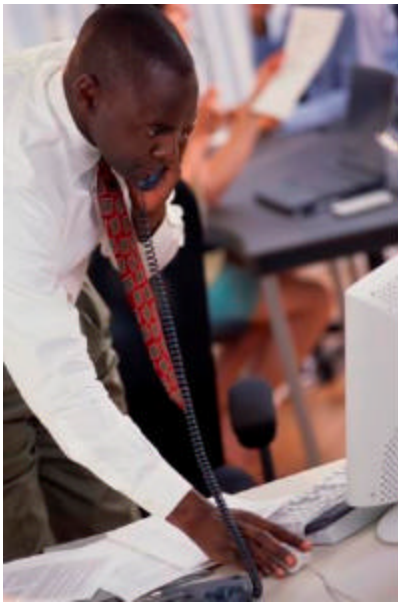
If any additional persons in your organization would like to receive this email newsletter just send an email to newsletter@assl.com with the words "Subscribe Newsletter" in the subject line and the email address, name and organization in the body. To opt out of the mailing list send an email with the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

Brian Ramsey
Editor



VoIP Wiretapping Widespread, Warns Security Firm

Firm points to lax security on company phones, new tools for hackers that simplify breaches



VoIP Wiretapping Widespread

"The most common reason in large companies is because no-one understood how to secure the system. Staff lacked adequate skills and understanding of the security aspects of the implementation itself. They relied on the vendor or system integrator to set the whole system up."

Security specialist Scanit says it has come across several popular installations being used in corporate environments without security in place to prevent VoIP wiretapping.

"Throughout the Middle East, the installations we have seen have not had strong security controls in place," Scanit engineer Sheran Gunasekera explains. "Primarily, the reason for this has been the fact that the system integrator or implementer had not paid much attention to the security of the entire setup."

It is possible, Scanit says, for an internal employee of the organisation, to intercept voice conversations and re-route calls outside of the firm's network. According to Sheran, a high percentage of installations he has audited had no encryption on the voice stream. There can be several reasons that a corporation or service provider will run an unsecured implementation, he explains.

In turn, the vendor's focus was on functionality of the system rather than security, Sheran says, and so a working system with no security was deployed.

So, how does a hacker find and exploit unprotected web calls?

"When a user first starts up his VoIP, it looks for a SIP Registrar - comparable to a traditional telephone exchange - to register and identify itself on the internet, by way of an IP Address, and to show the user is now contactable," Sheran explains. "If a SIP Registrar is set up with no consideration given to security, it is possible for a malicious user to imitate a legitimate registration request."

The Registrar itself will assume that this is a legitimate registration request because all the fields will be filled out correctly.

"The only difference is

the fact that the destination IP address has changed." It is comparable to changing your mailing address when your name and other details stay the same, he says. "If no steps are taken to verify the new address provided, then your mail will be delivered to this new address, which could be owned by someone else."

There are several safeguards to prevent this, like using encryption and strong authentication for requests with the SIP Registrar. The owner of the VoIP deployment (normally the corporation or service provider) will run one or many SIP registrars and it is the sole responsibility of the party that owns the VoIP implementation to ensure that it is secure, Sheran says.

"If it is a corporation, then the corporate IT security teams will have to ensure this. Security becomes a more serious issue when VoIP service providers are involved. This is because the service is sold to end-users."

There is a greater potential for abuse due to the varied user-base that the VoIP implementation is exposed to.

SMARTER SECURITY:
Experience & Discipline



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

In order to intercept Real-time Transport Protocol streams (or RTP, a standardised packet format for delivering audio over the web), a hacker needs to be physically connected to the network where other users make and receive VoIP calls. RTP streams are usually encoded with a specific codec. Popular tools like WireShark are able to detect when an RTP stream is traversing a network.

Sometimes if the Voice traffic is not segregated from the data, it is sufficient to run a "sniffer" like WireShark in order to capture the RTP streams. A program called Cain & Abel even allows direct saving to a .WAV file for playback. An attacker can capture any sound that travels over a VoIP conversation. This may be an entered PIN, confidential information relating to either financial or personal matters can be captured and listened to. Information such as confidential financial transactions with regard to mergers or acquisitions or personal information that can be used to blackmail people is also included.

According to Sheran, the threat of your VoIP calls being intercepted is made higher still by the low skills levels required to tap into such conversations.

"With the availability of these tools, you do not need to be very highly skilled. You just need to have a basic understanding of how VoIP works and a little bit of network knowledge," he says.

Some commercial VoIP services have taken commendable steps to ensure the privacy of their users' calls, Sheran says.

"Skype, for example, uses proprietary protocols for both signalling and for voice streams. It is significantly harder to sniff Skype traffic due to the encryption used in the protocol."

An example of an unprotected line Scanit engineers uncovered was while they were performing an internal audit for a large Middle - Eastern bank."

Their VoIP implementation used Virtual LANs to segregate specific voice streams for different departments. By connecting to a completely different VLAN reserved for consultants of the bank (with no access to other critical infrastructure servers) we were able to hop onto different VLANs and capture traffic from

from the CEO's office," Sheran says.

The security outfit puts the number of unsecured VoIP calls that could be exploited by hackers at 70 per cent.

"Within the region we work in, I can say that we are looking at high percentage figures of insecure VoIP calls," Sheran says. "Nearly three quarters of the corporate deployments we have audited have been exploitable from the inside."

Security experts around the world are rising to the challenge that unsecured VoIP networks pose. Phil Zimmermann - the legendary author of PGP, a program that offers the common email user military-spec encryption - told the Defcon hacker convention in the US this summer "point-and-click wiretapping" is being used "by organised criminals on the other side of the world". His response was to release Zfone, his own privately-developed software, which scrambles VoIP conversations from end-to-end. Taking matters into his own hands was a necessary step to protect his own VoIP conversations against eavesdropping. But not everyone supports such proactive measures. The Bush administration this year used a 1994 surveillance law to demand ISPs provide backdoors for government wiretapping of VoIP calls, citing terrorist and drug criminal usage.

"Encrypting VoIP is now more important than ever because computer networks are not nearly as safe as the public switched telephone network," Zimmermann says. However, even if the software you use to make VoIP calls offers a high level of encryption, the hardware connecting your system to the web may already have opened them up to eavesdropping.

The FBI drafted legislation in July to force makers of networking gear to build in backdoors allowing them access to all data going in and out. Sooner or later, and despite the best efforts of security companies to protect VoIP users from hackers, such a loophole will also leave the door open to hackers.

Concerns are being expressed from all sides. The Federal Deposit Insurance Corporation (FDIC) warned earlier this year: "If improperly implemented, VoIP can pose significant risks to financial institutions. Therefore, management should perform a comprehensive risk assessment before implementation to ensure the confidentiality, integrity and availability of voice communication using VoIP technology."

Among FDIC's recommendations is a caution against using "soft phones"; that is VoIP via desktop computer, using headphones and calling software, and pushing home the need for VoIP-ready firewalls. As VoIP deployments are gaining steam in enterprises of all sizes, tech analysts IDC estimate that revenue for network and premises-based VoIP services will grow from \$2.9 billion to \$6.9 billion over the next five years.

The electronic gold rush associated with VoIP means "companies eager to tap into its ROI without fully considering the security risks stemming from weaknesses in VoIP applications, operating systems, and structure and supporting services spells a huge opportunity for hackers," says David Endler, director of security research at 3Com. Cisco Systems has sold millions of VoIP phones, and research firm Gartner predicts that in four years, 30 per cent of US homes will use only VoIP or cellular phones. It is unsurprising that security is left playing catch-up.



"The problem lies in the session-initiation protocol, the leading signalling protocol for VoIP," Chris Rouland of ISS security explains. "SIP is similar to HTTP and SMTP; it's lightweight and easy to use. It's basically taking the world by storm, and it's inherently no more secure than existing protocols that have been completely taken over."

The sooner businesses can protect themselves and their customers from the threat of having their VoIP calls intercepted the better, because, as Gregory Lebovitz, technical director and solutions architect at Juniper Networks points out, there's nothing stopping them from running riot at the moment.

"No anti-intrusion or firewall currently supports all VoIP protocols and technologies," said Lebovitz, "and if they claim to, they're lying." Ψ

Reprinted from
Security Info Watch
December 2006

Insider security threats come in many forms

By Bill Brenner, Senior News Writer

As far as Kerry Anderson is concerned, insiders are as big a threat to her company's IT security as worms and spyware -- perhaps bigger. And like malware, insiders come in many variants.

Anderson, a vice president in the information security group at Fidelity Investments Brokerage Company, explained the different types of insider threats and ways companies can address them at the MIS Training Institute's Annual Conference and Expo

on Control and Audit of Information Technology in Boston last week. The best way to deal with any potential inside threat, she said, is to let everyone know Big Brother is watching them and that they can be fired for any security violation.

"Companies need to make it clear to their employees from day one that they are being monitored," she said.

Anderson has seen a variety of troublesome insiders in her career at Fidelity and other companies. There's the saboteur who tries to deface critical company data because they have an axe to grind against their bosses or fellow co-workers.

Then there's the sole living expert -- someone who has been around so long they think they own the network. They want everyone to be dependent on them, so they manipulate the network in a way to make other employees come to them to access certain pieces of data or perform certain network functions, Anderson said.

Anderson has also come across people who have what she calls the hero syndrome. They break something on the network so they can fix it and be seen as life savers.

"If something is breaking every three weeks and the same person is fixing it, I'd start taking a look at them," she said.

Whatever the insider's tactics or motives may be, Anderson said there are some common warning signs to look for, such as someone who isn't getting along with managers or co-workers and may be preparing to leave the company. If someone is leaving under unhappy circumstances, there's always the chance they could sabotage network data on the way out the door, she said.



Companies must also keep an eye on people who may start working hours when nobody else is around. Anyone who suddenly changes their normal work routine bears watching, Anderson said.

Companies must also be prepared to deal with people who create security risks without necessarily meaning to. If the network suffers a security breach because an employee was visiting seedy Web sites on company machinery, for example, there must be a plan for punishment.

"People need to understand that their computers are for business only and that they can be disciplined or even fired for using them for anything that isn't business related," Anderson said.

IT security professionals also need to watch for personal technology that could put the company at risk, she said. Cell phones with embedded cameras, for example, could be used to photograph and transmit sensitive data.

While these are important steps, Anderson acknowledged that companies can't prevent every insider-related incident.

"A lot of internal fraud goes unreported because it's embarrassing," she said.

If there is a security breach, companies must be honest about it and come clean publicly, she said. Otherwise, the company's reputation and the security of their customers could take a bigger hit later. Ψ

Reprinted from
SearchSecurity.com
21 Nov 2006

Cover Your Assets

DVRs can play role in controlling loss in a variety of industries

By Bob McCarthy

THE cost of lost assets to companies has been demonstrated in many studies to be significant. The application of DVR technology has been proven to reduce this type of loss in a cost-effective manner.

Asset theft and damage begins as a risk to manufacturers, distributors and shipping companies. Companies can expect to see a portion of the goods damaged or stolen when moved from the raw materials vendor, to the manufacturing site, to distribution centers and finally to retail outlets.

In addition to finished goods, manufacturers must protect raw inputs, which can be high value. Whether these assets are hard drives for DVRs or copper coils for air conditioners, manufacturers must guard assets against burglaries and employee theft. An integrated combination of DVRs, burglar alarms and access control systems act together as an effective deterrent and a tool to identify and prosecute offenders.

After manufacturing, products are shipped by various methods to customers or channel partners. The success of intermediate warehouses and cargo storage facilities is based on the ability to provide clients with an environment that is both safe from the elements and secure from damage or theft.

Securing Cargo

A major U.S. cargo handling service is the custodian of freight that comes through warehouses until it leaves.

The handler must consistently prove its capability to keep freight secure to protect its integrity as a freight handler.

Staff monitors multi-city sites on a 24/7 basis using Dedicated Micros' DVRs and network viewers. The system is used for theft deterrence, resolution of insurance disputes and as a marketing tool to show operations to prospective customers.

For assets in transit between manufacturers, distributors and retailers, even shipping vehicles can benefit from mobile DVR surveillance. The DVRs can embed GPS data in the video and trigger alarms when the vehicles stray from scheduled routes due to truck hijackings. Some even have a built-in inertia sensor that can mark when the vehicle stops or swerves suddenly, potentially causing damage to goods.

At the retail store level, several studies have shown that inventory losses have a significant impact on corporate profitability.

Retail Shrinkage

In the U.S. retail industry alone, an estimated \$37.4 billion is lost to shrinkage each year according to the 2005 National Retail Security survey conducted by the Security Research Project at the University of Florida. Forty-seven percent of the loss is attributed to employee theft, far outweighing the cost of shoplifting (33 percent) to retailers. The total loss equates to an average of 1.59 percent of sales across all retailers, but this percentage is significantly higher in certain segments of the market such as supermarkets (2.38 percent).



According to the 17th Annual Retail Theft survey conducted by Jack L. Hayes International, only 2.74 percent of retail theft losses were recovered in 2004.

The emergence of organized retail theft has increased the risk to assets in a broad range of industries. Criminals are targeting high-value assets from manufacturers, transporters, distributors and retailers.

According to the 2005 National Retail Theft survey, the average loss attributed to each non-employee, shoplifting theft incident has risen from \$265.40 in 2003 to \$802.83 in 2005. It is believed organized retail theft is at least partly responsible for the increase because of the high value of assets lost in ORT-related incidents.

DVR systems have become an invaluable tool in many organizations' efforts to improve the bottom line by reducing asset losses. Depending on the business, the largest threat of loss may come from employee fraud, product theft or damage/vandalism to vehicles and other assets used to conduct business.

IP-enabled DVRs allow businesses to deploy sophisticated asset protection measures with minimal investment and complexity. When integrated with other asset management systems, DVRs can reduce the level of asset theft and/or damage. The payback period on DVR-based, asset management investments can be short for companies currently operating with minimal protection.

A growing trend is to use networked DVRs to monitor assets and investigate incidents remotely from a centralized loss prevention/asset protection facility.

The approach allows for immediate access to live video or incident footage without the expense or delay of traveling to the scene of the incident.

Integrated Improvements

Simple monitoring of assets with DVRs will deter theft and help prosecute thieves, but the full benefit is gained when DVRs are integrated with point-of-sale, loss prevention, access control and other systems and sensors. Since the days of VCR surveillance systems, it has been recognized that the integration of POS systems with video is an effective way to discourage cashier theft and to identify problem employees. Modern DVRs can offer much more automation when integrated directly with POS systems than using the technique of overlaying transaction data from the receipt printer onto a VCR's video.

DVRs can now be triggered by suspicious transactions ("void," "no sale," "refund," etc.). The units also can use motion or other sensors to increase record rate to reposition a PTZ camera onto a specific area or to notify a centralized monitoring center of the incident in real-time. Just as importantly, the video associated with the incidents can be rapidly found in follow-up investigations when required.

Certain retail verticals have specific applications. Gas stations monitor for drive-offs (obtaining a clear shot of the license plate). Car dealerships monitor vulnerable fleets of new vehicles to discourage and record incidents of **vandalism**.

Some companies also use DVRs to reduce asset damage by monitoring adherence to operational procedures.

Reduction of theft by DVR-based asset protection systems, combined with visible cameras, has three primary components.

- Reduced theft due to fear of getting caught.
- Real-time notification of suspicious sales transactions, unauthorized access to storage facilities and improper use of assets.
- A detailed trends analysis to identify and investigate improper asset handling or transactions.

Containing Cash

Many other industries are now taking advantage of IP-enabled DVRs to reduce asset losses and improve financial performance.

A banking institution's whose main asset is cash and its use of DVRs is to combat robberies and prevent customer fraud. Many banks use hybrid DVRs -- those that can accept both analog and IP cameras -- with high-resolution IP cameras to replace the old 35 millimeter, analog film cameras that watch doorways and teller lines. These megapixel, IP cameras allow investigators to digitally zoom in on recorded video to increase the likelihood of identifying suspects.

Banks also use DVRs to capture video of ATM and teller-line transactions in order to capture fraudulent transactions. As this transaction video is typically saved for 90 or more days, it is critical that the DVR embed the transaction data within the video so disputed transactions can be quickly found. Specialty interface equipment is required to intercept transaction data from the many ATMs that still use legacy, bi-sync communications linked to bank mainframes.

Monitoring Infrastructure

Utilities make extensive use of DVRs to monitor assets. For these companies, the main assets is the infrastructure, as the loss of assets results in both replacement costs and lost service revenues. IP-enabled DVRs allow utility

operators to view key facilities in the electrical, gas, water, telephone or other networks remotely and instantly after sensors detect problems.

The risks to utility assets are more likely vandalism- or weather-related (flooding, lightning, high winds, high temperatures), rather than theft. But remote video monitors integrated with the proper sensors can reduce asset damage by allowing rapid assessment and resolution of the problem.

Many applications require real-time notification of asset problems while others are simply collecting information for use in investigations and/or trend analysis.

Not all DVRs are well-suited for asset management applications, and each organization considering a DVR deployment will have a unique set of asset management requirements. In general, users should look for a DVR solution that addresses the most common asset management requirements along with flexible configuration and integration capabilities.

A Feature Combination

The asset management features to look for today include some of the time-tested basics and some new application-specific capabilities.

For integration with POS and ATM transactions, the DVR must be able to embed data in video images. The technology can include RFID tags, bar codes, GPS or weight scale data that is time-stamped and associated with one or more video cameras.

The DVR should have a flexible set of alarm triggers that includes video motion detection, transaction text keyword matches and physical alarm inputs.

When alarms are triggered, the DVR should offer a flexible set of reactions to include increased record rates, increased resolution and reduced compression (for higher quality) on the individual cameras associated with the alarm.

DVRs with a software development kit allow the vendor or approved partners to develop custom software integrations with sales and inventory systems, providing an open architecture solution for customers.

While many legacy asset management systems require a direct, physical connection for integration, newer systems require communication over TCP/IP, with IP-enabled DVRs. Look for a manufacturer that offers integrations with the most popular POS systems and resources to add custom solutions quickly.

The effort required to manage and maintain DVR systems varies widely among vendors, so this aspect of the system should be evaluated carefully. A centralized management tool should be available for viewing permission assignments, software upgrades and DVR configurations backup and restoration across the entire security network.

Use of an embedded operating system instead of a PC-based DVR will reduce maintenance costs by removing the need to install monthly operating system patches. The vendor also should offer a health monitor for automated, proactive notification of maintenance or repair requirements.

Lastly, hold out for a DVR that offers easy identification, extraction and presentation of video evidence. Since the video of theft or damage to assets will be needed for investigations, it is imperative that the DVR provide search tools to easily find incident video for investigations.

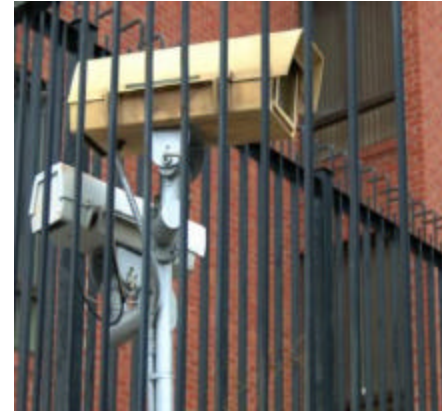
The DVR also should provide an easy method of creating auto-run evidence CDs (or DVDs), and proven methods must be employed to demonstrate there has been no tampering of the video on the evidence CDs since extraction from the DVR.

From commercial goods to utility infrastructures, the assets of modern businesses can benefit from increased protection and decreased losses by the implementation of an effective, DVR-based security system. The most effective implementations will be integrated with other asset management/protection systems and will have purpose-designed application software to provide effective and intuitive operation of the system. Ψ

Reprinted from
Security Products
November 2006

Remember to send your emails to newsletter@assl.com to add individuals to the circulation list

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



Speaking Encode

TODAY'S world is faced with every-evolving technologies - a world of ones and zeroes. Digital communication and storage networks have greatly facilitated access to information in every technology sector, and video security is no exception. The growth of high-speed IP networking has enabled the creation of highly-flexible video security systems with compact, digital cameras that can pan, tilt and zoom in on surrounding environments. With multiple digitally-networked IP cameras, a video security system can provide comprehensive observation of any sensitive area requiring video monitoring. Being able to view, save and transfer video digitally via Ethernet network feeding monitors and a server is far more easy and efficient than recording video to analog tapes.

Whether for reasons of cost, convenience or size, however, analog security cameras need not become obsolete when integrating IP networks with existing video security systems. When making the transition from an analog system to a digital one, no one wants to simply discard existing cameras in working order. As companies continue to make the transition to IP, equipment that can help get extra mileage from analog cameras has become more vital.

Right Tools for the Job

There are various ways to integrate legacy cameras into an IP video security network. One such method of integration is via an external module that acts as an encoder and allows the connection of analog cameras into the digital network. Canon's VB-EX50 multi-terminal module contains inputs and outputs for audio and video that allow an analog signal to be encoded and sent over the network.

The video input enables users to connect a single analog camera, or any video input device that needs to be transmitted over the Web, to a networked camera and use the networked camera itself to encode external source video. From a remote location where a user is watching the video source, he or she can select which video source location they want to see.

The multi-terminal module is easy to integrate into an existing camera system. It simply plugs into the back of a network video camera, and then the existing analog camera is plugged in. Voila, instant IP video.

Expanded Capabilities

In conjunction with video input, the audio input and output allows a camera to be used more effectively at a point of entrance. An analog camera can be installed at any entrance where a remote observer can listen from a monitoring station and -- at the touch of a button -- communicate via a microphone attached to their desktop or laptop. The voice data will transmit over the network to an external speaker at the camera's location where the entrant can respond. The feature is also useful for such applications as customer-service monitoring, event Webcasting and video conferencing.

In addition, a pre-recorded audio file can be played at the camera's location at scheduled times or when triggered by an event. In a security monitoring application, a powered speaker connected to the camera can play back a pre-recorded message any time visitors approach

a restricted area. Or, a department store can alert customers to special sales promotions at preset intervals.

For users with multiple analog cameras, use of a network camera server makes it easy to transmit full-motion, 640- x 480-pixel, real-time video over the Internet or intranet. Users can connect up to four analog cameras and also take advantage of the option for possible wireless networking. The server then encodes the signal from the connected analog cameras and transmits it via the Internet or an intranet.

Many specialty cameras used in security, such as small, hidden cameras used to detect theft, do not have IP capability. Storeowners, for example, may prefer to integrate these valuable, lipstick-sized cameras into the IP network. An encoder allows them to do just that, creating a seamless integration of all video inputs onto the digital server.

Integration with Ease

With any a system upgrade, ease of installation is a critical factor. Integration of the server is as simple as going to the location where all the cables terminate and plugging into the existing system. Users can then easily employ a splitter to keep recording to a DVR or VCR, and at the same time, the video source will be encoded over the Web. Remotely, users can now access the server and potentially access all cameras installed.

With any security system, there will be incidents where simply monitoring an area is not enough. As an additional feature and valuable benefit, some cameras come equipped with connectors for alarm contacts -- such as door contacts or motion detection -- that can be activated with various kinds of triggers. When used in conjunction with door contacts or motion detection, an incident can trigger a PTZ camera to a specific, pre-determined view while the output relay triggers an alarm light or signal.

The world of video security is changing rapidly. As IP video continues to strengthen its foothold in the industry, analog cameras will need to be modified or phased out. Transitional technology allows companies to get as much life as possible from the original investment by creating a means for analog cameras to transmit video as an integrated part of an IP network. By using inexpensive options, users can efficiently manage the gradual transition from a wholly analog video security system to a digital system. Ψ

Reprinted from
Security Products
January 2007

Remember to send your emails to newsletter@assl.com to add individuals to the circulation list

What Lurks Outside Your House is Sometimes Not as Bad as What is Already Inside It

By: Gordon Basichis

Who has been hanging around your house? Seems like a simple question, but when you stop to think about all the people who cross your threshold in the course of a year, then you really don't know, do you?

Chances are you feel protected from intrusion. If you own a house you may have an electronic security system. Probably there is a Neighborhood Watch in your area. The police are just a phone call away and everyone in your building or on your street always seem so nice.

If you are a single parent, chances are you have housekeepers and nannies looking out for your children. If you are a homeowner, then chances are you have contractors and their workman coming and going. Sure the contractor may be thoroughly licensed. But what about the people they hire? Who looks into their backgrounds to see if they are who they really say they are and what they are all about?

If you are dating, then chances are new romantic prospects are coming by your place to pick you up. They may be interested in only you. They may be even more interested in your children? How can you really tell?

It may sound distracting and even annoying to bother looking into the people other than your family who populate your home. Let's face, it is tough to take time from our modern busy schedules to bother verifying people and their histories. We have to make a serious effort, and then we have to confront the results of our research. Certain people may turn out to be other than who we supposed they are. Then what?



That seemingly gifted plumber who will even make night calls may be used to working nights, since his last profession was burglary. It may matter; and then it may not. How about the new guy working for the contractor who is redoing your kitchen, the one adjacent to the master bedroom? Where you keep your jewelry and natural possessions. Yeah, what about him?

This article is not designed to make you paranoid or render you so full of fear you forbid anyone access to your house. What it is designed to do is to point out the different places in your daily life where you are vulnerable to theft and possible bodily harm. Sure, we all know about street crime, burglars, scam artists and having the misfortune of encountering someone of a violent nature. The thing is, most of us never take the necessary precautions, the available precautions on the people who can con us, harm us and steal from us.

If you have a contractor working on your house, then research his business references and, above all, make sure he is licensed and bonded to perform the services for which he was hired. You should do the same for nannies and housekeepers. Avoid tragedies by running criminal checks, credit checks, and check out their license, if necessary. Doing so will help you avoid costly and often tragic mistakes. The last thing you need is to be telling sad stories on the six o'clock news.

I could go on all day about how many women who use online dating services are snookered by the scam artists who design everything to appeal only to you....and maybe the next dozen or so women they encounter. Reveal the wrong information, invite them over to your place, and you may discover months in the future that you are now a victim of identity theft. If you have children then the last thing you need is to be allowing pedophiles the chance to get near your kids. Check out your state's sexual offenders registry. It's free. And for a nominal charge you can run the search in the sexual offender's registry in all fifty states. Many have, and many are grateful that they have done so.

Your home is supposed to be your one secure spot in a messed up world. You are supposed to be able to relax, attend to your hobbies, have love affairs, and be with your children in peace and safety. You are not supposed to be concerned about interlopers, molesters and thieves posing as workmen or nannies. We may have forgotten that there are, after all, certain rights to which we are entitled. Only today, to protect those rights, there is a price. Often the ounce of prevention is gotten for a nominal fee. The cure can be very costly.

So do yourself a favor and do the homework on the people you have working for you and maybe even the person whom you are dating. There are all kinds of research tools available, and there are many respectable background checking services. There may be an effort in protecting self and family, but then what did you expect in this life? The cost is nominal. And the peace of mine, to quote a credit card commercial, is priceless. **Ψ**