



**ÆGIS** e-journal

***Addressing threats that affect your bottom line***

Volume 4 Number 12, December 2001

From the case files of

**The LUBRINCO Group**

<http://www.lubrinco.com/>

and

**Financial Examinations and Evaluations, Inc.**

<http://www.feeinc.com/>

**Intellectual property being stolen or at risk? Call us!**

**This month's features:**

- 1. Due Diligence — Workplace violence is a serious problem**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Using outside sources to help establish an OPSEC program**
- 3. Executive Protection — The real deal about nuclear, chemical, and biological warfare**
- 4. Technical Issues — The twenty most critical internet security vulnerabilities: The experts' consensus**
- 5. Real Stories from the Field — Unprofessional practices, unprofessional behavior**
- 6. Book and Product Reviews — CopyTele DCS-1200 and USS-900**
- 7. Free-Subscription/Unsubscription/Copyright Information**

## **1. Due Diligence — Workplace violence is a serious problem**

Contributed by Jay Crawford, CPP, <http://home.switchboard.com/jbcrawfordCPP> (jbcrawford@hotmail.com). Contributed articles do not necessarily reflect the viewpoint of the ÆGIS e-journal.

Editors note: There are three classes of workplace violence. The most common is crime that spills over into the workplace. Examples of this are convenience stores or gas stations being robbed, or cops injured by criminals. The second most common is domestic violence that spills over into the workplace (the domestic partner shows up at the workplace and injures the employee, and possibly those that try to protect the employee). The least common is an employee or customer becoming violent.

Pick up the newspaper and chances are you will find an announcement that a small, medium, or large-sized company is laying off employees.

Downsizing, increased workload and questions concerning the future are causing stress and worry in today's workforce.

Each workday an estimated 16,400 threats are made, 723 workers are attacked, and 43,800 are harassed, according to the Workplace Violence Institute. According to OSHA, more than 1,000 workers are victims of homicide at work. The US Department of Justice says about 2,000,000 assaults and threats occur each year in the workplace. Estimates are that workplace violence costs businesses as much as \$4.2 billion annually. A spouse, ex-spouse, boyfriend/girlfriend or relative is the victim in one out of ten incidents of workplace violence, according to the Society of Victimized Employees for Human Resource Management.

It's no wonder then that workplace violence, and the trauma caused by such events, has been the leading concern of security managers at America's largest corporations for the last three years, according to recent surveys.

Employee willingness to work non-standard hours and a changing demography of the workforce has added to work and travel risk.

Fundamentally, there is only one cause of loss: Inadequate protection of assets. Employers have a legal obligation to provide a safe working environment to employees. Organizations should be proactive to reduce their exposure to costly workers' compensation claims and/or civil lawsuits and large damage awards for incidents of workplace violence. Unfortunately, it is difficult for some company executives to believe it can happen in their organization.

A two-pronged approach of prevention and protection can help guide business leaders safely through the turmoil while protecting their company's image, reputation, products and most important assets, their employees.

A workplace assessment of an organization is a good place to start. Businesses can call on experienced, proven professional security consultants, in addition to using in-house resources and public crime prevention opportunities. The advantage a consultant offers is that he/she can remain objective and apart from any office politics. Another immediate step a company can take is to implement a three-point company policy to reduce outbreaks of employee violence.

- Criminal, educational and employment background checks on potential employees and any current employees who were not checked upon being hired.
- A drug testing policy. *The National Institute on Drug Abuse* has reported that the typical employee abusing drugs was:
  - Five times more likely to file a claim for worker's compensation
  - Involved in accidents almost four times more than other employees
  - Took sick leave twice as often and others and
  - Late for work three times more often than employees not using drugs
- Establishment and enforcement of a solid non-harassment policy

Two points must be kept in mind when predicting who will commit an act of violence. First, no litmus test exists that can accurately predict potential incidents of violence. Second, it is important to know your employees. When a disgruntled employee goes off the deep end, it rarely comes as a surprise to his or her co-workers. Warning signs are almost always present and those who are in contact with the potentially violent person on a daily basis see these signs. Open lines of communications should be encouraged to allow management to deal with the problem before it becomes a tragedy.

To reduce the potential for workplace violence, employee-training programs should include issues such as stress management, how to handle confrontations and drug abuse awareness. Awareness training, additional supervisory training, annual physical vulnerability surveys and liaison with law enforcement can also help reduce the chances of violent acts on company property.

One should not overlook the importance of the above survey of the property. Much can be accomplished at little cost. Limiting and controlling access, rearranging offices and furniture, security awareness briefings and training, and security hardware can all contribute to reducing employee vulnerability to angry co-workers.

Again, companies must be prevention-oriented. Despite what one might read in the newspapers or see in movies or on TV, the workplace is still one of the safest places to be. Organizations must do their part by ensuring that they are actively taking measures to provide a safe and healthy workplace for its employees, customers, vendors and visitors. Nothing can be done to guarantee a violent incident will not take place on company property, but much can be done to reduce the chances of its happening.

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — Using outside sources to help establish an OPSEC program**

There has been a lot of talk (including advertisements) from the government in the past month or so about protecting information. For those of us who do this sort of thing for a living, what they are talking about is having companies put an OPSEC program in place.

The sad fact is that OPSEC is an area about which many executives know nothing, and, in most cases, their security staff doesn't know much more. This is, neither a surprise nor unexpected: Until now OPSEC hasn't made much of an impact on most corporations because loss of information has not seemed terribly critical. And this is precisely why it is reasonable for companies to turn to professionals such as LUBRINCO to help them establish an OPSEC program.

Although this has worked out well for most of our clients, we occasionally run across security departments that can't bring themselves to admit that there are things outside their ken, and don't see this as an opportunity to expand their area of competence. This is, of course, silly, as most managers recognize that certain specialized knowledge need not actually be available in-house. Even large financial institutions with competent domestic due diligence expertise have no problem turning to us for financial investigations abroad, where they are weak, and VPs of finance have no problem going to tax specialists for tax advice. There may also be a needless fear that we will make them look bad or displace them, which is patently absurd; professional outside security assessments, like any other service a company contracts for, are carried out by professionals with a special level of expertise, who are hired to provide a specific service, to provide some follow-on work, and to then move on. We are not set up for, nor are we interested in running a day-to-day security department, and it is to our benefit to make our peers look good so that they can work more fruitfully with their organizations.

As an example of how things can go badly, we recently met with a management team to discuss OPSEC. Things were going fairly well until their security director showed up. He assured management that OPSEC was appropriate for the Feds (true), but not for private enterprise (not true). The meeting broke up shortly thereafter. We were surprised at his attitude, as he was not saying he could and would do the work himself (which we could have understood), but that this issue, which management believed to be critical, shouldn't be addressed at all.

Not long after that we got a call asking if we could have another meeting, this time without the security manager. This is not good for any of the players. It is not good for the company because it is not productive for them to be bypassing their security manager. It is not good for the security manager to be bypassed. It is absolutely the worst position for us, not merely because we don't like to end-run our peers in security, but also because we don't like to help implement programs that are doomed to fail because of a lack of support from one of the key players.

The moral of this is not that this security director is a bad person (which he undoubtedly is not), but, rather, that professionals need to recognize the limits of their expertise (we ourselves only handle a few highly specialized areas, and make no claim to being a full-service protective firm), and be prepared to either bring in the resources needed to get the job done while they learn, or to develop them in advance if it would be a cost effective way to fulfill a new, but ongoing, need.

### **3. Executive Protection — The real deal about nuclear, chemical, and biological warfare**

Contributed by Red Thomas (REDNAGGIE@aol.com). Contributed articles do not necessarily reflect the viewpoint of the *ÆGIS* e-journal.

Since the media has decided to scare everyone with predictions of chemical, biological, or nuclear warfare on our turf, I have decided to write a paper to put things in their proper perspective. My credentials: I am a retired military weapons, munitions, and training expert.

#### ***Chemical Weapons***

Lesson number one: In the mid 1990s there were a series of nerve gas attacks on crowded Japanese subway stations. In spite of the perfect conditions for an attack, fewer than 10% of the people there were injured (the injured were better in a few hours), and only one percent of the injured died. 60 Minutes once had a fellow telling us that one drop of nerve gas

could kill a thousand people. Well, he didn't tell you the thousand dead people per drop was theoretical. Drill Sergeants regularly exaggerate how terrible this stuff is to keep the recruits awake in class (I know this because I was a Drill Sergeant too).

Forget everything you've ever seen on TV, in the movies, or read in a novel about this stuff; it was all a lie (read this sentence again out loud!)! These weapons are about terror. If you remain calm, you will probably not die. This is far less scary than the media and their "Experts," make it sound.

Chemical weapons are categorized as Nerve, Blood, Blister, and Incapacitating agents. Contrary to the hype of reporters and politicians, they are not weapons of mass destruction. They are "area denial," and terror weapons that don't destroy anything. When you leave the area you almost always leave the risk. That's the difference: You can leave the area and the risk. Soldiers may have to stay put and sit through it and that's why they need all that spiffy gear.

These are not gasses; they are vapors and/or airborne particles. The agent must be delivered in sufficient quantity to kill/injure, and that defines when/how it's used.

Every day we have a morning and evening inversion where "stuff," suspended in the air gets pushed down. This inversion is why allergies (pollen) and air pollution are worst at these times of the day. So, a chemical attack will have its best effect an hour or so either side of sunrise/sunset.

Also, because vapors and airborne particles are heavier than air they will seek low places like ditches, basements and underground garages. This stuff won't work when it's freezing; it doesn't last when it's hot, and wind spreads it too thin too fast for it to be effective. They've got to get this stuff on you, or, get you to inhale it for it to work. They also have to get the concentration of chemicals high enough to kill or wound you. Too little and it's nothing, too much and it's wasted.

What I hope you've gathered by this point is that a chemical weapons attack that kills a lot of people is incredibly hard to do with military grade agents and equipment, so you can imagine how hard it will be for terrorists. The more you know about this stuff the more you realize how hard it is to use.

We'll start by talking about nerve agents. You have these in your house: Plain old bug killer (like Raid) is nerve agent. All nerve agents work the same way; they are cholinesterase inhibitors that mess up the signals your nervous system uses to make your body function. It can harm you if you get it on your skin,

but it works best if they can get you to inhale it. If you don't die in the first minute and you can leave the area you're probably going to live.

The military's antidote for all nerve agents is atropine and pralidoxime chloride. Neither one of these does anything to cure the nerve agent: They send your body into overdrive to keep you alive for five minutes, after which the agent is used up. Your best protection is fresh air and staying calm. Listed below are the symptoms for nerve agent poisoning.

- Sudden headache
- Dimness of vision (someone you're looking at will have pinpointed pupils)
  - Runny nose
  - Excessive saliva or drooling
  - Difficulty breathing
  - Tightness in chest
  - Nausea
  - Stomach cramps
  - Twitching of exposed skin where a liquid just got on you.

If you are in public and you start experiencing these symptoms, first ask yourself, did anything out of the ordinary just happen? A loud pop? Did someone spray something on the crowd? Are other people getting sick too? Is there an odor of new mown hay, green corn, something fruity, or camphor where there shouldn't be? If the answer is yes, then calmly (if you panic you breathe faster and inhale more air/poison) leave the area and head up wind, or outside. Fresh air is the best "right now antidote".

If you have a blob of liquid that looks like molasses or Karo syrup on you, blot it or scrape it off and away from yourself with anything disposable. This stuff works based on your body weight; what a crop duster uses to kill bugs won't hurt you unless you stand there and breathe it in deeply, then lick the residue off the ground for while. Remember they have to do all the work: They have to get the concentration up, and keep it up for several minutes while all you have to do is quit getting it on you/quit breathing it by putting space between you and the attack.

Blood agents are cyanide or arsine, which affect your blood's ability to provide oxygen to your tissue. The scenario for attack would be the same as for a nerve agent. Look for a pop, or someone splashing/spraying something,

and folks around there getting woozy/falling down. The telltale smells are bitter almonds or garlic where there shouldn't be. The symptoms are blue lips, blue under the fingernails, rapid breathing. The military's antidote is amyl nitrite and, just like nerve agent antidote, it just keeps your body working for five minutes till the toxins are used up. Fresh air is the your best individual chance.

Blister agents (distilled mustard gas) are so nasty that nobody wants to even handle, let alone use it. It's almost impossible to handle safely, and may have a delayed effect of up to 12 hours. The attack scenario is also limited to the things you've seen from other chemicals. If you do get large, painful blisters for no apparent reason, don't pop them. If you must pop them, don't let the liquid from the blister get on any other area, because the stuff just keeps on spreading. It's just as likely to harm the user as the target. Soap, water, sunshine, and fresh air are this stuff's enemy.

Bottom line on chemical weapons (it's the same if they use industrial chemical spills): They are intended to make you panic, to terrorize you, to herd you like sheep to the wolves. If there is an attack, leave the area and go upwind, or to the sides of the wind stream. They have to get the stuff to you, and on you. Your odds get better if you leave the area. Soap, water, time, and fresh air really deal this stuff a knock-out-punch.

Don't let fear of an isolated attack rule your life. You're more likely to be hurt by a drunk driver on any given day than be hurt by one of these attacks. The odds are really on your side.

### ***Nuclear Weapons.***

Nuclear weapons are the only weapons of mass destruction. The effects of a nuclear bomb are heat, blast, electro-magnetic pulse (EMP), and radiation. If you see a bright flash of light like the sun, where the sun isn't, fall to the ground! The heat will be over in a second. Then there will be two blast waves, one outgoing, and one on its way back. Don't stand up to see what happened after the first wave; anything that's going to happen will have happened in two full minutes. These will be low yield devices, and will not level whole cities. If you live through the heat, blast, and initial burst of radiation, you'll probably live for a very, very long time. Radiation will not create fifty-foot tall women, or giant ants and grasshoppers the size of tanks. These will be at the most 1 kiloton bombs; that's the equivalent of 1,000 tons of TNT.

Here's the real deal: Flying debris and radiation will kill a lot (not all!) of exposed people within a half mile of the blast. Under perfect conditions this is about a half mile circle of death and destruction, but, when it's done it's done.

EMP (Electro-Magnetic Pulse) will fry every transistor for a good distance. It's impossible to say what and how far, but probably not over a couple of miles from ground zero is a good guess. Cars, cell phones, computers, ATMs: You name it, and it will be out of order.

There are lots of kinds of radiation, but you only need to worry about three; the others you have lived with for years. You need to worry about "Ionizing radiation." These are little sub atomic particles that go whizzing along at the speed of light. They hit individual cells in your body, kill the nucleus, and keep on going. That's how you get radiation poisoning: You have so many dead cells in your body that the decaying cells poison you. It's the same principle as getting radiation treatments for cancer, only a bigger area gets irradiated.

The good news is you don't have to just sit there and take it, and there is a lot you can do rather than panic. You just try to avoid inhaling dust that's contaminated with atoms that are emitting these things and you'll be generally safe from them. First, your skin will stop alpha particles, and a sheet of a newspaper or your clothing will stop beta particles. Gamma rays are particles that travel like rays (quantum physics makes my brain hurt) and they create the same damage as alpha and beta particles, except that they keep going and kill lots of cells as they go all the way through your body. It takes a lot to stop these things, lots of dense material. On the other hand, it takes a lot of this to kill you.

Your defense is as always not to panic. Basic hygiene and normal preparation are your friends. All canned or frozen food is safe to eat. The radiation poisoning will not affect plants, so fruits and vegetables are OK if there's no dust on them (rinse them off if there is). If you don't have running water and you need to collect rain water, or use water from wherever, just let it sit for thirty minutes and skim off the water gently from the top. The dust with the bad stuff in it will settle to the bottom; and the remaining water can be used for the toilet, which will still work if you have a bucket of water to pour in the tank.

### ***Biological Warfare***

There's not much to cover here. If biological warfare were as easy as a TV makes it sound, why has Saddam Hussein spent twenty years and millions of dollars trying to get it right?

Basic personal hygiene and sanitation will take you further than a million doctors. Wash your hands frequently, don't share drinks, food, sloppy kisses, etc., with strangers. Keep a tight lid on your garbage can. Don't leave standing water (like old buckets, ditches, or kiddie pools) lying around to allow mosquitoes breeding room. This stuff is carried by vectors such as bugs, rodents, and contaminated material. If you keep yourself and your environment clean, eat well and are active, you're going to live.

Overall preparation for any terrorist attack is the same as you'd take for a big storm. If you want a gas mask, fine, go get one. I know this stuff and I'm not getting one, and I told my Mom not to bother with one either (how's that for confidence). We have a week's worth of cash, several day's worth of canned goods, and plenty of soap and water. We don't leave stuff out to attract bugs or rodents, so we don't have them.

These criminals can't conceive of a nation this big with this many resources. Their weapons are designed to cause panic, terror, and to demoralize. If we don't run around like sheep, they won't use this stuff after they find out it's no fun.

The government is going nuts over this stuff because it has to protect every inch of America. You only have to protect yourself, and, by doing that, you help the country.

Finally, there are millions of caveats to everything I have written here, and you can think up specific scenarios where my advice isn't the best. This article is intended to help the greatest number of people in the greatest number of situations. If you don't like my work, don't nit pick, just sit down and explain chemical, nuclear, and biological warfare in a document around three pages long yourself. This is how we, the people of the United States, can rob these people of their most desired goal, your terror.

## Anthrax

The talking heads on TV have learned to pronounce the word "anthrax," and now they're addicted to saying it. Let's put this hype to rest.

First, ask yourself honestly "What are the odds of my getting picked out of 270,000,000 other Americans for this attack?"

Second, realize that more people have choked to death on food than have gotten anthrax in the last two weeks and, as of the time this is written, only four died. According to the Centers for Disease Control (CDC), 20,000 Americans will die of the flu this year, so if you haven't gotten a flu shot

you *certainly* shouldn't be worried about anthrax! The terrorists are preying on your fear and the media's addiction to lazy reporting of sensational news. Here's another real deal from Red: The fastest way to cut these attacks is to not show them we're scared. The more times they see us shaking in our boots the happier they will be. As FDR said "The only thing you have to fear is fear itself."

#### **4. Technical Issues — The twenty most critical internet security vulnerabilities: The experts' consensus**

Last year we listed the SANS Institute list of the ten most critical Internet security vulnerabilities. This year the list has grown to twenty items, and is a bit too long to print here. Each vulnerability has a description (included here), a list of systems affected, ways to determine if you are vulnerable, and how to protect against it. If you are involved in Internet security, we recommend you go to <http://www.sans.org/top20.htm> and look at the full report, which is updated regularly.

##### ***1 - Default installs of operating systems and applications***

Most software, including operating systems and applications, comes with installation scripts or installation programs. The goal of these installation programs is to get the systems installed as quickly as possible, with the most useful functions enabled, with the least amount of work being performed by the administrator. To accomplish this goal, the scripts typically install more components than most users need. The vendor philosophy is that it is better to enable functions that are not needed, than to make the user install additional functions when they are needed. This approach, although convenient for the user, creates many of the most dangerous security vulnerabilities because users do not actively maintain and patch software components they don't use. Furthermore, many users fail to realize what is actually installed, leaving dangerous samples on a system simply because users do not know they are there.

Those unpatched services provide paths for attackers to take over computers.

For operating systems, default installations nearly always include extraneous services and corresponding open ports. Attackers break into systems via these ports. In most cases the fewer ports you have open, the fewer avenues an attacker can use to compromise your network. For applications, default installations usually include unneeded sample programs or scripts. One of the most serious vulnerabilities with web servers is sample scripts; attackers

use these scripts to compromise the system or gain information about it. In most cases, the system administrator whose system is compromised did not realize that the sample scripts were installed. Sample scripts are a problem because they usually do not go through the same quality control process as other software. In fact they are shockingly poorly written in many cases. Error checking is often forgotten and the sample scripts offer a fertile ground for buffer overflow attacks.

## ***2 - Accounts with No Passwords or Weak Passwords***

Most systems are configured to use passwords as the first, and only, line of defense. User IDs are fairly easy to acquire, and most companies have dial-up access that bypasses the firewall. Therefore, if an attacker can determine an account name and password, he or she can log on to the network. Easy to guess passwords and default passwords are a big problem; but an even bigger one is accounts with no passwords at all. In practice all accounts with weak passwords, default passwords, and no passwords should be removed from your system.

In addition, many systems have built-in or default accounts. These accounts usually have the same password across installations of the software. Attackers commonly look for these accounts, because they are well known to the attacker community. Therefore, any default or built-in accounts also need to be identified and removed from the system.

## ***3 - Non-existent or Incomplete Backups***

When an incident occurs (and it will occur in nearly every organization), recovery from the incident requires up-to-date backups and proven methods of restoring the data. Some organizations make daily backups, but never verify that the backups are actually working. Others construct backup policies and procedures, but do not create restoration policies and procedures. Such errors are often discovered after a hacker has entered systems and destroyed or otherwise ruined data.

A second problem involving backups is insufficient physical protection of the backup medium. The backups contain the same sensitive information that is residing on the server, and should be protected in the same manner

## ***4 - Large number of open ports***

Both legitimate users and attackers connect to systems via open ports. The more ports that are open the more possible ways that someone can connect

to your system. Therefore, it is important to keep the least number of ports open on a system necessary for it to function properly. All other ports must be closed.

### ***5 - Not filtering packets for correct incoming and outgoing addresses***

Spoofing IP addresses is a common method used by attackers to hide their tracks when they attack a victim. For example, the very popular smurf attack uses a feature of routers to send a stream of packets to thousands of machines. Each packet contains a spoofed source address of a victim. The computers to which the spoofed packets are sent flood the victim's computer often shutting down the computer or the network. Performing filtering on traffic coming into your network (ingress filtering) and going out (egress filtering) can help provide a high level of protection.

### ***6 - Non-existent or incomplete logging***

One of the maxims of security is, "Prevention is ideal, but detection is a must." As long as you allow traffic to flow between your network and the Internet, the opportunity for an attacker to sneak in and penetrate the network, is there. New vulnerabilities are discovered every week, and there are very few ways to defend yourself against an attacker using a new vulnerability. Once you are attacked, without logs, you have little chance of discovering what the attackers did. Without that knowledge, your organization must choose between completely reloading the operating system from original media, and then hoping the data back-ups were OK, or taking the risk that you are running a system that a hacker still controls.

You cannot detect an attack if you do not know what is occurring on your network. Logs provide the details of what is occurring, what systems are being attacked, and what systems have been compromised.

Logging must be done on a regular basis on all key systems, and logs should be archived and backed up because you never know when you might need them. Most experts recommend sending all of your logs to a central log server that writes the data to a write once media, so that the attacker cannot overwrite the logs and avoid detection.

### ***7 - Vulnerable CGI Programs***

Most web servers, including Microsoft's IIS and Apache, support Common Gateway Interface (CGI) programs to provide interactivity in web pages

enabling functions such as data collection and verification. In fact, most web servers are delivered (and installed) with sample CGI programs.

Unfortunately, too many CGI programmers fail to consider that their programs provide a direct link from any user anywhere on the Internet directly to the operating system of the computer running the web server.

Vulnerable CGI programs present a particularly attractive target to intruders because they are relatively easy to locate and operate with the privileges and power of the web server software itself. Intruders are known to have exploited vulnerable CGI programs to vandalize web pages, steal credit card information, and set up back doors to enable future intrusions. When the Department of Justice web site was vandalized, an in-depth assessment concluded that a CGI hole was the most probable avenue of compromise. Web server applications are similarly vulnerable to threats created by uneducated or careless programmers. As a general rule, sample programs should always be removed from production systems.

### ***8 - Windows Unicode Vulnerability (Web Server Folder Traversal)***

Unicode provides a unique number for every character, no matter what the platform, no matter what the program, no matter what the language. The Unicode Standard has been adopted by most vendors, including Microsoft. By sending an IIS server a carefully constructed URL containing an invalid Unicode UTF-8 sequence an attacker can force the server to literally ‘walk up and out’ of a directory and execute arbitrary scripts. This type of attack is also known as the directory traversal attack.

The Unicode equivalents of / and \ which are %2f and %5c, respectively. However, you can also represent these characters using so-called “overlong” sequences. Overlong sequences are technically invalid Unicode representations that are longer than what is actually required to represent the character. Both / and \ can be represented with a single byte. An overlong representation, such as %c0%af for / represents the character using two bytes. IIS was not written to perform a security check on overlong sequences. Thus, passing an overlong Unicode sequence in a URL, will bypass Microsoft’s security checks. If the request is made from a directory marked as “executable” the attacker can cause the executable files to be executed on the server.

### ***9 - Windows ISAPI Extension Buffer Overflows***

Microsoft’s Internet Information Server (IIS) is the web server software found on most web sites deployed on Microsoft Windows NT and Windows

2000 servers. When IIS is installed, several ISAPI extensions are automatically installed. ISAPI, which stands for Internet Services Application Programming Interface, allows developers to extend the capabilities of an IIS server using DLLs. Several of the DLLs, like idq.dll, contain programming errors that cause them to do improper error bounds checking. In particular, they do not block unacceptably long input strings. Attackers can send data to these DLLs, in what is known as a buffer overflow attack, and take full control of an IIS web server.

### ***10 - Windows IIS RDS exploit (Microsoft Remote Data Services)***

Microsoft's Internet Information Server (IIS) is the web server software found on most web sites deployed on Microsoft Windows NT 4.0. Malicious users exploit programming flaws in IIS's Remote Data Services (RDS) to run remote commands with administrator privileges.

### ***11 - Windows NETBIOS - unprotected Windows networking shares***

The Server Message Block (SMB) protocol, also known as the Common Internet File System (CIFS), enables file sharing over networks. Improper configuration can expose critical system files or give full file system access to any hostile party connected to the Internet. Many computer owners unknowingly open their systems to hackers when they try to improve convenience for coworkers and outside researchers by making their drives readable and writable by network users. Administrators of a government computer site used for software development for mission planning made their files world readable, so that people at a different government facility could get easy access. Within two days, attackers had discovered the open file shares and had stolen the mission planning software.

Enabling file sharing on Windows machines makes them vulnerable to both information theft and certain types of quick-moving viruses. Macintosh and Unix computers are also vulnerable to file sharing exploits if users enable file sharing.

The SMB mechanisms that permit Windows File Sharing may also be used by attackers to obtain sensitive system information from Windows systems. User and Group information (usernames, last logon dates, password policy, RAS information), system information, and certain Registry keys may all be accessed via a "null session" connection to the NetBIOS Session Service.

This information is useful to hackers because it helps them mount a password guessing or brute force password attack against the Windows target.

## ***12 - Windows Information leakage via null session connections***

A Null Session connection, also known as Anonymous Logon, is a mechanism that allows an anonymous user to retrieve information (such as user names and shares) over the network, or to connect without authentication. It is used by applications such as explorer.exe to enumerate shares on remote servers. On Windows NT and Windows 2000 systems, many local services run under the SYSTEM account, known as LocalSystem on Windows 2000. The SYSTEM account is used for various critical system operations. When one machine needs to retrieve system data from another, the SYSTEM account will open a null session to the other machine.

The SYSTEM account has virtually unlimited privileges and it has no password, so you can't log on as SYSTEM. SYSTEM sometimes needs to access information on other machines such as available shares, user names, etc. -- Network Neighborhood type functionality. Because it cannot log into the other systems using a UserID and password, it uses a Null session to get access. Unfortunately attackers can also log in as the Null Session.

## ***13 - Windows Weak hashing in SAM (LM hash)***

Though most Windows users have no need for LAN Manager support, Microsoft stores LAN Manager password hashes, by default, on Windows NT and 2000 systems. Since LAN Manager uses a much weaker encryption scheme than do the more current Microsoft approaches, LAN Manager passwords can be broken in a very short period of time. Even strong password hashes can be cracked in under a month. The major weaknesses of LAN Manager hashes is the following:

password truncated to 14 characters

password padded with spaces to become 14 characters

password converted to all upper case characters

password split into two seven character pieces

This means that a password cracking program has to crack only two seven-character passwords without even testing lower case letters. In addition, LAN Manager is vulnerable to eavesdropping of the password hashes. Eavesdropping can provide attackers with user passwords.

## **14 - UNIX Buffer Overflows in RPC Services**

Remote procedure calls (RPCs) allow programs on one computer to execute programs on a second computer. They are widely used to access network services such as NFS file sharing and NIS. Multiple vulnerabilities caused by flaws in RPC are being actively exploited. There is compelling evidence that the majority of the distributed denial of service attacks launched during 1999 and early 2000 were executed by systems that had been victimized through the RPC vulnerabilities. The broadly successful attack on U.S. military systems during the Solar Sunrise incident also exploited an RPC flaw found on hundreds of Department of Defense systems.

## **15 - UNIX Sendmail Vulnerabilities**

Sendmail is the program that sends, receives, and forwards most electronic mail processed on UNIX and Linux computers. Sendmail's widespread use on the Internet makes it a prime target of attackers. Several flaws have been found over the years. In fact, the very first advisory issued by CERT/CC, in 1988, made reference to an exploitable weakness in Sendmail. In one of the most common exploits, the attacker sends a crafted mail message to the machine running Sendmail, and Sendmail reads the message as instructions requiring the victim machine to send its password file to the attacker's machine (or to another victim) where the passwords can be cracked.

## **16 - UNIX Bind Weaknesses**

The Berkeley Internet Name Domain (BIND) package is the most widely used implementation of Domain Name Service (DNS) -- the critical means by which we all locate systems on the Internet by name (e.g., [www.sans.org](http://www.sans.org)) without having to know specific IP addresses -- and this makes it a favorite target for attack. Sadly, according to a mid-1999 survey, as many as 50% of all DNS servers connected to the Internet are running vulnerable versions of BIND. In a typical example of a BIND attack, intruders erased the system logs and installed tools to gain administrative access. They then compiled and installed IRC utilities and network scanning tools, which they used to scan more than a dozen class-B networks in their search for additional systems running vulnerable versions of BIND. In a matter of minutes, they had used the compromised system to attack hundreds of remote systems, resulting in many additional successful compromises. This example illustrates the chaos that can result from a single vulnerability in the software for ubiquitous Internet services such as DNS. Outdated versions of Bind also include buffer overflow exploits that attackers can use to get unauthorized access.

## **17 - UNIX R Commands**

Trust relationships are widely used in the UNIX world, particularly for system administration. Companies frequently assign a single administrator to be responsible for dozens or even hundreds of systems. Administrators often use trust relationships and the related UNIX r commands to switch from system to system conveniently. r commands enable someone to access a remote system without supplying a password. Instead of requiring a username/password combination, the remote machine authenticates anyone coming from a trusted IP addresses. If an attacker gains control of any machine in such a trusted network, he or she can gain access to all other machines that trust the hacked machine. The following r commands are often used:

1. rlogin – remote login  
    rsh – remote shell  
    rcp – remote copy

## **18 - UNIX LPD (remote print protocol daemon)**

In Unix, the in.lpd provides services for users to interact with the local printer. LPD listens for requests on TCP port 515. The programmers who developed the code that transfers print jobs from one machine to another made an error that creates a buffer overflow vulnerability. If the daemon is given too many jobs within a short time interval, the daemon will either crash or run arbitrary code with elevated privileges.

## **19 - UNIX sadmin and mountd**

Sadmin allows remote administration access to Solaris systems, providing a graphical user interface for system administration functions. Mountd controls and arbitrates access to NFS mounts on UNIX hosts. Buffer overflows in these applications, enabled by programming errors made by the software developers, can be exploited to allow attackers to gain control with root access.

## **20 - UNIX Default SNMP Strings**

The Simple Network Management Protocol (SNMP) is widely used by network administrators to monitor and administer all types of network-connected devices ranging from routers to printers to computers. SNMP uses an unencrypted “community string” as its only authentication mechanism. Lack of encryption is bad enough, but the default community string used by

the vast majority of SNMP devices is “public”, with a few “clever” network equipment vendors changing the string to “private” for more sensitive information. Attackers can use this vulnerability in SNMP to reconfigure or shut down devices remotely. Sniffed SNMP traffic can reveal a great deal about the structure of your network, as well as the systems and devices attached to it. Intruders use such information to pick targets and plan attacks.

Note: SNMP is not unique to Unix. However, the reason it is listed under Unix is because the contributors have seen a majority of attacks on Unix systems caused by poor SNMP configurations. The contributors have not seen this as a major problem on Windows Systems.

## **5. Real Stories from the Field — Unprofessional practices, unprofessional behavior**

Some time ago we ate in a restaurant that had bad service. One customer within our hearing complained to the waiter, who was indifferent to his complaints. He then complained to the manager, who was equally indifferent to the complaints.

We finished at about the same time as did the more verbally cranky customer, and as we left heard the man tell his companion to make a fuss and distract everyone for a bit, which his companion did.

While everyone but us was distracted, we watched in some fascination as, the customer went over to the alarm keypads and started punching in codes. We happened to be with our alarm guy, who watched bedazzled as the customer accessed the panel using the factory default codes, and reset the panel so that the activation time was reduced to five seconds.

This behavior was petty (the manager would be unable to make it to the door before the alarm sounded, and would have to wait for the alarm company to reset the panel before he could go home), and unprofessional. Worse, it reminded us of how many companies do alarm installations – sometimes even sophisticated installations – yet leave in the default codes, much as the default codes are often left in computer installations. While the actions of the customer were as petty and unprofessional as the behavior of the restaurant staff, when default codes are not removed from any device they present a serious security lapse that goes way beyond the potential for mere pranks.

Because of this you should make sure that default codes have been removed on installations done for you. How do you do this? Ask the installers whether they have removed the default codes. If the response is negative, tell

them to remove the default codes and then have them test the system to see that the removal was done properly.

## **6. Book and Product Reviews**

### *CopyTele DCS-1200 and USS-900*

CopyTele, Inc.

900 Walt Whitman Road Melville, NY 11747

Tel: 1-631-549-5900 Fax: 1-631-549-5974 <http://www.copytele.com/>

DCS-1200- \$1595, USS-900 \$1095.

The *CopyTele DCS-1200* and *USS-900* are small (6" x 4.38" x 1.38"), portable (9 ounces) telephone encryption devices. They come with international power adapters.

The *DCS-1200* connects between the handset of your telephone and the body of the telephone, which allows it to be used on analog and digital PBXs, ISDN , and Satellite Communication Terminals, as well as standard analog telephones. Connecting it is easy: You unplug the coiled handset cord from your telephone and plug it into the side of the *DCS-1200*, or else use the included headset/mike. You then take a short (provided) cable and connect the *DCS-1200* to the jack where you just unplugged the handset. The *DCS-1200* can connect to a satellite or cellular phone – a feature we will test in the future – and has a built-in battery which will last up to six hours when so used. In addition, it can be used to encrypt data on your PC and encrypt files for e-mail communication. While the *DCS-1200* is set for a standard phone, it may require tweaking, and this will require a call to the help desk, as there is no real manual to adequately explain the features offered.

The *USS-900* works on an analog telephone system, and goes between the telephone and the RJ-11c wall jack, rather than the handset. It involves no tweaking, and is therefore a better bet if you do not plan to use a digital PBX or satcom. The *USS-900* additionally can secure fax and data transmissions, and can also encrypt email attachments and the files on your PC.

Voice quality was adequate with a good line. In our worst-case test involving a bad line, far from a switch, with, according to the analysis, frayed insulation, which has made many devices fail, we were still able to connect and speak. While the voice quality in this worst-case situation was not great, and while dropouts required repetition, we *were* able to make a secure connection with these devices, which is way better than a device failing to connect, and having to make a clear but non-secure connection.

The CopyTele encryption devices use the Harris CITADEL™ CCX cryptographic engine chip for key generation and encryption, with the option of having either 168 Bit Triple DES or Harris' own encryption algorithm. While we have a personal bias against proprietary algorithms, Harris is an experienced defense contractor, and their products have a good reputation. This chip and algorithm are used widely within NATO which means that it will certainly be adequate for commercial use.

Will the encryption impede real-time legal wiretaps? As always, we have no idea, and it remains one of those questions to which we don't actually expect a serious answer.

## **7. Free-Subscription/Unsubscription/Copyright Information**

•• AEGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2001 by The LUBRINCO Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com) and L. Burke Files (LBFiles@lubrinco.com).

**The LUBRINCO Group** provides services in three high-threat areas, too specialized to be dealt-with in-house, that can adversely affect domestic and international bottom lines.

- **Protection of trade secrets and intellectual assets.**
  - Anti-economic espionage.
  - OPSEC: The identification and protection of information that would give your competitors and adversaries an advantage.
- **International financial investigations and due diligence consulting.**
  - Location and recovery of missing and hidden assets.
  - Establishing business relationships and strategic partnerships in Central and Eastern Europe, the offshore financial centers, Beijing and Shanghai, Central Asia, and Latin America and the Caribbean.
  - Anti-money laundering and financial fraud requirements under the *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001* and the *EU Revised Money Laundering Directive of 2001*.
- **Protection of management, staff, and families.**
  - In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.

- When traveling and living overseas.
- When transporting items of substantial value.

LUBRINCO identifies and quantifies threats and vulnerabilities, and their associated risk, then manages the vulnerabilities so you can transfer or live with the residual risk. We prevent disastrous financial loss to your company, and physical harm to you, your family, and your staff.

For information on **The LUBRINCO Group** and its services, or for the archive of all past issues of *ÆGIS* e-journal in PDF format, please go to <http://www.lubrinco.com/>.

To sign up for a **complimentary subscription** to *ÆGIS* e-journal or the *ÆGIS* e-journal PDF notification list, go to <http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com).

To subscribe to our AvantGo channel, go to [http://avantgo.com/channels/\\_add\\_channel.pl?cha\\_id=1773](http://avantgo.com/channels/_add_channel.pl?cha_id=1773)

To be removed from the subscription list, follow the instructions on the mailing you received, or send an e-mail to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com).

If you know of anyone else who should be receiving *ÆGIS* e-journal, please send their e-mail address to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com).

If there is a topic that you would like to know more about, send it to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com) and the editors will consider it as the topic for an article in an upcoming issue.

If you would like to submit an article for publication in *ÆGIS* e-journal, send it as an attachment to an e-mail to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com). Submission of an article certifies that (a) all information in the article is in the public record, or (b) that you are authorized to release any personal or corporate proprietary information contained in the article, and (c) that none of the article has previously been copyrighted. The submission of materials for publication in *ÆGIS* e-journal constitutes a license to The LUBRINCO Group Ltd, Inc., and/or Financial Examinations and Evaluations, Inc, their assigns, associates, or affiliates, to abridge and/or edit said submission, and to copyright and publish/republish any submitted materials in whatever written and/or electronic form they may choose.

If you would like to go beyond normal fair-use in reproducing articles from this issue of *ÆGIS* e-journal, you may do so freely as long as appropriate source, copyright, accreditation, and link to the LUBRINCO website is

included. This should be in the form

*Article Title*, from the December 2001 ÆGIS e-journal (© 2001 LUBRINCO & FEE), to be found at <http://www.lubrinco.com/>.

ÆGIS e-journal is a forum for the exchange of information, ideas, operating styles, theories, and related topics for corporate managers who make decisions about threats typically outside the expertise available in-house, yet which have the potential to affect their company's domestic and international bottom lines. Nothing appearing in ÆGIS e-journal should be construed as legal advice. The information provided is "general information," not "specific advice."

The solution to any problem is highly dependent upon the precise facts involved. Thus, before making any reliance upon anything said here, you should consult with an appropriately skilled professional. Opinions expressed by contributors are not necessarily endorsed by the publisher, and may be presented to encourage a dialogue among subscribers. The publisher and any re-publisher cannot be held responsible for any loss incurred as a result of the application of any information published in ÆGIS e-journal.

Please be safe, and be smart.