BROADCAST SECURITY ARCHITECTURE FOR THE DIGITAL AGE - THE NEXT LEVEL

David Baden
Radio Free Asia
Washington, DC
badend@rfa.org

Paul Flint
Security Analyst.
Washington, DC
flint@flint.com

Abstract

In the converged digital broadcast ecology a proactive approach towards Information Assurance (IA) is required. The goal of the paper is help develop and describe broadcast network security architecture based on the "protect, detect and react" methodology.

FOUNDATIONS

For the broadcaster, the digital ecosystem is the result of a convergence between computer systems, networks and broadcast technologies. Broadcast facilities have evolved from stand-alone physical analog, to networked-analog, to integrated digital, to networked digital, and now to internetwork digital workplaces. Modern facilities must maintain symbiotic connections for the World Wide Web; access to electronic mail and Internet broadcast streaming.

Once your system attaches to the non-physical environment of the Internet, there is no longer any way to assure who has access to and control of your broadcast equipment. Even at the fourth level it becomes impractical to monitor who is doing what. Up until now the best method to solve this Identification and Authentication problem has been to "share a secret" between some part of the equipment and those authorized to use it. This software part has come to be known as The "Trusted Computing Base," or TCB. The TCB is always supported and often supplied by the operating system software.

"Hardware" engineers are largely helpless in the face of software attacks against the operating system TCB or the sub components that trust it. The Internet's arrival at your site has resulted in a suddenly very insecure environment for your broadcast facilities and the information you purvey.

THE DIGITAL ECOSYSTEM

In an alternate view, the broadcast digital ecology starts physically connected in the first four layers of the seven-layer International Standards Organization/Open Systems Interconnect (ISO/OSI) model illustrated in Table 1. Information warfare begins at the login prompt, represented here at the end of the transport layer and the beginning of the presentation layer. This coincidentally, is the point where you change from hardware engineering to software engineering.

It is at this point in security architecture where the struggle for security commences. Imagine a castle wall topped with a magic parapet. Friends or foes need only the spell to breach the parapet and enter the castle. While it is your castle, you cannot see this parapet and there is no visible sign to you of the struggle-taking place on your behalf between abstract forces of good and bad.

Table 1. ISO/OSI Model

ISO/OSI MODEL	
LAYER	REALM
7. Session	Software Engineer
6. Application	
5. Presentation	
4. Transport	Hardware Engineer
3. Network	
2. Protocol	
1. Physical	

Current digital technology has made possible signals of improved quality, with easily manipulated sound and video streams, coupled with magnificent distribution capabilities. Audience acceptance of this evolution has been complete and irrevocable. With this technology came an accessory digital ecology and astronomical risks.

Trust

Can operating systems ever be trusted? Along with the rest of our information society, we find the operating system is well entrenched in broadcast technology. The operating system has become the principal component that assigns roles and receives human trust.

The present security controversy between operating systems involves the original human readable format of the source instructions that are processed into machine-readable format for use by computing systems. Like the floor plan of the castle this "source code" element must be analyzed and reviewed to find security weaknesses. With this criterion in mind it is possible to divide operating systems into two broad categories, open-source and closed-source. The developer keeps the source instructions of closed-source systems, and various barriers exist to your knowing the details of how these operate. These systems

are "intellectually cheap" to install and easy to use, but are costly (unless you are the developer) to enhance and troubleshoot. The information necessary to operate closed systems is strictly compartmentalized by role. The delineation of roles within closed-source systems makes it difficult to change roles and get from one compartment to another when circumstances require it.

Open-source systems are defined by full disclosure. Users of all types are encouraged to discover how the system operates, including the security mechanisms. It has been suggested that open-source began with developer frustration with the exclusionary tendencies of closed-source. Open source operating systems are "intellectually expensive" to install, often tricky to use but easy to troubleshoot, enhance and maintain. The information necessary to operate these systems need not be role-based. Roles within open-source systems are elastic but can be clearly defined as part of the installation.

THE NEW DISMAL SCIENCE

Risk analysis reveals acceptable risk. Risk is the opposite of assurance, and is nothing new. Information risk, the opposite of information assurance, is a new branch of an old tree. To assess risk, we first must define it. Engineers revel in simple algebraic ways to relate fundamental matters. This equation below attempts to do the same, if only by identifying the variables involved:

Risk = function of (Threats, Vulnerabilities)

Threats are forces committed to disruption of your service.

Vulnerabilities are the opportunities available to disrupt it.

Threats and vulnerabilities are the result of system design and implementation choices. Assessing and minimizing digital environmental risk is a new task in an old chore.

CONVENTIONAL RISK

Broadcast engineers have historically had to deal with risk. Traditional Broadcast Architecture is based upon tying to minimize the relationship between threats and vulnerabilities. This should not arrive as a revelation for the broadcast engineer. Consider the following risk categories to solidify these terms how they relate:

Human Error

Human error is the most prevalent cause of "dead air time" for the any broadcast facility. Operators pushing the wrong button, missing a cue, playing the wrong promo, cutting to the wrong feed, etc. The self-protective aspect of human nature generally translates such incidents into "technical failures" are classic in our field. This is a special class of technical failures that cannot be duplicated and usually magically disappear when an engineer walks into the room. A guiding maxim for all IA practitioners must be:

"Never assume malice when the facts can be explained through incompetence."

Intentional Malicious Actions

Every human being is subject to the occasional "bad mood". The risk to any technical facility is how that occasionally mood manifests itself. However this is not the forum to examine the psychology of intentional malicious acts on the part of a disgruntled individual.

The corresponding vulnerability to this treat in a broadcast facility is the allowed level of access to systems and resources that can disrupt service that the disgruntled or malicious individual(s) have access to. The best any engineer can do to limit vulnerability is to limit access to critical systems. Further protection can be afforded with logging or monitoring systems (such as security cameras). The risk of intentional malicious acts can be greatly reduced if the individual considering the act is convinced that there is a real chance their actions will be observed and punished. Therefore any monitoring techniques used for internal intrusion work best if publicly known (or even exaggerated). The real goal is the prevention of damage not prosecution after the fact.

Physical Damage

Facility threats are characterized as threats that can do hard physical (real-estate) damage to a broadcast facility or its equipment. The threat of physical damage comes from numerous sources, power failures or fluctuations, flood, fire, extreme weather, natural disasters and common vandalism.

Broadcast engineers have been dealing with minimizing the vulnerabilities of physical damage for years. Protective systems such as, fire, moisture and smoke detectors, sprinklers systems, generators, power conditioners, sump pumps, etc. are universal standard equipment for all broadcast facilities. In mission critical system redundancy is often a requirement. Antennas, transmitters STL and studio facilities are often designed and built with redundancy in mind.

CYBER - THE NEXT LEVEL OF RISK

Physical damage could not be done unless the agent of that damage came to the facility. Attacks from cyberspace can come from any individual with access to the Internet. Worldwide the Internet Population today is over 450 million and growing; all should be considered potential hackers.

Modern broadcast facilities exist within an overall corporate framework. This framework may or may not have an Information Assurance structure. Broadcast Information Assurance needs to rely on an institutional baseline if one is provided, but must be prepared to enhance this with separate and distinct local organizational controls.

As broadcast engineers it has become your task to be knowledgeable and proactive in dealing with Information Assurance (IA), the comprehensive term for information security. Damage to your information systems can at worse knock you off the air, and lack of Information As-

surance can compromise broadcast content, scheduling information or vital corporate data.

You now do business in the new frontier of the Cyber.

Hackers

An active hacker attack is best described as a person that is knowledgeable of computer and network security, dedicating their time and personal attention to gain unauthorized advantage within your system.

The motivation for this access is varied. Some hackers break into systems simply to prove they can, bragging rights for geeks. This type of hacker generally does not do damage but can be expected to leave some possibly benign "calling card". Criminal intent may be the motivation for some hackers. Accessing your system for the purpose of stealing data or to gain access to finical records and accounts. Attacks can be vandalistic in nature with malicious intent, gaining access to deface a web page or destroy broadcast program or corporate data.

Malicious hackers in most cases have a personal vendetta against your organization; some times they are politically motivated. This motivation can be trite if it is ever known, such as they simply don't like the music you play or hold a more personal grudge.

Anonymous Attack

Anonymous attacks utilizing malicious logic, viruses and other destructive programs are in most cases not specifically targeted and any one organization. These Programs are often crafted not against a person or institution but rather against a particular and widespread vulnerability. In our introduction to the current age of acknowledged operating system monopoly, the existence of "monocultures", vast areas of similarity in particularly vulnerable information processing program segments creates irresistible targets of opportunity.

Attacks intended to damage or discredit a monoculture, (e.g. Microsoft OS and email attacks, Yahoo and ebay denial of service, or the Morris sendmail worm) in a way may be considered a "cyberlogical" (cyber biological) consequence. In the biological sense, these programs are performing a selection process in exploiting the weakest and most vulnerable systems. Unfortunately these are the very same systems you are depending on.

Thus these types of anonymous attacks come in the form of programs created to interrupt service or do damage that are let loose to affect as may systems as they can.

Viruses A virus infects other programs with copies of itself. It can clone itself and multiply constantly seeking new host environments. These self-replicating viruses can be harmless (outside of consuming resources), while more malicious viruses can damage other programs (including operating systems) and/or alter data. After finding a host, viruses, like a biological infection, can rapidly spread through Local Area Networks (LAN) and/or Wide Area Networks (WAN) and affect other computer systems.

Viruses can initialize as active-destructive as soon as they enter a computer, or can lie dormant until activated. Activation of a virus can also be event-based, for example, initiated by a programmed date/time or a specific sequence of keystrokes.

Viruses are characterized by the damage that they do, the methodology of its infectious spread and how they damage a computer system.

Disk Based Viruses The first popular virus method exploited the fact that the operating systems did not protect the initial or "bootstrap" sectors against malicious logic. Boot sector viruses are thus those that infect the boot sector on a computer system. File infecting viruses are viruses that infect files. These viruses strive to become memory resident, which allow them to infect with full control. File infecting viruses will commonly infect executable files on a system. Detection of these types of viruses is through known signature analysis. Signature analysis has been countered by Polymorphic viruses which change their appearance with each infection. Polymorphic viruses are encrypted viruses that are difficult to detect. The encryption algorithm is usually altered with each new infection. These Stealth viruses can hide from anti-virus software. In operation they load into active memory and intercept all attempts to use the operating system calls, propagating themselves at every opportunity. Stealth viruses additionally hide changes made to file sizes, directory structures, and other operating system aspects. Multi-partite viruses infect both boot sectors and executable files.

Macro Viruses Viruses not only come as standalone programs. The ability to include "macro script", a programming instruction set in prevalent standard document types, has become a robust platform for virus attacks. Viruses embedded in document files hitchhike by attaching themselves to your documents and are exchanged through applications, macro viruses are application-specific, not operating system dependent. When embedded in documents, macro viruses can spread quickly over networks or in email disguised in attachments.

Note that application based viruses are only effective when a particular application is so widespread that it can vector the virus effectively.

Virus Hyper Evolution Embedded, stealth and polymorphic viruses are also being developed for popular file types once thought to be safe. The first PDF file virus was discovered tin the wild, January 8, 2002 the first virus that infects Shockwave Flash files SWF/LFM-926 infects users who download and play Flash files. Not affected is Web content viewed in a browser; according to the purveyor of Flash (Macromedia), the virus can only affect content sent via E-mail or downloaded from a site and then run outside

a browser. Macromedia is providing additional information on mitigation via its Web site.

Destructive Non-Virus Programs Worms spread from system to system by exploiting vulnerabilities and replication. Worm attacks are often mistaken for virus attacks. The difference is that a worm program does not replicate itself as a virus does. In the biological sense, a worm is similar to a benign tumor while a virus is like a malignant one.

Trojan Horses A Trojan Horse is a destructive program that has been disguised an innocuous piece of software.

Logic Bombs Logic Bombs are malicious programs, which include a timing device so it will go off at a particular date and time or event. Logic bombs are usually timed to do maximum damage. The logic bomb is a favored device for revenge by disgruntled former data processing employees who can set it to activate after they have left the company.

Distributed Denial of Service Distributed Denial of Service (DDoS) attacks employ armies of "zombie" computers taken over and controlled by a single master computer in order to overwhelm the resources of an intended target with floods of packets. The growing number of home computer users with high-speed Internet access with lax security have increased the numbers of computers available of take over and use in DDoS attacks. A hacker who will use it launch an overwhelming number of requests toward an attacked web site can easily compromise unsecured computers. Coordinating with other compromised computers Web servers are overwhelmed by the simultaneous volume of data request preventing the normal function of the site.

Attacks From Within Intentional or accidental damage from your own users is an area of special concern. In a recent actual incident, an employee started his workday by logging into the network and randomly deleting all the folders on the file server that he could gain access to. The incident was initially treated as a virus attack having all the classic signs of data being randomly destroyed. Subsequently, the cause was traced to the specific user by through the tracing logs. When confronted with this evidence the employee denied any wrong doing and pleaded innocence (even after termination). The motivation for such personal destructive actions remains a mystery.

Cyber Vulnerabilities Vulnerabilities can be best being described as defects or bugs in computer systems. These vulnerabilities can affect the modern broadcast facility in diverse ways. On the local facility level these vulnerabilities can manifest themselves as the intermittent failure of systems in the broadcast chain (i.e. the automation software in a video switch failing once a month necessitating a reboot).

When these system defects exist on a networked system they lead to security points of failures. Usually this type of vulnerability is publicly known and is the first weakness that is probed for exploit.

RISK MITIGATION

The only method of protection is for broadcasters to embrace this new area of conflict and use collective resources to master the digital realm. Technology advances made in military environment have often defined broadcast technology. In the Defense department sector, several important concepts and requirements have been developed. These include:

- Initial Mandate and Empowerment
- Information System Policy
- Risk Assessment
- Security Concept of Operations
- Incident Response Plans

It would be unrealistic for us to hope to entirely eliminate all risk. It is realistic to believe you can understand and accept the risks that you do take. Nevertheless you must not take the fact that some risks are inevitable as a license to neglect your responsibility to mitigate the vulnerabilities and minimize the damage that threats to your systems might inflict.

Mandate and Empowerment

The first step towards IA is to mandate a Designated Authority for Security. Often as not this role will the responsibility of the facility Chief Engineer. Well-defined roles of accountability and lines of responsibility will provide key personnel with both the authority and the resources needed for IA. This empowered individual should immediately conduct a Risk Assessment and audit all policies. If no clear mandate is provided by upper management (or you are upper management) empower yourself by assuming the mandate and a set of policies.

An Information System Policy

Any business with more then one computer needs a formal Information Systems (IS) Policy. An IS Policy is a document that defines ownership of and responsibility for a company's IS (e.g. computer, software and network) resources. Users are advised of their responsibilities and obligations to the company when they are granted access to these IS systems. An IS Policy helps users comply with when using these IS resources. Not only should an ISW Policy include company policy but also any applicable local, state, and federal laws.

An IS Policy should outline acceptable use that is ethical, shows restraint in the consumption of shared resources, and demonstrates a respect for intellectual property. Ownership of data should be clearly defined in the document as well as system security mechanisms and the consequences for violating the IS Policy. Additionally an IS Policy should ensure users of their rights to privacy and freedom from intimidation and harassment.

Trust is an important concept of IS security. It is a measure of how much users can depend on what any system offers. It also requires a commitment from the user base to utilize the systems in a responsible manner. How can an employee be blamed for opening a virus infected e-mail attachment when they have never been told not to? Ignorance of the law is no excuse but having no laws is inexcusable. All is permitted unless it is forbidden.

An IS Policy should specifically list the IS services being supported by the technical staff for the users and under what conditions that support is offered and define the formal mechanisms for requesting that support.

Risk Assessment

The third step towards Information Assurance is to perform a Risk Assessment. All systems must be individually evaluated and known vulnerabilities listed. Working from the list of vulnerabilities the possible threats must be analyzed. This is a listing of what is vulnerable, why it is vulnerable and who could possibly exploit these vulnerabilities.

The Penetration Test format is an excellent one to follow. Start from the outside wall of your facilities and work inward. When conducting a Risk Assessment it is critical not to concentrate on major systems only. All systems have crucial minor support systems that can sometimes be overlooked. All dependencies and the effect of their failures must be analyzed, your entire security architecture and design I based upon this document.

Concentrating on systems dependencies cannot be over stressed. While you may be looking at the affect of a special failure to a networked digital audio system what would happen if the network failed? Could audio still be accessed? What if there is a routing switch in the signal stream to this system? Would its failure render the system useless? Signal flow diagrams (both analog and digital) and network architecture should be reviewed on every major system. You may find surprising the number of possible points of failure.

The result of a Risk Assessment should be a list of the risk broken down to vulnerabilities and the probability of exploits that your facility faces. This list should be reviewed and what steps to remedy deficiencies should be implemented. After corrections are made the exercise should be repeated before moving on.

A Security Concept of Operations

This high-level architecture document should initially be completed in the design phase of a facility. For an operational facility this document is a plan to mitigate any security issues uncovered in the Risk Assessment phase. The primary question that should be answered by a Security Concept of Operations is specifically what constitutes "being in business" and what minimal systems are required to stay there. In the case of the broadcast facility the question should be what is the least required to stay on the air.

This exercise must separate the essential from the convenient. While everyone in a facility enjoys corporate e-mail, Internet access and phone service, is it needed to stay on the air? The approach when preparing a Security Concept of Operations should proceed on the assumption that all systems are down. One section of your concept of operations should deal with the "restoration priority" question. What systems are to be brought up first and in what order should service be restored to all?

Careful consideration should be paid to assumed support systems as this exercise is sometimes very illuminating as to how little is actually needed to get and stay on the air.

A Security Concept of Operations should work forward as well as backwards. The order of restoration should be capable of implementation in the reverse shutdown mode. Due to the speed at which most cyber attacks occur the only way to save some systems may be to shut them down as soon as possible. Consider for example a virus that is rapidly spreading through the servers in a facility. To contain and isolate this virus you may be required to get all the uninfected servers off the network as fast as possible. (A fast way to do this is to power down your hubs or central switches.) Critical operations that are keeping you on the air must go into an isolated standalone mode. Remember a virus cannot affect what it cannot reach.

Incident Response Plans

The Incident Response Plan (IRP) is the course of action that will be followed in an emergency event. It is authority is the cumulative distillation of data available in both the Risk Assessment and the Security Concept of Operations. From the Risk Assessments you know the vulnerabilities and threats to the facility and should have an idea of what damage can be sustained if left unchecked. The Security Concept of Operations defines the priority as to what systems need to be protected first.

The Incident Response Plan allows the technical staff to take coordinated and efficient (as in no wasted efforts) action in order to provide continuity of service. The IRP should be a public document know to all staff members so they may know in the event of an emergency where they are suppose to be (or not be) and what is expected of them. In a sense the Incident Response Plan acts as the choreography for a very sophisticated fire drill. In the event of actual emergency additional surprises are not needed.

PROTECT DETECT AND REACT

Having the mandate and being empowered to act on it, armed with an Information System Policy, a Risk Assessment, a Security Concept of Operations and an Incident Response Plans you are now ready to assume the normal IA mode of protect, Detect and React. While this is your

day-to-day security operation mode it is by no means a passive task.

Protect

Backup Facilities In the broadcast area there are often systems that cannot go offline for any reason. If broadcast digital facilities were not designed with testable redundant backups, they constitute an unacceptably high level of risk. The single most important thing about backups is no matter what your backup methodology; it is not operational until they have been thoroughly tested.

Test all backup equipment regularly. Test standby network routing by disconnecting the primary route. Declare "Lights Out" drills by designating a specific critical service off line or off limits to test backup and help speed up reaction times. Until your operation can stand up to these tested backup solutions you have the illusion of backup. Know that this illusion is far more dangerous than accepting the risk of no backup, which is unthinkable in the broadcast industry.

Data Systems Backup The five most hated words in the computer realm are: "Did you back it up?" Proper data backups will get you though viruses, disaster, or all other manner of calamity. Incomplete backup will leave you in a technically untenable position with a wistful memory of the few hours ago when you had the system to do the job, and the unfulfilled wish that you had done the right thing at the right time.

Backing up data is crucial. Develop automated system for incremental and full backups. Store the backup medium not only on-site but keep copies off site as well. Remember not only to back up data but also have backup copies of all system and application software. Audit and test all backup systems and practice their recovery routines. A backup that fails to restore is worse than not having a backup. Test a workstation back up by replacing the current drive with a blank. Backup equipment needs to be regularly tested in the rest of your operation. Personally test the end-to-end back up for each critical system.

Virus protection software Anti-virus software as the name implies is a program that seeks and destroys virus infected files before they cam harm you system. Effective anti-virus software should be able to test files and directories for the presence of known viruses, clean or remove infected files and provide ongoing real-time protection against memory resident viruses. Software is an essential component in the war against viruses.

Establish and maintain a virus-free environment. The software should be installed on every computer in a broadcast facility including mail servers, file servers, gateway servers and even on dedicated broadcast related servers. When you are installing make sure to run a complete virus scan on the computer. Only when you are certain that your current computing environment has no viruses can you begin to control future infections.

Patches and Updates Keep current on all software and firmware updates and patch releases. Patches in the software world usually fix known bugs that slow down your systems performance or are security vulnerabilities. Get on vendor mailing lists for automatic notification if available and try to check the vendor's web sites at least twice a month. Be systematic in doing this, keep a spreadsheet of all the software and firmware packages in your facility with last patch and version information and a last checked column.

Installing all publicly available patches even when installing software recently purchased. Patches are not always included on the latest version release due to the time cycles involved in getting the media updated in the distribution chain. Hackers exploit known vulnerabilities weeks, months, sometimes years after flaws have been made public. Patches not only apply to Operating Systems but to all applications especially e-mail and browser packages. Firmware should not be overlooked. It can, and should, be backed up as well. At a minimum know what bios versions are installed in your critical servers.

Firewall Firewalls are to the Internet what Barbed Wire was to the western Prairie. It fences you in and fences you out. In the real world a firewall is a structure intended to keep a fire from spreading. IS firewalls are intended to keep unwanted intrusion off of your LAN (Local Area Network) or to deny LAN users access undesirable Internet services. The original computer firewall was a non-routing Unix host computer with connections to two separate NIC (Network Interface Cards) connections, one to the Internet and the other to a private LAN. To access the Internet from the LAN a users had to logon to the firewall (Unix) server and use the resources of that system to reach the Internet.

There are two primary types of firewalls, proxy and filtering. Filtering firewalls block administrator defined network data packets and are transparent to the user. Proxy firewalls make the Internet connection for the user and limit access based on a set of server internal rules. A filtering firewall works at the network level and accepts data to be received or transmitted only if the firewall policies (rules) allow it. Data packets can be filtered by protocol, state-full inspection, and network address of either the source or destination. Filtering firewalls do not log or analyze data but merely block what traffic is not allowed. This function is not very processor intensive and this fact contributes to the firewall causing little or no additional latency on the LAN.

A Proxy Server acts as an IP network addresses translation firewall to controls and monitor data traffic. To lower bandwidth requirements and decreases access time proxy servers can also cache data. With application proxy servers the user sends a request to access outside the LAN to the proxy first. The proxy server acts on the request and connects to the Internet server requested. Proxy servers process all communication and are capable of logging all LAN to Internet traffic.

Proper Authorization Inadequate user access controls and authentication place systems at risk. Make sure that all systems that can be are protected by passwords. Administrators must keep all accounts current and delete dead accounts as users stop using them. All sessions should be logged and checked on occasion. Enforce in all administrators and users of like minds that passwords should be in mixed case with numbers and special characters.

Administrators should change all system default passwords in all systems as soon as possible. Gaining access through the use of a gateway router's factory default account cracks many systems. All passwords system wide should be changed at least once every two months. Emphasis should be placed on identification, authorization and authentication methods. User session should be protected with end-to-end encryption and safe data-handling practices.

It is also crucial that system administrators grant the highest level of system access and privileges to users that allow them to do their job and no more. This is called the "least privilege" doctrine. If a users job function does not require the ability to download files from the Internet do not allow them to. If the user would have no job related reason to load data from a floppy disk or CD onto their computer, disable it from the system BIOS.

Encryption Widely available encryption programs, such as PGP (Pretty Good Privacy), are often used to protect data that is sent via the Internet. Modern cryptographic systems use publicly reviewed cryptographic algorithms and secret cryptographic session keys. If you know the algorithm and apply the correct key the code is broken and the data is revealed. Encryption itself does not provide data integrity and encryption should not be a panacea causing a facility to ignoring other aspects of security. Viruses can come to poorly protected systems as attachments in encrypted email and bypass your bridgehead mail server scanning software. Smart attackers will get around or exploit encryption. Encryption should be viewed as a lock on data, but as with any lock, it is only designed by keep out the honest. Cryptographers and mathematicians in many places are dedicated to the task of finding weaknesses in cryptographic algorithms. If they succeed a new algorithm is deployed. The unscrupulous are constantly working to obtain the crypto keys, or cracking the crypto by use of the "brute force" method, where you attempt every possible key in existence. This is referred to as a "dictionary attack".

The Internet is not a secure environment. All e-mail traffic over the Internet should be liked to sending a post card. While encryption places that post card in an envelope one should not make the assumption that it still will not be opened. The best way to protect sensitive confidential information is not to send it over the Internet. Finally, PGP is a special type of encryption scheme that encrypts and exchanges session keys in a very novel way (Asymmetric Key Cryptography). While beyond the scope of this document, this method is of critical interest to the all media professionals, and should be a subject you get familiar with.

Block all expected ports of entry for malicious code. The use of external media such as floppy disks, Zip disks, CD-ROMs and peripheral storage devices should be discouraged if not entirely eliminated. The IS policy should require that all external media be tested by the technical staff before use. Corporate e-mail and gateways should have filtering to scan and block all incoming attachments with executable extensions such as .exe, .com or .vbs. The use of Web mail (e.g. Yahoo, Hotmail, etc.) that bypass corporate e-mail filters and Web downloads should be discouraged if not entirely eliminated. The IS policy should require that all Web mail users register with the technical department. All Web users should be educated to understand the risks involved and what behavior is acceptable as per the IS Policy.

Detect

Log Turn on every log option available to you, and synchronize your system clocks. Automated logs with alarms should be used for the timely and appropriate notification of activities that violate or attempt to violate IS systems. This includes, but is not limited to, log file analysis, port watching, traffic monitoring, intrusion detection systems, or sniffing/snooping. The best gate will do no good if you do not know when some one is trying to knock it down. Log behavioral security measures that monitor employees' use of technology resources. If someone's behavior deviates from normal practice investigate the situation.

Intrusion-Detection Intrusion detection systems (IDS) monitor trunk lines and collect information about the packets that traverse the lines. This information is normally collected in logs that must be audited for malicious behavior. Sophisticated Intrusion-detection can be set up to notify administrators when systems are being accessed illegally.

Keep current of ways around intrusion detection. The coming widespread use of modern cryptographic techniques (Asymmetric Key Cryptography) will cripple the capability of some Intrusion Detection. Through encryption and redirection the competent hacker either is or will be completely immune to (IDS) security tools.

Set Limits Set up rules that prevent strange behavior on your system that is potentially damaging regardless of whether the threat is caused by a virus, human error, buffer overflow attacks, etc. Monitor all activity coming from outside as well as inside.

React

When an incident is discovered the entire staff must be prepared to react collectively in order to contain and minimize damage. This includes the user population who also should expect brief outages to service and know not to in-

terfere with the recovery process by making demands on affected services.

Remain Calm Panic breeds confusion, which cripples communication and makes coordination impossible. Staying calm helps avoid making critical errors. Staying calm also ensures the user base that the technical team is in charge and has the situation well in hand.

Setup a Central Command Have one designated contact point in one central command center. This is where all of the technical team will rally for their initial briefing. The command center will serve as the one point where all actions to fight the incident will be coordinated from. When a virus is spreading facility wide a command center will save time by allowing the responsible staff member in one known location. Here the task commander can be reached quickly to make the decisions that need to be made and to assign tasks based upon these decisions. The central command center should also be the one point of contact for the release of information to the users.

Work Your Plan Your Incident Response Plan is your greatest ally while in the "Hot Zone". It is the course of action that will be followed and defines what priority systems need to be protected restored first. By following the Incident Response Plan the technical staff will be focused and know where they are supposed to be and what is expected of them.

Document Take good notes on every thing no matter how trivial. Use a standard incident form that answers the four Ws; Who, What, When, and Where. Make sure that all staff members working on the incident have a notepad. Make a backup of the affected system and programs for future forensics whenever possible. Use new, unused hard drives or media and replace effected media. Keep the effected media as primary forensic evidence after the incident is resolved. Avoid speculation except when it is required to decide what to do. Too often the initial information in an incident is misinterpreted.

Notify Inform the user base as to the general nature of the situation and how it affects the normal workflow. Information prevents the start of the rumor chain. One person on the technical team, if staffing permits, should be assigned to update the general staff in close coordination with the command center. Enforce a "need to know" policy. The users should hear the prognosis not the diagnosis. Keep the details of the incident to the minimum for the users, what system are affected and how long they are expected to be out. Detailed technical information should be kept to a limited number of trusted individuals on the technical team involved in fighting the problem. Detailing vulnerabilities and how you were violated publicly can only lead to more attacks.

Use Alternate Communication Use out of band communications. If there is a possibility that the computers have been compromised, avoid using them for incident handling discussions, use telephones and faxes instead. Do not send information about the incident by electronic mail, talk, chat, or news this information may be intercepted by the attacker and used to worsen the situation.

Contain Take all the necessary steps to keep the problem from getting worse and spreading. Work with your Security Concept of Operations Plan. Separate critical on-air systems from the effected network and go into a protected standalone mode of operations. Disconnect all non-critical computers and systems as defined in your Concept of Operations Plan that are not yet affected in order to ensure that they stay clean. The easy way to do this type of mass disconnection is to shut down all but the critical Ethernet switches and hubs in your network. Do not be afraid to separate the sheep from the goats (with your current backups you know you can sort this out later). Remove all affected systems from the network as soon as possible.

Identify Know exactly what you are fixing and make sure that you have all the information to accomplish a clean fix. Missing one affected file on a single computer could restart the entire infection.

Resolve Fix it; take steps to correct the deficiencies that allowed the problem to occur. Again make sure that the complete fix is known and all the steps to make the fix are implemented.

Restore Get back in business. After checking your backups to ensure they are not compromised, restore your system from backups and monitor the system closely to determine whether it can resume its tasks.

Learn Do a full post mortem on the incident. Collect all notebooks and examine all notes taken during the incident. Diagnose in an isolated environment the affected data files that were collected. Meet with staff members both from the technical staff and the user base and solicit their input on how the event was handled. Learn from the experience, so you won't get caught unprepared the next time an incident of the same type occurs. Make sure that what is learned is used, add to your protective measures, update documentation and policies as needed. Information assurance is a dynamic process and will eventually fail if allowed to stagnate.

CONCLUSIONS

All broadcasters must become knowledgeable and proactive in dealing with Information Assurance (IA). Damage to your information systems can at worse knock you off the air, and lack of Information Assurance can compromise broadcast content, scheduling information or vital corporate data. Information assurance is a dynamic process and will eventually fail if allowed to stagnate.