☙GIAC Enterprises❧

Council for the Digital Age

Security Analysis and Recommendations

Rodney Caudle
GIAC-E Security Advisory Council
GISO – Basic Practical Assignment
Version 1.2
May 7th, 2002

Company Overview

GIAC Enterprises is a prominent law firm located in San Diego, CA. GIAC-E provides services for an assortment of clients ranging from large corporations to small estates at hourly increments. In addition, they also offer pro-bono work to qualifying individuals and organizations in order to give back to the community. GIAC Enterprises' most important asset is their reputation. They have established a reputation of unwavering integrity when dealing with their clients' private information. To maintain their reputation GIAC Enterprises requires a focused determination to remain on the cutting edge of Information Technology Security while providing a stable environment for its business operations.

IT Infrastructure

GIAC Enterprises has multiple satellite offices located throughout the United States. Their corporate network is a star topology; all branch offices connect through a private network to the corporate headquarters for access to centralized services. The services of interest are: Internet access, corporate email and collaboration, financial services, and the corporate document repository. The centralization of services allows for better management of critical information, the ability to share common research across offices and cost effective use of these services by all branch offices. Services, such as corporate email and collaboration, are provided at each branch office in addition to being maintained at the corporate headquarters where faster access is needed to information is needed for backup and recovery.

The corporate headquarters' local area network (LAN) is divided into four main areas: an Internet segment, an external demilitarized zone (DMZ), an internal DMZ and the internal networks. The Internet segment is the un-trusted connection to the Internet (see chart). The external DMZ is a semi trusted Virtual LAN (VLAN) that contains all the servers and services offered to customers, clients and business partners (see chart). The internal DMZ is a semi trusted VLAN that contains all the servers and services that provide a link to the branch offices (see diagram and chart). The internal networks represent the trusted corporate networks where the clients and client services reside (see chart). For extremely high-risk areas (like the Internet segment and the external DMZ) the division is logically and physically implemented with dedicated switches providing connectivity for each area. Separation of network traffic is augmented by Intrusion Detection System (IDS) Servers; connected to each area and tuned to detect "interesting" traffic for that area. Appendix A contains a diagram of the Local Area Network (LAN) at the corporate headquarters and a diagram of the Wide Area Network (WAN).

The branch office LANs resemble a simplified version of the corporate office LAN and are configured identically. This allows effective utilization of hardware and resources to administer the networks. The branch office LAN contains two areas: a DMZ and the internal networks. The DMZ of the branch offices contains all the equipment and services needed to connect to the corporate WAN. A list of this equipment can be found in Appendix B and a diagram in Appendix A. The internal networks contain all the equipment needed to support the general business activities for the branch office. IDS servers are utilized at each branch office to detect and report any "interesting" traffic.

MCI WorldCom, a first tier access provider of Internet connectivity, supplies the redundant T1 connections to the corporate office network and the frame relay connections to the branch offices. In addition, MCI WorldCom's Network Operations Center (NOC) provides first level monitoring, via dedicated frame relay access. Escalation procedures and contact personnel have been provided to MCI WorldCom's NOC for incident handling purposes. To support the NOC, MCI WorldCom co manages monitoring and alert servers at each GIAC-E office, including the corporate headquarters. GIAC-E is responsible for all hardware requirements for the monitoring and alert servers; while MCI WorldCom is responsible for providing and configuring the necessary software. Additionally, a software agent to receive alerts from Snort is installed on the monitoring and alert server. MCI WorldCom monitors servers and services within the corporate network as well as the connectivity links for the Internet and frame relay connections.

All inbound Internet resources, such as email, extranet websites, external DNS resolution, and VPN client access is filtered through the servers located in the external DMZ at the corporate headquarters. This provides a buffer between internal services and the Internet. If a denial of service (DoS), or some other form of attack, is commenced, the attackers must first "capture" one of the servers residing on the external DMZ before being able to commence an attack on the internal firewall. With adequate IDS servers and monitoring the attacker can be isolated and blocked before completing their attack. Internet email is filtered through the SMTP email gateway servers where, if the account exists, the email is forwarded to the corporate exchange servers located in the internal DMZ. Once the SMTP email gateway servers validate the account, the email is scanned with virus detection software. If a virus is found, the email is deleted and a notice is forwarded to the intended receiver. Extranet web servers allow customers to view billing records and submit claims or requests through these services. GIAC-E employees who travel can authenticate to the Avaya VPN server where their session is redirected to the appropriate VPN server on the internal DMZ or branch office. This provides access to corporate resources while the employees are traveling. The VPN servers also offer a backup to the corporate frame relay network through Digital Subscriber Line (DSL) connection at each branch office.

Internet access for GIAC-E is centralized through a tiered implementation of the open source proxy server Squid. First tier proxy servers are located in the external DMZ at the corporate headquarters. The second tier proxy servers reside in the internal DMZ at the corporate headquarters and provide access to clients at the corporate headquarters. If the clients request a website from the second tier servers that does not exist in the cache, the request is sent to the first tier proxy servers for retrieval. In each of the branch offices there are third tier proxy servers providing access to Internet resources. Similar to a client at the corporate headquarters, if request for a file that is not in the cache of the third tier proxy servers is received, this request is sent to the second tier proxy servers for retrieval. This provides for centralized control and use of Internet resources for conducting business because all requests for Internet resources occur between the proxy servers until the first tier is reached. The first tier proxy servers require filtering of clients' access to restricted sites. To help enforce these rules, all outbound Internet traffic for HTTP, FTP, and HTTPS is blocked except traffic originating from the IP addresses of the first tier proxy servers. Appendix A contains a diagram of the proxy architecture for GIAC-E.

Domain Name Service (DNS) is also centralized through a hierarchical structure. This allows standardization of client configuration across the branch offices. The DNS is also configured to receive automatic updates from DHCP clients when a successful lease occurs. DNS has two aspects that must be addressed: updating the relevant zone files and responding to client requests. A master/slave relationship is used to control updating the relevant zone files. The master DNS server, which receives all the updates, is located in the internal DMZ at the corporate headquarters. All other DNS servers are slaves, receiving updates of the zone files from the master. The second aspect, responding to client requests also includes two types of servers. The primary DNS server for "giac-e.com", which is always asked first for resolution of a name, is located in the external DMZ at corporate headquarters. The secondary DNS server, used only if the primary doesn't respond, is located with the service provider, MCI WorldCom. Utilizing the concept of different views for clients, the internal clients are referred to the DNS server at their local office LAN first.

The corporate document repository is a custom application developed especially for GIAC-E. This application allows employees to manage the enormous amounts of research conducted during normal business proceeding. All data is stored encrypted on the Network Appliance cluster. Documents are classified in different categories depending on the sensitivity of the data contained. The document maintainer controls access to these documents. To gain access to the document, the document maintainer must enter the employee's public RSA key into the encryption of the document. This will allow the employee to decrypt and view the document. In addition, the employee must have the appropriate unique key generator needed to log into the server. This generator uses a S-Key encryption scheme to control communications between the client desktop and the server. Special access is given to employees who need to make changes to the document. At each branch office there is a smaller version of the document repository server that handles requests for local clients. Documents are kept in the local cache of the document repository server for the access lifetime of the document. After the lifetime expires, the document is digitally "wiped" from the disk. The document can be requested from the main document repository at any time until it is purged from the main repository server.

In summary, the IT infrastructure at GIAC-E, segmented network architecture provides controlled access to centralized services located at the corporate headquarters. All branch offices are connected to the corporate headquarters through a frame relay cloud; utilizing VPN connections over DSL as a backup. All inbound and outbound Internet traffic is filtered through the servers located in the external DMZ for access control, content filtering and virus detection. Traveling employees can gain access to corporate resources through Avaya's VPN client software. Intrusion Detection System (IDS) Servers provide detection of "interesting" traffic, which is reported to the NOC located at MCI WorldCom. The document repository provides secure access to sensitive documents in a controlled manner. Internet services are provided to GIAC-E employees using a tiered proxy server architecture. Finally, employees are given access to resources through many devices, including laptops, desktops and PDAs.

Business Operations

The key business functions for GIAC-E, supported by Information Technology (IT), include group communication and collaboration, employee time tracking, information management and distribution, and backup and disaster recovery. The unique requirements of GIAC-E require that these services be available twenty-four hours a day, seven days a week. All services present in the external DMZ and internal DMZ are considered critical business services. These services facilitate interaction with external entities and branch offices. A complete list of the software packages utilized in the different areas of GIAC-E's corporate networks is available in Appendix B.

Group communication and collaboration includes functionality such as email and sharing of calendars. GIAC-E specific servers and services directly supporting this functionality include the email gateway servers (running Qmail 1.03), corporate exchange servers (running Microsoft Exchange Server 2000) at the corporate office, and the corporate exchange servers at the branch offices. The DNS server architecture is important for facilitating the smooth flow of collaboration services. The primary DNS server (running BIND 8.2.3) at the corporate headquarters and the secondary DNS servers (running BIND 8.2.3) at the branch offices complete the necessary components of the communication architecture.

The employee time tracking application is hosted by a Value Added Reseller (VAR) for Oracle Financial Suite. This allows for centralized management and access to the financial applications for GIAC-E. This financial suite is used for all financial aspects of GIAC-E corporate and the branch offices. To facilitate tracking of employee time, employees enter the number of hours worked and which case file the hours should be billed against. This allows GIAC-E customers to view up-to-date billing information quickly and easily without compromising corporate network security.

The information management and distribution system is a customized application facilitating the management of information for GIAC-E. This information is a comprehensive representation of all business activities currently under way at GIAC-E. Depending on the classification of the document, access is granted through a specific network. Access to GIAC-E private and proprietary information is only accessible through the use of a Virtual Private Network (VPN) client. This VPN client grants access to an isolated network within the internal DMZ that only network traffic bound for the protected vaults of the information repository is allowed. The switch filters this traffic, only allowing traffic from the VPN Server bound for the interfaces of the document repository. Information creators are granted special access to necessary information to control changes that can be introduced to the information. A special server is required at each branch office as well as a central repository at the corporate headquarters. All information is retained at the corporate headquarters for backup and recovery purposes.

Information is cached at the branch office servers for local access as needed and allowed. A diagram of the document repository architecture is located in Appendix A.

Backup and disaster recovery is an important aspect of GIAC-E's business. The loss of a single document could cause irreplaceable harm to the company's reputation. Backups are performed using Tivoli Storage Manager 4.1. Iron Mountain Data Services provides disaster recovery and offsite tape management. Onsite backups are stored in a locked, fireproof vault until they are picked up by Iron Mountain once a week. All backups are duplicated with one copy going to a local offsite location and a second copy going to the disaster recovery site. Data retention for data is 1 year of tapes for disaster recovery, 6 months for the local offsite copy and 3 months for the onsite copy of data. Disaster recovery is currently being evaluated to determine which services would benefit from a hot-site to guarantee better availability.

Areas of Risk

There are many areas of risk when conducting business within an organization. Company and client information must be secured against loss of confidentiality, loss of integrity and loss of availability with a reasonable guarantee of success. The three areas of highest risk for GIAC-E are damage to the confidentiality and/or integrity of the document repository (Crown Jewels), loss of availability of communications (group communication and collaboration), and loss of integrity and confidentiality due to weak or non-existent client passwords. Addressing these issues with appropriate policies and guidelines will assist GIAC-E in meeting their security requirements.

No. 1: Protecting the Corporate Value Proposition

There are two aspects to the protection of GIAC-E's core business: confidentiality and integrity. Confidentiality is compromised when unauthorized access to the information stored in the corporate repository occurs. Integrity is lost when data is corrupted or deleted within the corporate repository. Confidentiality takes priority because of the loss of business and/or revenue due to lack of customer confidence in GIAC-E's ability to protect confidential customer information. However, loss of the availability of important business records can have a direct impact on business revenues as well. According to BBC News[1] the largest threat to a corporation's security is disgruntled employees. According to the article, "48% of large companies blame their worst security incident on employees". GIAC-E should implement multiple-layers of protection for the information stored in the corporate repository.

The first level of protection should be developing a comprehensive policy for granting access to the different classifications of information. Depending on the classification of the information in question, multiple levels of approval should be required when granting access to the information. Once access has been granted, all actions should be monitored and reported to the NOC. GIAC-E has a policy in place to categorize and control GIAC-E private and proprietary information, but the policy needs to be updated to reflect recent advances in Information Technology practices.

[1] BBC News article: http://news.bbc.co.uk/hi/english/sci/tech/newsid_1946000/1946368.stm

The second layer of protection should be isolation of access to the corporate repository. Access to the corporate repository should be enabled by the use of a VPN Client to gain access to the isolated network segment where this information would be available. The VPN Client should use different account information from the VPN Client used when traveling. GIAC-E currently does not have this layer in place. The corporate repository is accessible through the internal DMZ without filtering of packets. GIAC-E should implement an isolated network segment to protect access to this information. GIAC-E also needs to develop policies, procedures and guidelines for enabling access to this network segment for current technology such as LAN, Wireless LAN, and PDAs.

The third layer of protection should be the software used when viewing the information. A distinction should be made between the software used by clients to access the corporate repository and the software used by the servers in the branch offices to request access to the documents. Whether the information is intended to be viewed or retrieved, the software should keep the data encrypted at all times, only allowing the viewable portion of the document to be unencrypted in memory at the time of viewing. When transmitting the information between servers the information stream should also be encrypted. This custom software should disable some functions within the environment, like printing and saving, prior to displaying the information. GIAC-E currently has a custom software package in place today that accomplishes most aspects of this requirement. However, the software does make use of temporary files on the client computers when viewing the information. These files are unencrypted and could be used to gain unauthorized access to information. Also, this software does not currently encrypt the information stream from the server to the client/server. The encryption of the information stream would also be accomplished with the implementation of the isolated network segment.

Monitoring the document repository using non-invasive measures, such as MD5 Checksum comparison, would provide a fourth layer of protections. Monitoring the current state of the information and ensuring that appropriate backup and archival policies are in place can protect against loss of integrity. If inappropriate changes occur, the existing document can be replaced with a backup copy and an appropriate notification sent to the effected parties. GIAC-E currently has detailed policies on backup and retrieval of information. This aspect has been completed recently with the implementation of the Tivoli Storage Manager and procedures surrounding that project. These policies adequately handle this aspect of protecting the corporate information repository.

GIAC-E conducts business based on a reputation for integrity when dealing with confidential customer information. This information is a direct result of an investment that GIAC-E made to address this aspect of its business landscape. GIAC-E has technological restraints in place to protect the corporate information repository. Additional technological restraints should be added to further protect the information. In addition to technological restraints, strict policies should exist to determine acceptable actions to the classifications of information stored within the repository. GIAC-E current policies to categorize and control GIAC-E private and proprietary information do not provide for recent advances in Information Technology. These policies should be updated immediately and procedures put in place to handle these new technologies.

No. 2: Loss of communication

The speed of business is driven by group collaboration and communication between GIAC-E branch offices. The ability to effectively communicate has a direct effect on the number of billable hours each month. Minimizing the outages to non-business hours means greater possible revenue each month. Loss of billable time due to outages during business hours directly affects the financial revenue of GIAC-E. To mitigate the threat of communication outages and their threat to the financial bottom line, GIAC-E has taken several prevention steps.

First, they provide user training for email features in the form of a one-hour course, which is attended four times a year by all employees. This course covers appropriate use of email and how to avoid "suspicious" emails that might contain a virus. Secondly, virus detection software is used at several points along the email trail of delivery. The firewall scans incoming Simple Mail Transfer Protocol (SMTP) connections for certain information, rejecting email with suspicious content. The corporate email servers scan all incoming email, looking more in depth to find suspicious content. Finally, the user's computer is running an up-to-date copy of virus detection software as a final line of defense before the user gains access to the email.

Second, implementation of after-hour maintenance windows when standard work may be performed on the server base allows for controlled outages to be completed without reducing the number of billable hours. During these windows, the employees should not be conducting business that would require access to IT resources. Communication between appropriate parties can eliminate the possible conflict between an outage and a required over-night preparation session.

Finally, the use of redundancy for critical resources is in place. Redundant T1 lines for providing connectivity to the Internet are currently in place. A corporate frame relay provides connectivity with the branch offices. A DSL line is installed with VPN support as a backup for the frame relay during outages. Redundant servers with fail-over capability are in place for critical services such as email, DNS and the corporate information repository.

GIAC-E has taken appropriate steps to protect against loss of communications. Without considering extreme circumstances, the protections in place will provide adequate availability of group communication and collaboration resources for GIAC-E.

No. 3: Weak or non-existent client passwords

Passwords have always been a point of contention for secure access to network resources. Every business faces the need to balance an easily maintained client password convention against a non-guessable password formula. The ramifications of an easily guessed password must be weighed against a more difficult password that requires the users to keep a copy in an unsecured location. Gaining unauthorized access to information and resources by guessing a user's password could cause a loss of business revenue, legal action against GIAC-E, and financial liability. Reducing this possibility is easily avoided by implementing a number of safeguards.

GIAC-E has implemented a password policy requiring: a minimum of six letters for a password, the inclusion of a non-alpha character and tracking a certain number of old passwords to reduce password recycling. This policy provides adequate protection against easily guessed passwords if the clients adhere to the policy. GIAC-E periodically scans their client passwords with a password cracker to determine if any weak or non-existent passwords exist. All users found with a weak or non-existent password should be dealt with according to the actions stated within the policy.

GIAC-E has taken the necessary precautions for protecting against weak and/or non-existent client passwords. Updating the password cracker's dictionary will ensure that these measures are sufficient.

Evaluation of Security Policy for Categorization and Control of GIAC-E Information

A full copy of the security policy being evaluated can be found in Appendix C. This policy defines the categories of information and the means of control for each category. This policy is a sanitized version of a currently active policy. To suit the nature of this paper, the name of the company has been changed to GIAC-E. All references to this policy will be treated as an existing policy within GIAC-E.

Information embodies two forms: physical information (paper) and digital information (electronic files). Overall this policy does a good job of addressing the categorizing and control of physical information. However, as in any robust security policy, additional information is needed to reflect the growing trend toward digital media and electronic distribution of information. Additional instructions for electronic media such as Digital Versatile Discs (DVDs), Compact Discs (CDs), Compact Flash and other forms to come in the future need to be addressed and maintained to keep the policy up to date. Guidelines for controlling electronic distribution of electronic information need to be included in this policy. These guidelines would enable this policy to handle the changes that the digital age has brought to Information Technology (IT).

The "Storage and Handling of Controlled Information – Electronic" section mentions that "Information Technology and the system owner are responsible during system development to identify and/or update the identification of controlled information and assure necessary security". At first glance, this seems like an adequate statement. However, the scope of the policy did not restrict itself from addressing electronic information. In addition, no policy was present within Information Technology to address this assignment leading to inconsistent goals and implementations across the project base. Corporations are heading towards a "paperless" environment to reduce costs and waste bringing the need for more definite policies addressing the special aspects of digital information. These policies should be as clear, if not clearer, than the standards that this policy describes for physical information.

An attempt to address electronic media in this policy mentions email and information present on an Intranet. Additional forms of electronic media, such as DVD, CD, Compact Flash Cards, and other forms that represent digital copies of information need to be addressed. As the price of the CD Recorder has dropped dramatically in recent years and the level of expertise present in the average user has increased, making a digital copy of information can be accomplished in a very short period of time. Without instructions to address and control this kind of reproduction of information adequate protection cannot be in place.

Electronic distribution of information is not mentioned in this policy. Restriction of the distribution of information in general is only addressed adequately in the case of GIAC-E PRIVATE information. All other forms of information distribution are not mention even when the possibility of a blanket statement is included. This would include File Transfer Protocol (FTP), copying of information across a network, caching instructions for proxy servers and many more. In the past, all of these forms required a physical connection to the corporate LAN to make use of these forms of distribution. However, with the introduction of wireless LANs into the corporate landscape the boundaries between “inside” and “outside” are significantly blurred. Wireless LANs broadcast a signal that requires no physical attachment to the corporate network allowing anyone with the appropriate technology access to the information present. In addition to wireless LAN technologies there are also portable devices, like cell phones, personal data assistants (PDAs), and even PCMCIA cards that can connect a user to the external network of a cellular telephone company like Sprint.

In conclusion, this policy adequately addresses the concerns of physical information but falls short of addressing electronic information and the distribution of electronic information. The consideration of information as electronic and physical would help this policy become better able to address issues for Information Technology. Periodic revalidation by subject matter experts would provide the continuity needed to keep the policy in sync with current business practices of corporate IT.

Revision of Security Policy for Categorization and Control of GIAC-E Information

Policy

Information of a private and sensitive business nature shall be controlled and protected so as to preclude arbitrary or careless disclosure.

Purpose

The purpose of this Corporate Policy (CP) is to define the five (5) categories of GIAC-E-controlled information and the means of control required for each category.

Ownership

This CP is the responsibility of the Legal Department.

Limitations

This CP is limited to the categories of information as described herein.

Definitions

GIAC-E PROPRIETARY – Information specifically related to GIAC-E-generated concepts, discoveries, techniques, processes, products, and other information that gives GIAC-E an advantage over its competitors who do not know or use such information. Such information is commonly referred to as trade secrets. Examples are: new products, developments, inventions, design drawings, test methods, test results, production drawings and listings of suppliers, technical innovations and supporters.

NOTE: Special care must be taken in the identification of controlled information submitted to the government. The terms or legends that the government will observe vary from those used by GIAC-E or others in non-governmental business. To prevent disclosure, information submitted to the government should be identified as GIAC-E Proprietary.

GIAC-E PROPRIETARY – LIMITED ACCESS – Information that is determined by the responsible control executive to be especially sensitive, and for which tighter controls are required. Examples are: critical process and material specifications, and technical information that is known to be especially valuable to GIAC-E.

GIAC-E PRIVATE – Sensitive administrative information, primarily of a financial or marketing nature. Examples are: proposal data, prices, contractural negotiations, financial records, wage/salary data, and marketing plans. In addition, technical information such as minutes, internal memoranda, and other documents containing sensitive technical data.

GIAC-E PRIVATE – LIMITED DISTRIBUTION – GIAC-E Private information that is determined by the responsible control executive to be especially sensitive, and for which tighter controls are required. Examples are: financial summaries, giving the financial status of the company or any operating unit, and information relating to critical business strategies.

OTHER THAN GIAC-E DATA – Proprietary and private information of other companies, specifically relating to the company's techniques, processes and products. Examples are: customer design drawings, supplier design drawings, engineering data and technical information that is known to be especially valuable and has been accepted on that basis by GIAC-E.

NOTE Proprietary and private information of other companies will be handled and stored in the same manner as similar GIAC-E information, unless other restrictions or conditions have been agreed to by GIAC-E and the other party, or in accordance with proprietary information agreements in effect between GIAC-E and the other party. GIAC-E employees will not accept information that is represented by the other party as proprietary unless an agreement exists, or has first been prepared and approved by the Corporate Law Office, and executed by the parties. Prospective suppliers, associate contractors, contractors or customers who attempt to leave proprietary or private information with a GIAC-E employee shall be asked to sign an Agreement Regarding Unsolicited Non-Proprietary Disclosure unless there is an existing agreement. It is the responsibility of GIAC-E personnel receiving or holding such information to ensure that all authorization receipts are advised of any restrictions or conditions governing its use.

ELECTRONIC INFORMATION FILES -- digital representation of information stored on floppy disks (3.5" & 5.25"), compact discs, DVDs, magnetic tape, hard drives (SCSI, IDE, UDMA-33/66/100/133, USB, PCMCIA), compact flash cards, memory sticks (Sony), and all other forms where information is stored as bits (1's and 0's) while "at rest".

ELECTRONIC INFORMATION FILES – APPLICATIONS – digital representation of information stored as bits and accessed from remote computers using applications. This includes such applications as proxy servers, HTTP servers, electronic mail servers, electronic mail caches, temporary file systems and temporary file caches.

ELECTRONIC INFORMATION STREAM – digital representation of information as a binary stream, text stream, digital video stream or any other stream where information is in transit between two physical mediums such as protocols like SCP, FTP, SMTP, POP3, IMAP, HTTP, HTTPS, and TCP/IP[2].

ELECTRONIC INFORMATION STREAM – WIRELESS -- digital representation of information as a binary stream, text stream, digital video stream or any other stream where information is in transit between two physical mediums broadcast without the use of a physical connection between exchanging devices. This includes transmission mediums like 802.1x, Infrared, microwave, and cellular phone networks.

[2] TCP/IP is actually a suite of protocols used as a basis for a large part of electronic distribution today. Please see the Glossary for a more in depth definition of TCP/IP.

GENERAL

Application

The general types of proprietary and private information covered by this CP include but are not limited to the following:

- Manufacturing methods, techniques, concepts, discoveries and test methods
- Design drawings
- Financial matters
- Proposal data and marketing plans
- Information of other companies
- Business relationships, lists of suppliers, associate and subcontractor
- Exhibits and models

Media

Physical

The five categories of controlled physical information could be conveyed by means of:

1. Written documentation
2. Photographs or slides
3. Motion picture or video tapes
4. Technical discussions such as meetings, presentations and phone conversations

Electronic

Electronic media is the digital representation of GIAC-E controlled information. The types of electronic media covered by this CP include but are not limited to the following:

1. Electronic Information Files
2. Electronic Information Files - Applications
3. Electronic Information Stream
4. Electronic Information Stream - Wireless

The technical data disclosed should be limited to that which generally explains any given process or concept and should not disclose such details which would enable a competitor to take advantage of the data (i.e., to form a counter approach or proposal).

Classification of Information

The decision to classify, declassify and control GIAC-E information (including verbal communication, reproduction, distribution, and disposition) shall be made at the following levels:

GIAC-E PROPRIETARY – The originator of the information

GIAC-E PROPRIETARY- LIMITED ACCESS – The manager of the generating department.

GIAC-E PRIVATE – The originator of the information

GIAC-E PRIVATE – LIMITED DISTRIBUTION – The vice president responsible for the generating department

OTHER THAN GIAC-E DATA – The originator of the information

Identification of Controlled Information

Physical

GIAC-E-controlled information will be identified by stamping the appropriate category name on both the outside cover and all pages and by including the following statements on the cover and first numbered page, where applicable:

GIAC-E PROPRIETARY – This document contains information that is proprietary to GIAC-E or to one of its customers. Any reproduction, disclosure or use of this information without GIAC-E's written consent is expressly prohibited.

GIAC-E PROPRIETARY- LIMITED ACCESS – This document contains sensitive information that is proprietary to GIAC-E or one of its customers and is not to be copied or disclosed to unauthorized persons. Disclosure to unauthorized persons may result in disciplinary action, including discharge and legal proceedings.

GIAC-E PRIVATE – These documents only require the stamp and do not have any statement following.

GIAC-E PRIVATE – LIMITED DISTRIBUTION – This document is limited in distribution and is not to be copied or disclosed to unauthorized persons. Disclosure to unauthorized persons may result in disciplinary action, including discharge and legal proceedings.

Electronic Information Streams& Electronic Information Streams – Wireless

No requirements are present for these streams.

Electronic Information Files & Electronic Information Files - Applications

GIAC-E-controlled information will be identified by prepending appropriate header information with the category name present on all pages and by including the following statements on the first page, where applicable:

> **GIAC-E PROPRIETARY** – This digital document contains information that is proprietary to GIAC-E or to one of its customers. Any reproduction, distribution, disclosure or use of this information without GIAC-E's written consent is expressly prohibited.
>
> **GIAC-E PROPRIETARY- LIMITED ACCESS** – This digital document contains sensitive information that is proprietary to GIAC-E or one of its customers and is not to be copied or disclosed to unauthorized persons. Disclosure to unauthorized persons may result in disciplinary action, including discharge and legal proceedings.
>
> **GIAC-E PRIVATE** – These digital documents only require the header information and do not have any statement following.
>
> **GIAC-E PRIVATE – LIMITED DISTRIBUTION** – This digital document is limited in distribution and is not to be copied or disclosed to unauthorized persons. Disclosure to unauthorized persons may result in disciplinary action, including discharge and legal proceedings.

Storage and Handling of Controlled Information

NOTE: Management has the responsibility to insure GIAC-E controlled information, as defined herein, is stored properly, and to take disciplinary action when unprotected information is discovered.

Physical

The following criteria must be followed in order to ensure proper storage and handling of controlled information.

- Only approved storage containers (safes and filing cabinets) will be used. These containers must be locked during nonworking hours unless the container is in a locked room.
- Safes and files must *be* identified as to the highest category of information contained therein.
- Access to Safes and files will be controlled by regulated keys and combinations and authorized personnel working in area.
- Controlled access areas will be established where feasible.

- Cover sheets noting the category of the controlled information must be on al proprietary information at all times when not in direct working control of an individual.
- Reproduction of subject information must only be done on machines that do not have a memory, i.e., an internal tape or other means that records what is being reproduced.

ELECTRONIC INFORMATION FILES

In addition to the general requirements found elsewhere in this document, controlled information on the Intranet must meet the following criteria.

GIAC-E PROPRIETARY – Security shall be provided such that (1) a password shall be required to access the information and (2) access will be monitored and recorded. Backup will be provided such that there are adequate copies of this digital information to protect against loss.

GIAC-E PROPRIETARY- LIMITED ACCESS – Security shall be provided such that (1) the information may not be printed by the user; (2) a password shall be required to access the information and (3) access will be monitored and recorded. Backup will be provided such that there are adequate copies of this digital information to protect against loss.

GIAC-E PRIVATE – Security shall be provided such that (1) the information may not be printed by the user; (2) a password shall be required to access the information; and (3) public key/private key encryption (1024 bits or greater) shall be used to protect data at rest; and (4) access will be monitored and recorded. Backup will be provided such that there are adequate copies of this digital information to protect against loss.

GIAC-E PRIVATE – LIMITED DISTRIBUTION – Security shall be provided such that (1) the information may not be printed by the user; (2) a password shall be required to access the information; and (3) public key/private key encryption (1024 bits or greater) shall be used to protect data at rest; (5) temporary copies will remain encrypted in RAM and decrypted only when viewed by the user; (6) digital copies will be present only for the purposes of backup and disaster recovery and (7) access will be monitored and recorded. Backup will be provided such that there are adequate copies of this digital information to protect against loss. *Information in this category shall not be available through the use of* *technologies that are unencrypted, such as an Intranet or Extranet.*

OTHER THAN GIAC-E DATA – In general, information in this category is treated as GIAC-E Proprietary and is available through the Automated Blueprint Crib (ABC).

ELECTRONIC INFORMATION FILES – APPLICATIONS

In addition to the general requirements found elsewhere in this document, controlled information on the Intranet must meet the following criteria.

GIAC-E PROPRIETARY – Security shall be provided such that (1) a password shall be required to access the information and (2) access will be monitored and recorded.

GIAC-E PROPRIETARY- LIMITED ACCESS – Security shall be provided such that (1) the information may not be printed by the user; (2) a password shall be required to access the information and (3) access will be monitored and recorded.

GIAC-E PRIVATE – Security shall be provided such that (1) the information may not be printed by the user; (2) a password shall be required to access the information; and (3) public key/private key encryption (1024 bits or greater) shall be used to protect data at rest; and (4) access will be monitored and recorded.

GIAC-E PRIVATE – LIMITED DISTRIBUTION – Security shall be provided such that (1) the information may not be printed by the user; (2) a password shall be required to access the information; and (3) public key/private key encryption (1024 bits or greater) shall be used to protect data at rest; (5) temporary copies will remain encrypted in RAM and decrypted only when viewed by the user; (6) digital copies will be present only for the purposes of backup and disaster recovery and (7) access will be monitored and recorded. *Information in this category shall not be available through the use of technologies that are unencrypted, such as an Intranet or Extranet.*

OTHER THAN GIAC-E DATA – In general, information in this category is treated as GIAC-E Proprietary and is available through the Automated Blueprint Crib (ABC).

ELECTRONIC INFORMATION STREAMS

ELECTRONIC INFORMATION STREAMS - WIRELESS

GIAC-E PROPRIETARY – Security shall be provided such that (1) at least 40-bit encryption is used.

GIAC-E PROPRIETARY- LIMITED ACCESS - Security shall be provided such that (1) at least 128-bit encryption is used to protect the information stream and (2) restriction of distribution of the information stream to appropriate IP addresses is in use.

GIAC-E PRIVATE - Security shall be provided such that (1) at least 128-bit encryption is used to protect the information stream; (2) restriction of distribution of the information stream to appropriate IP addresses is in use and (3) technologies which do not keep a temporary copy on a physical medium will be used to distribute the data.

GIAC-E PRIVATE – LIMITED DISTRIBUTION- Security shall be provided such that (1) at least 128-bit encryption is used to protect the information stream; (2) restriction of distribution of the information stream to appropriate IP addresses is in use and (3) technologies which do not keep a temporary copy on a physical medium will be used to distribute the data.

OTHER THAN GIAC-E DATA - In general, information in this category is treated as GIAC-E Proprietary and limited to the same restrictions as defined above.

Distribution of Controlled Information

Distribution of subject material will be as specified herein. When GIAC-E internal mail system is utilized, the outside envelope must be clearly stamped reflecting the highest category of information contained therein.

When proprietary or private electronic information is transmitted outside GIAC-E, such information must be encrypted prior to distribution. This includes technologies such as email, web services, and FTP.

When proprietary or private information is transmitted outside GIAC-E, such information must be in a double envelope with the category of information clearly marked on the inner envelope. When appropriate, a nondisclosure statement will be included outside the inner envelope.

Transmittal of GIAC-E Proprietary – Limited Access or GIAC-E Private – Limited Distribution information must be by hand or by registered mail only.

Release of Controlled Information

When proprietary or private information is included in bids, proposals, or in any way issued to companies or agencies for their review, a nondisclosure statement approved by the Corporate Law Office must be included in the bid or proposal.

When proprietary or private information is included in bids, proposals or in any way viewable by companies or agencies for their review through GIAC-E Intranet or GIAC-E Extranet sites, a nondisclosure statement approved by the Corporate Law Office must be acknowledged prior to access being granted.

No proprietary or private information will be released to the public without prior approval of the Corporate Law Office and Corporate Public Affairs.

Destruction Procedure

GIAC-E-controlled proprietary and private information no longer needed will be disposed of in a manner which eliminates the danger of them falling into the hands of unauthorized recipients. For example, this may be accomplished by returning the information to the originator, by shredding, or by depositing in a receptacle dedicated to destruction of proprietary and private data.

GIAC-E controlled proprietary and private electronic information no longer in use will be disposed of in a manner that eliminates the ability to extract such data from the physical medium at a later time.

PROCEDURE

Not Applicable

REFERENCES

Not Applicable

Procedure for Enabling Access of GIAC-E Proprietary and Private Information with ELECTRONIC INFORMATION STREAMS – WIRELESS

Purpose

The purpose of this Corporate Procedure (CP) is to define the steps necessary to enable access to GIAC-E-controlled information utilizing wireless technologies.

Background

With the introduction of wireless LANs into the corporate landscape the boundaries between "inside" and "outside" are growing increasingly blurred. Wireless LANs communicate with a signal that requires no physical attachment to the corporate network allowing anyone with the appropriate technology access to the information present. Wireless LANs are incredibly useful in certain application, such as a production floor. The use of a wireless LAN can significantly reduce the total cost of ownership for a facility. However, adequate procedures need to be in place to protect the information that is broadcast.

GIAC-E has a Corporate Policy addressing critical information within an Electronic Information Stream – Wireless. This policy requires the use of encryption technology to access protected resources. This procedure addresses how to gain access to these protected resources using a wireless LAN.

Ownership

This CP is the responsibility of the Information Technology – Wireless Department.

Limitations

This CP is limited to the categories of information as described in Security Policy for the Categorization and Control of GIAC-E Information. This CP is limited to the categories of wireless technologies as described below.

Definitions

There are many divisions of wireless technologies; this CP is limited to this type:

> WIRELESS – LAN – this includes technologies surrounding 802.11, 802.11a, 802.11b, and 802.11g and any derivative technologies developed in the future. These technologies facilitate the connecting of a single device to the corporate network without the presence of a physical connection to the corporate network.

Procedure

WIRELESS-LAN

1. Request a wireless Ethernet (802.11b) card from the Information Technology – Fulfillment Department. The appropriate form (80211b-REQ) is available from the Intranet. The wireless cards are PCMCIA, if the system in question is not a laptop, a PCI adapter must also be requisitioned. Add the line "PCI Adapter for wireless PCMCIA card" in the Additional Hardware section of the form.

2. If this card will use static addressing, acquire the appropriate information from the Information Technology – Network Department (form IPREQ). The following information is needed:

   □ IP Address ____________________
   □ Network Mask (255.255.xxx.xxx) ____________________
   □ a. I Broadcast Address ____________________
   □ P Default Gateway ____________________
   □ DNS Server(s) ____________________

3. Acquire credentials for wireless VPN connectivity to the Corporate Information Store (form VPNREQ-CORPINFO).

4. Install the wireless network card into the laptop

5. Install the wireless software

   a. If this card is going to be DHCP, no adjustments need to be made

   b. If this card will use static IP addressing, enter the appropriate information acquired in step #2.

6. Configure wireless software for connectivity. When connecting to the wireless LAN, all information is encrypted using the Wireless Encryption Protocol (WEP). The following information is for all GIAC-E wireless LANs:

□	Bits for encryption	256
□	Frequency number (1..11)	7
□	Unique key	!giac-(e)

7. Test and verify connectivity using the following checklist:

   □ Ping 127.0.0.1 ______________
   □ Ping IP Address entered in step 5b ______________
   □ Ping default gateway entered in step 5b ______________
   □ Open web browser and go to http://www.yahoo.com ______________

8. Install the VPN Connectivity software from Avaya Communications

9. Configure the VPN Connectivity software according to the Standard Job Instructions – Avaya VPN Client Configuration. This will enable access to the isolated network segment for the corporate information store.

10. Activate VPN Client and verify access to GIAC-E protected information using the Standard Job Instructions for "Accessing the corporate information store".

    Note: Access to general network resources requires a wireless network card, software and configuration information for the wireless card. Access for GIAC-E proprietary and private information requires VPN Access for access to the protected network.

References

The SANS Institute, “The Twenty Most Critical Internet Security Vulnerabilities (Updated)” Version 2.502 January 30th, 2002. URL: http://www.sans.org/top20.htm (March 7th, 2002)

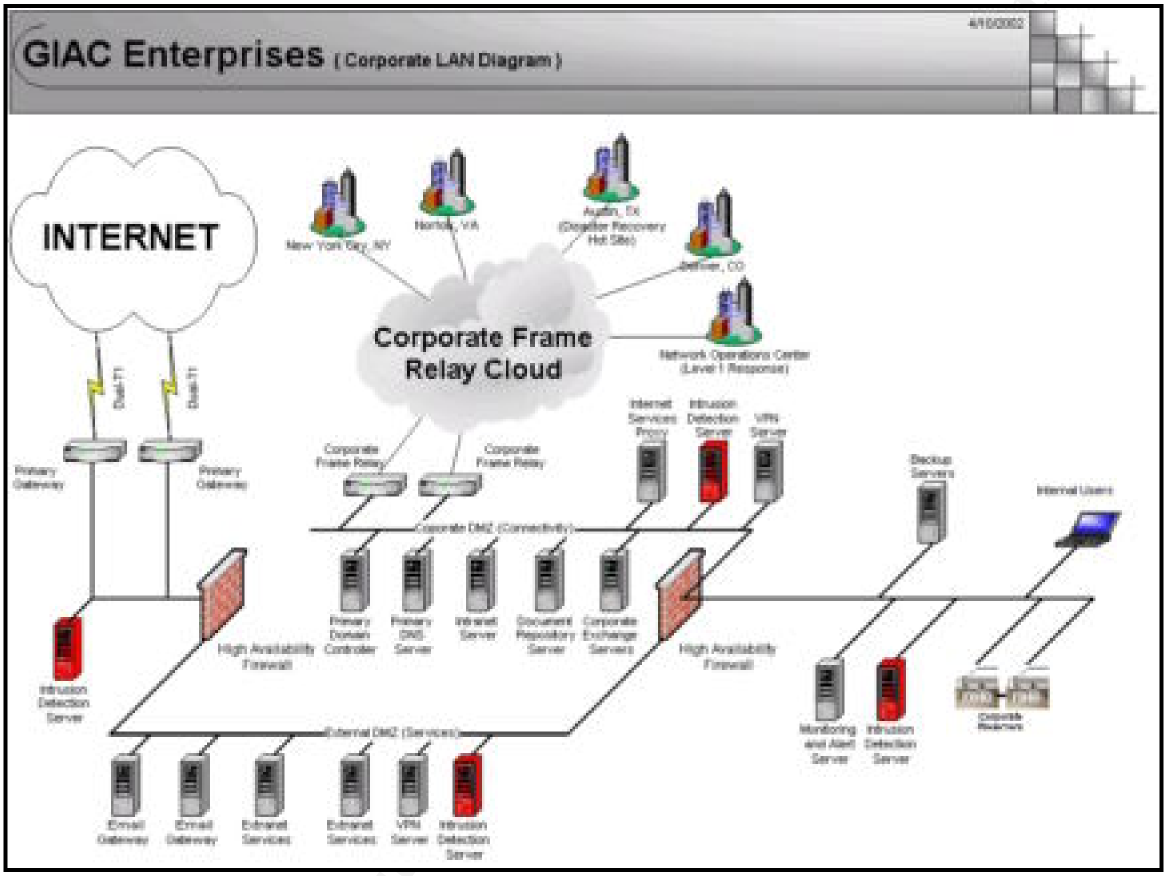
Sun Microsystems, Inc. “How to Develop a Network Security Policy White Paper” URL: http://www.sun.com/software/white-papers/wp-security-devsecpolicy/ (March 25th, 2002)

J. Patrick Lindley, “Technical Writing for IT Security Policies in Five Easy Steps” September 20th, 2001. URL: http://rr.sans.org/policy/tech_writing.php (March 25th, 2002)

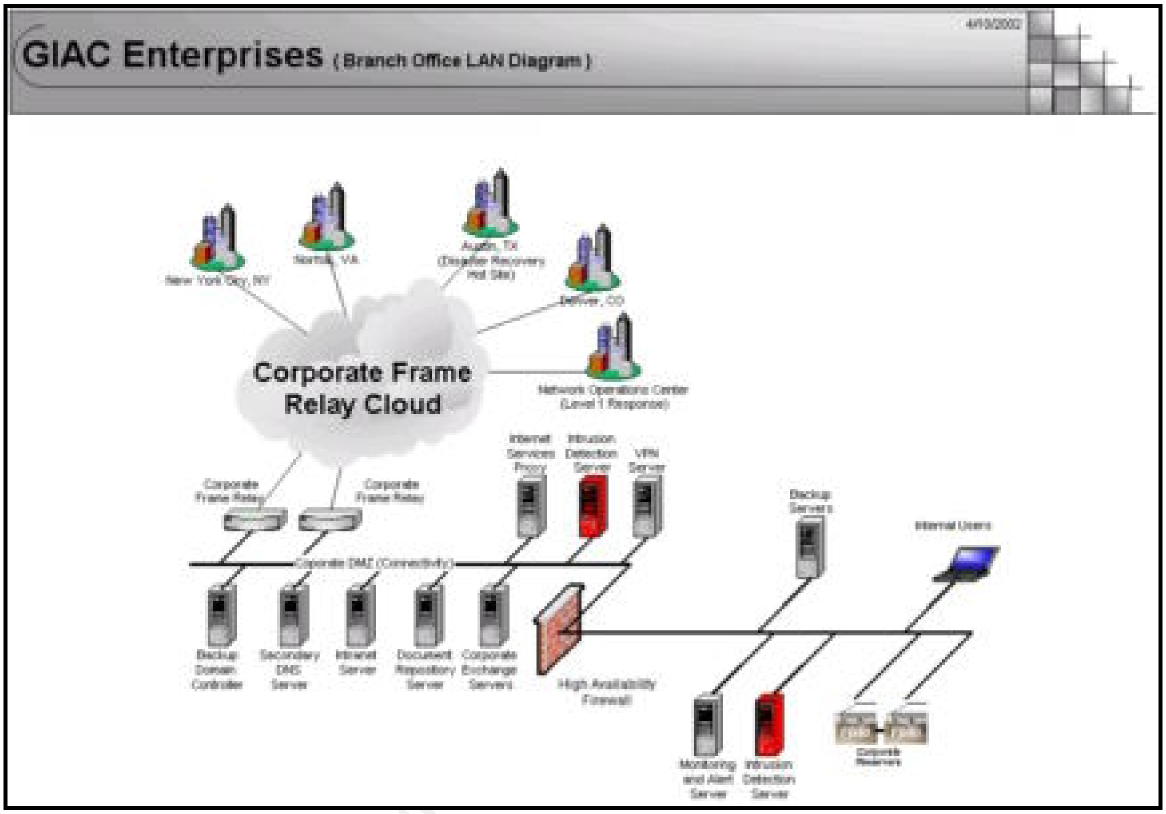
TechTarget, “whatis?com: Part of the TechTarget Network of Enterprise IT Web Sites” URL: http://www.whatis.com/ (March 7th, 2002 ~ May 7th, 2002)

Appendix A: Figures

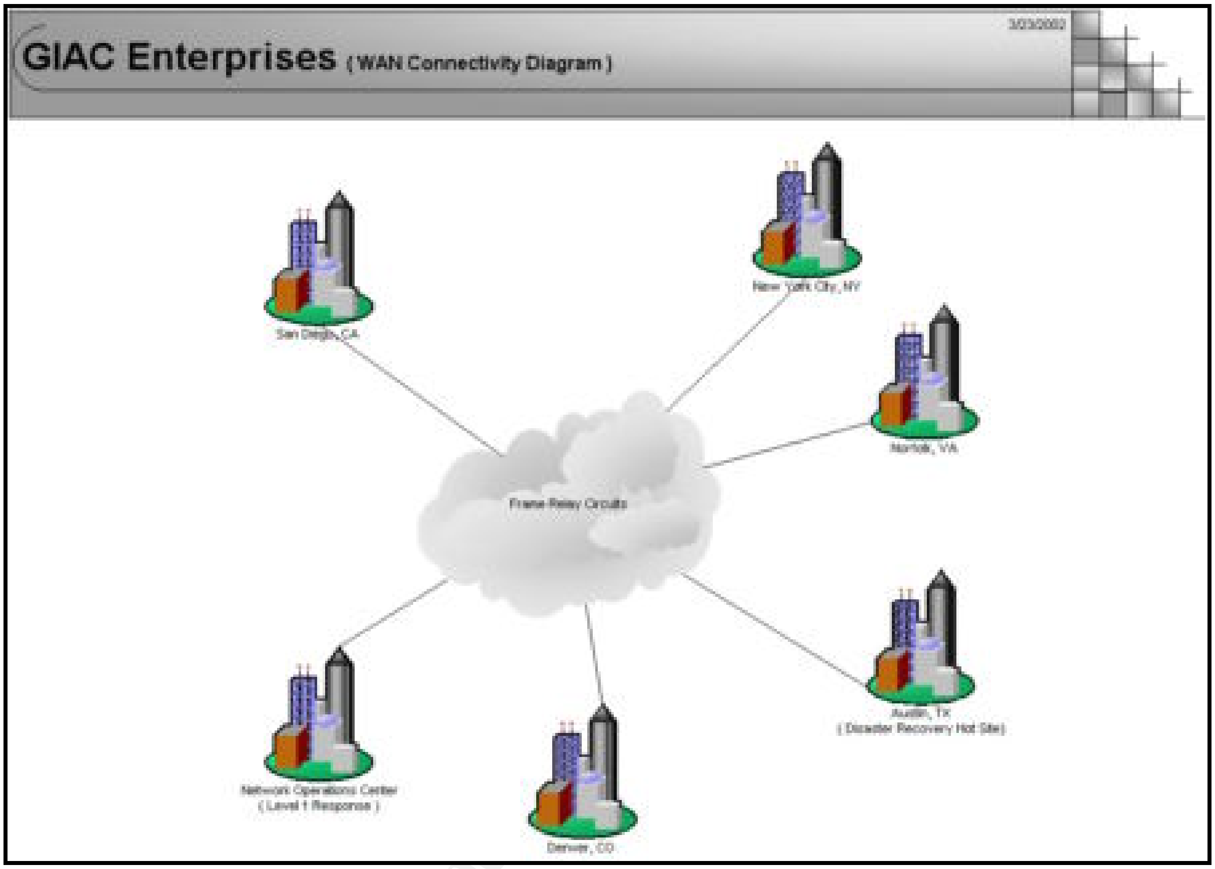
Corporate LAN Diagram


GIAC Enterprises (Corporate LAN Diagram)
4/10/2002
INTERNET
Dual-T1
Dual-T1
Primary Gateway
Primary Gateway
New York City, NY
Norfolk, VA
Austin, TX (Disaster Recovery Hot Site)
Denver, CO
Network Operations Center (Level 1 Response)
Corporate Frame Relay Cloud
Corporate Frame Relay
Corporate Frame Relay
Internet Services Proxy
Intrusion Detection Server
VPN Server
Corporate DMZ (Connectivity)
Primary Domain Controller
Primary DNS Server
Intranet Server
Document Repository Server
Corporate Exchange Servers
High Availability Firewall
High Availability Firewall
Intrusion Detection Server
Backup Servers
Internal Users
Monitoring and Alert Server
Intrusion Detection Server
Corporate Printers
External DMZ (Services)
Email Gateway
Email Gateway
Extranet Services
Extranet Services
VPN Server
Intrusion Detection Server

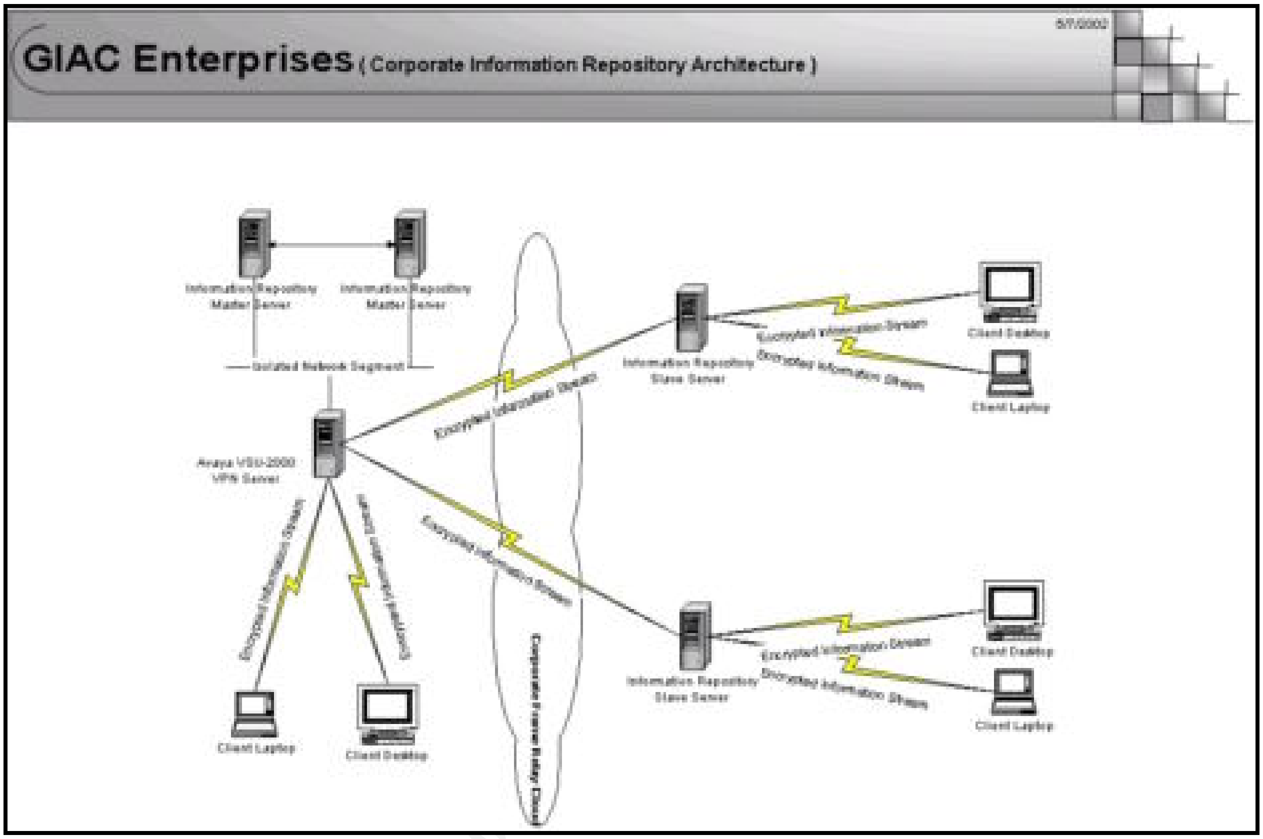
Branch Office LAN Diagram


4/10/2002
GIAC Enterprises (Branch Office LAN Diagram)
New York City, NY
Norfolk, VA
Austin, TX (Disaster Recovery Hot Site)
Denver, CO
Network Operations Center (Level 1 Response)
Corporate Frame Relay Cloud
Corporate Frame Relay
Corporate Frame Relay
Internet Services Proxy
Intrusion Detection Server
VPN Server
Corporate DMZ (Connectivity)
Backup Domain Controller
Secondary DNS Server
Intranet Server
Document Repository Server
Corporate Exchange Servers
High Availability Firewall
Backup Servers
Internal Users
Monitoring and Alert Server
Intrusion Detection Server
Corporate Printers

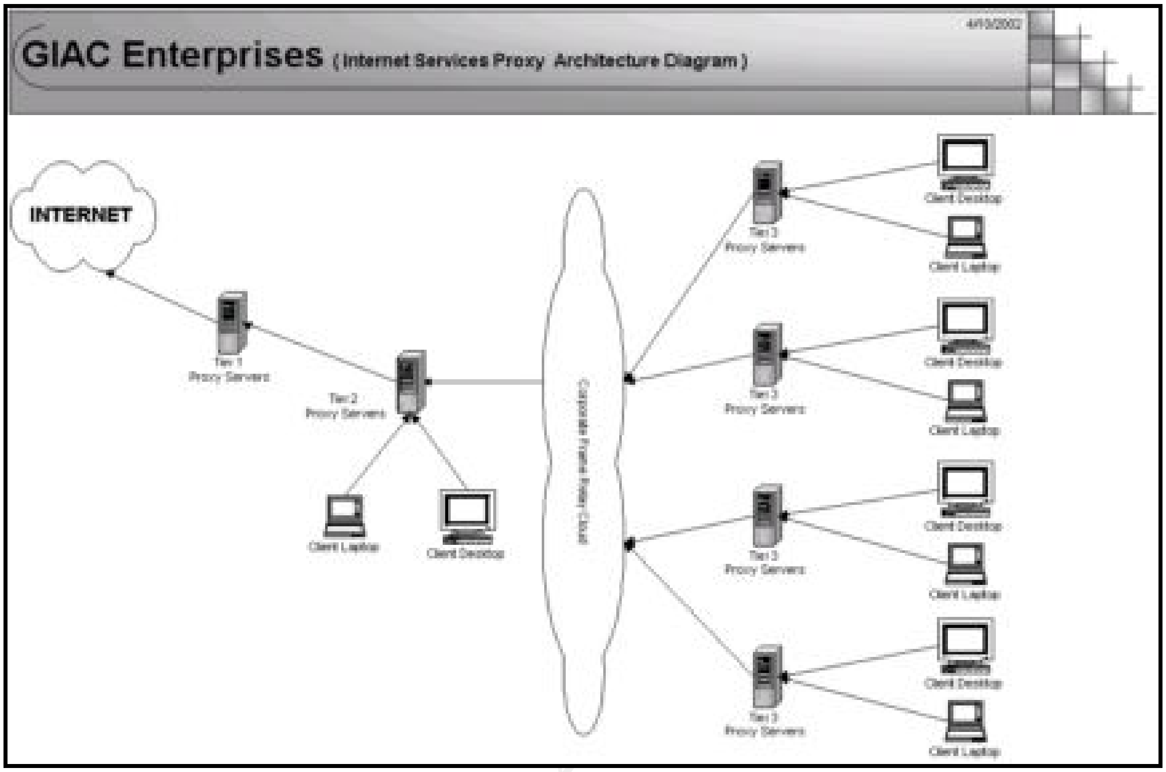
WAN Connectivity Diagram



Corporate Information Repository Architecture


5/7/2002
GIAC Enterprises (Corporate Information Repository Architecture)
Information Repository Master Server
Information Repository Master Server
Isolated Network Segment
Avaya VSU-2000 VPN Server
Encrypted Information Stream
Encrypted Information Stream
Encrypted Information Stream
Encrypted Information Stream
Client Laptop
Client Desktop
Corporate Frame Relay Cloud
Information Repository Slave Server
Encrypted Information Stream
Encrypted Information Stream
Client Desktop
Client Laptop
Information Repository Slave Server
Encrypted Information Stream
Encrypted Information Stream
Client Desktop
Client Laptop

Internet Services Proxy Architecture Diagram



Appendix B: Charts

Corporate LAN – Hardware Chart

Internet Segment

Device	Description	Quantity
Primary Gateway	Cisco 3640 Routers, Cisco IOS, quad-T1 adapters	2
Intrusion Detection System Server	Compaq DL380G2, Redhat Linux, Read-Only File systems on CD (local disk used for temporary storage), No default route, only accessible from Monitoring and Alert Server on Internal Network, SNORT Intrusion Detection Software	1
High Availability Firewall	Sun 420R, Solaris 2.8, Checkpoint Firewall-1, High-Availability with Failover Capability	2

External Demilitarized Zone (DMZ)

Device	Description	Quantity
Email Gateway / Relay	Compaq DL380G2, Redhat Linux, Qmail SMTP Server, SMTP Relay for internal clients only	2
Extranet Services	Compaq DL380G2, Redhat Linux, Apache Web server, OpenSSH Server, Named DNS Server (Primary – Slave), Squid Proxy Server (1st Tier)	2
VPN Server	Avaya VSU-2000[3]	1
Intrusion Detection System Server	Compaq DL380G2, Redhat Linux, Read-Only File systems on CD (local disk used for temporary storage), No default route, only accessible from Monitoring and Alert Server on Internal Network, SNORT Intrusion Detection Software	1

Internal Demilitarized Zone (DMZ)

Device	Description	Quantity
Corporate Frame Relay Gateways	Cisco 3640 Routers, Cisco IOS	2
Intranet Server	Compaq DL380G2, Redhat Linux, Apache Web server, SAMBA Server	2
Corporate Exchange Servers	Compaq DL380G2, Windows 2000 SP2, Microsoft Exchange Server 2000 (mounts the Network Appliance)	2
Primary Domain Controller	Compaq DL380G2, Windows 2000 Server SP2	1
DNS Server	Compaq DL380G2, Redhat Linux, Named DNS Server (Secondary – Master)	1
Internet Services Proxy	Compaq DL380G2, Redhat Linux, Squid Proxy Server (2nd Tier)	2
Intrusion Detection System Server	Compaq DL380G2, Redhat Linux, Read-Only File systems on CD (local disk used for temporary storage), No default route, only accessible from Monitoring and Alert Server on Internal Network, SNORT Intrusion Detection Software	1
VPN Server	Avaya VSU-2000	1

[3] Avaya VSU-2000 is available here.

Document Repository Server	Compaq DL380G2, Redhat Linux, Custom Document Repository Software (mounts the Network Appliance)	2

Internal Networks		
Device	**Description**	**Quantity**
Monitoring and Alert Server	Compaq DL380G2, Redhat Linux, BigBrother Monitoring Software	1
Backup Domain Controller	Compaq DL380G2, Windows 2000 Server, Printer Services	2
Backup Servers	Compaq DL380G2, Windows 2000 Server, External Tape Library, Tivoli Storage Manager (HSM)	2
Intrusion Detection System Server	Compaq DL380G2, Redhat Linux, Read-Only File systems on CD (local disk used for temporary storage), No default route, only accessible from Monitoring and Alert Server on Internal Network, SNORT Intrusion Detection Software	1
Corporate File Servers	Network Appliance F840 (Clustered)	2
User Desktops	Compaq iPaq, Windows 2000 Professional, Microsoft Office	
User Laptops	Dell Inspirion, Windows 2000 Professional, Microsoft Office, Avaya VPN Client Software	

Branch Office LAN Equipment Chart

Internal Demilitarized Zone (DMZ)		
Device	**Description**	**Quantity**
Corporate Frame Relay Gateways	Cisco 3640 Routers, Cisco IOS	2
Intranet Server	Compaq DL380G2, Redhat Linux, Apache Web server, SAMBA Server	1
Corporate Exchange Server	Compaq DL380G2, Windows 2000 SP2, Microsoft Exchange Server 2000 (mounts the Network Appliance)	1
Backup Domain Controller	Compaq DL380G2, Windows 2000 Server SP2	2
DNS Server	Compaq DL380G2, Redhat Linux, Named DNS Server (Secondary – Slave)	1
Internet Services Proxy	Compaq DL380G2, Redhat Linux, Squid Proxy Server (3rd Tier)	1
Intrusion Detection System Server	Compaq DL380G2, Redhat Linux, Read-Only File systems on CD (local disk used for temporary storage), No default route, only accessible from Monitoring and Alert Server on Internal Network, SNORT Intrusion Detection Software	1
VPN Server	Avaya VSU-2000	1
Document Repository Server	Compaq DL380G2, Redhat Linux, Custom Document Repository Software (mounts the Network Appliance)	1

Internal Networks		
Device	**Description**	**Quantity**
Monitoring and Alert Server	Compaq DL380G2, Redhat Linux, BigBrother Monitoring Software	1
Backup Servers	Compaq DL380G2, Windows 2000 Server, External Tape Library, Tivoli Storage Manager (HSM)	1
Intrusion Detection System Server	Compaq DL380G2, Redhat Linux, Read-Only File systems on CD (local disk used for temporary storage), No default route, only accessible from Monitoring and Alert Server on Internal Network, SNORT Intrusion Detection Software	1
Corporate File Servers	Network Appliance F80	1
User Desktops	Compaq iPaq, Windows 2000 Professional, Microsoft Office	
User Laptops	Dell Inspirion, Windows 2000 Professional, Microsoft Office, Avaya VPN Client Software	

Corporate Software Chart

Software List		
Vendor	**Description**	**Function**
Cisco IOS	Cisco Internet Operating System	Routers, Switches
Network Appliance	Data ONTAP Release 6.1.2R3	File Servers
Microsoft	Windows 2000 Professional, Service Pack 2	OS
Microsoft	Windows 2000 Server	OS
Microsoft	Microsoft Exchange Server 2000	Email
Microsoft	Microsoft SQL Server 2000	DB
Microsoft	Office 2000 Professional	Collaboration and Productivity
Big Brother	Big Brother Monitoring Software	Monitoring
Snort	Snort Intrusion Detection System Server	IDS
Qmail	Qmail 1.0.3	SMTP Gateway
Squid	Squid Proxy Server	Proxy Server
Avaya	Avaya VSU-2000	VPN Server
	BIND Version 8.2.3	DNS
Hewlett Packard	HP OpenView	Monitoring and Alert
Tivoli	Tivoli Storage Manager (TSM) 4.1	Backup

Appendix C: Information Control – Proprietary and Private Information Policy

My current employer provides this document. Their name has been changed to protect their interests. All other aspects of this document remain unchanged.

Policy

Information of a private and sensitive business nature shall be controlled and protected so as to preclude arbitrary or careless disclosure.

Purpose

The purpose of this Corporate Policy (CP) is to define the five (5) categories of GIAC-E-controlled information and the means of control required for each category.

Ownership

This CP is the responsibility of the Legal Department.

Limitations

This CP is limited to GIAC-E PROPRIETARY and GIAC-E PRIVATE information as described herein.

Definitions

GIAC-E PROPRIETARY – Information specifically related to GIAC-E-generated concepts, discoveries, techniques, processes, products, and other information which gives GIAC-E an advantage over its competitors who do not know or use such information. Such information is commonly referred to as trade secrets. Examples are: new products, developments, inventions, design drawings, test methods, test results, production drawings and listings of suppliers, technical innovations and supporters.

NOTE: Special care must be taken in the identification of controlled information submitted to the government. The terms or legends which the government will observe vary from those used by GIAC-E or others in non-governmental business. To prevent disclosure, information submitted to the government should be identified as GIAC-E Proprietary.

GIAC-E PROPRIETARY – LIMITED ACCESS – Information that is determined by the responsible control executive to be especially sensitive, and for which tighter controls are required. Examples are: critical process and material specifications, and technical information that is known to be especially valuable to GIAC-E.

GIAC-E PRIVATE – Sensitive administrative information, primarily of a financial or marketing nature. Examples are: proposal data, prices, contractural negotiations, financial records, wage/salary data, and marketing plans. In addition, technical information such as minutes, internal memoranda, and other documents containing sensitive technical data.

GIAC-E PRIVATE – LIMITED DISTRIBUTION – GIAC-E Private information which is determined by the responsible control executive to be especially sensitive, and for which tighter controls are required. Examples are: financial summaries, giving the financial status of the company or any operating unit, and information relating to critical business strategies.

OTHER THAN GIAC-E DATA – Proprietary and private information of other companies, specifically relating to the company's techniques, processes and products. Examples are: customer design drawings, supplier design drawings, engineering data and technical information that is known to be especially valuable and has been accepted on that basis by GIAC-E.

NOTE Proprietary and private information of other companies will be handled and stored in the same manner as similar GIAC-E information, unless other restrictions or conditions have been agreed to by GIAC-E and the other party, or in accordance with proprietary information agreements in effect between GIAC-E and the other party. GIAC-E employees will not accept information which is represented by the other party as proprietary unless an agreement exists, or has first been prepared and approved by the Corporate Law Office, and executed by the parties. Prospective suppliers, associate contractors, contractors or customers who attempt to leave proprietary or private information with a GIAC-E employee shall be asked to sign an Agreement Regarding Unsolicited Non-Proprietary Disclosure unless there is an existing agreement. It is the responsibility of GIAC-E personnel receiving or holding such information to ensure that all authorization receipts are advised of any restrictions or conditions governing its use.

GENERAL

Application

The general types of proprietary and private information covered by this CP include but are not limited to the following:

- Manufacturing methods, techniques, concepts, discoveries and test methods
- Design drawings
- Financial matters
- Proposal data and marketing plans

- o Information of other companies
- o Business relationships, lists of suppliers, associate and subcontractors
- o Exhibits and models

Media

The five categories of controlled information could be conveyed by means of:

5. Written documentation
6. Photographs or slides
7. Motion picture or video tapes
8. Electronic media (includes intranet, disks, mag tape, e-mail)
9. Technical discussions such as meetings, presentations and phone conversations

The technical data disclosed should be limited to that which generally explains any given process or concept and should not disclose such details which would enable a competitor to take advantage of the data (i.e., to form a counter approach or proposal).

Classification of Information

The decision to classify, declassify and control GIAC-E information (including verbal communication, reproduction, distribution, and disposition) shall be made at the following levels:

GIAC-E PROPRIETARY – The originator of the information

GIAC-E PROPRIETARY- LIMITED ACCESS – The manager of the generating department.

GIAC-E PRIVATE – The originator of the information

GIAC-E PRIVATE – LIMITED DISTRIBUTION – The vice president responsible for the generating department

OTHER THAN GIAC-E DATA – The originator of the information

Identification of Controlled Information

GIAC-E-controlled information will be identified by stamping the appropriate category name on both the outside cover and all pages and by including the following statements on the cover and first numbered page, where applicable:

GIAC-E PROPRIETARY – This document contains information which is proprietary to GIAC-E or to one of its customers. Any reproduction, disclosure or use of this information without GIAC-E's written consent is expressly prohibited.

GIAC-E PROPRIETARY- LIMITED ACCESS – This document contains sensitive information which is proprietary to GIAC-E or one of its customers and is not to be copied or disclosed to unauthorized persons. Disclosure to unauthorized persons may result in disciplinary action, including discharge and legal proceedings.

GIAC-E PRIVATE – These documents only require the stamp and do not have any statement following.

GIAC-E PRIVATE – LIMITED DISTRIBUTION – This document is limited in distribution and is not to be copied or disclosed to unauthorized persons. Disclosure to unauthorized persons may result in disciplinary action, including discharge and legal proceedings.

Storage and Handling of Controlled Information

NOTE: Management has the responsibility to insure GIAC-E controlled proprietary and private information is stored properly, and to take disciplinary action when unprotected information is discovered.

The following criteria must be followed in order to ensure proper storage and handling of controlled information.

- Only approved storage containers (safes and filing cabinets) will be used. These containers must be locked during nonworking hours unless the container is in a locked room.
- Safes and files must *be* identified as to the highest category of information contained therein.
- Access to Safes and files will be controlled by regulated keys and combinations and authorized personnel working in area.
- Controlled access areas will be established where feasible.
- Cover sheets noting the category of the controlled information must be on al proprietary information at all times when not in direct working control of an individual.
- Reproduction of subject information must only be done on machines that do not have a memory, i.e., an internal tape or other means that records what is being reproduced.

Storage and Handling of Controlled Information – Electronic

Information Technology and the system owner are responsible during system development to identify and/or update the identification of controlled information and assure necessary security.

Storage and Handling of Controlled Information – Intranet

In addition to the general requirements found elsewhere in this document, controlled information on the Intranet must meet the following criteria.

GIAC-E PROPRIETARY – No additional requirements.

GIAC-E PROPRIETARY- LIMITED ACCESS – Security shall be provided such that (1) the information may not be printed or downloaded by the user; (2) a password shall be required to access the information and (3) access will be monitored and recorded.

GIAC-E PRIVATE – Security shall be provided such that (1) the information may not be printed or downloaded by the user; (2) a password shall be required to access the information and (3) access will be monitored and recorded.

GIAC-E PRIVATE – LIMITED DISTRIBUTION – Information in this category shall not be available on the Intranet.

OTHER THAN GIAC-E DATA – In general, information in this category shall not be available on the Intranet. However, customer production drawings and specifications used in the manufacture of GIAC-E proprietary hardware are treated as GIAC-E Proprietary and are available through the Automated Blueprint Crib (ABC).

Distribution of Controlled Information

Distribution of subject material will be as specified herein. When GIAC-E internal mail system is utilized, the outside envelope must be clearly stamped reflecting the highest category of information contained therein.

When proprietary or private information is transmitted outside GIAC-E, such information must be in a double envelope with the category of information clearly marked on the inner envelope. When appropriate, a nondisclosure statement will be included outside the inner envelope.

Transmittal of GIAC-E Proprietary – Limited Access or GIAC-E Private – Limited Distribution information must be by hand or by registered mail only.

Release of Controlled Information

When proprietary or private information is included in bids, proposals, or in any way issued to companies or agencies for their review, a nondisclosure statement approved by the Corporate Law Office must be included in the bid or proposal.

No proprietary or private information will be released to the public without prior approval of the Corporate Law Office and Corporate Public Affairs.

Destruction Procedure

GIAC-E-controlled proprietary and private information no longer needed will be disposed of in a manner which eliminates the danger of them falling into the hands of unauthorized recipients. For example, this may be accomplished by returning the information to the originator, by shredding, or by depositing in a receptacle dedicated to destruction of proprietary and private data.

PROCEDURE

Not Applicable

REFERENCES

Not Applicable

Index

Glossary

All entries here were defined from http://whatis.techtarget.com/. The links to the definition has been included with each term as well as the definition provided.

A

B

C

Compact Disc

A compact disc [sometimes spelled *disk*] (CD) is a small, portable, round medium made of molded polymer (close in size to the floppy disk) for electronically recording, storing, and playing back audio, video, text, and other information in **digital** form. Tape cartridges and CDs generally replaced the phonograph record for playing back music. At home, CDs have tended to replace the tape cartridge although the latter is still widely used in cars and portable playback devices.

Initially, CDs were read-only, but newer technology allows users to record as well. CDs will probably continue to be popular for music recording and playback. A newer technology, the digital versatile disc (**DVD**), stores much more in the same space and is used for playing back movies.

Some variations of the CD include:

CD-ROM	**CD-i**
CD-RW	**CD-ROM XA**
CD-W	**Photo CD**
Video CD	

D

Demilitarized Zone, DMZ

In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. (The term comes from the geographic buffer zone that was set up between North Korea and South Korea following the UN "police action" in the early 1950s.) A DMZ is an optional and more secure approach to a **firewall** and effectively acts as a **proxy server** as well.

In a typical DMZ configuration for a small company, a separate computer (or **host** in network terms) receives requests from users within the private network for access to Web sites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests on the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested.

Users of the public network outside the company can access only the DMZ host. The DMZ may typically also have the company's Web pages so these could be served to the outside world. However, the DMZ provides access to no other company data. In the event that an outside user penetrated the DMZ host's security, the Web pages might be corrupted but no other company information would be exposed. Cisco, the leading maker of **routers**, is one company that sells products designed for setting up a DMZ.

Denial of Service, DoS

On the Internet, a denial of service (DoS) attack is an incident in which a user or organization is deprived of the services ofa resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. In the worst cases, for example, a Web site accessed by millions of people can occasionally be forced to temporarily cease operation. A denial of service attack can also destroy programming and files in a computer system. Although usually intentional and malicious, a denial of service attack can sometimes happen accidentally. A denial of service attack is a type of security breach to a computer system that does not usually result in the theft of information or other security loss. However, these attacks can cost the target person or company a great deal of time and money.

Common forms of denial of service attacks are:

Buffer Overflow Attacks

The most common kind of DoS attack is simply to send more traffic to a network address than the programmers who planned its data **buffer**s anticipated someone might send. The attacker may be aware that the target system has a weakness that can be exploited or the attacker may simply try the attack in case it might work. A few of the better-known attacks based on the buffer characteristics of a program or system include:

Sending e-mail messages that have attachments with 256-character file names to Netscape and Microsoft mail programs

Sending oversized Internet Control Message Protocol (**ICMP**) **packet**s (this is also known as the Packet Internet or Inter-Network Groper (**ping**) of death)

Sending to a user of the Pine e-mail progam a message with a "From" address larger than 256 characters

SYN Attack

When a session is initiated between the Transport Control Program (**TCP**) client and server in a network, a very small buffer space exists to handle the usually rapid "hand-shaking" exchange of messages that sets up the session. The session-establishing **packet**s include a SYN field that identifies the sequence in the message exchange. An attacker can send a number of connection requests very rapidly and then fail to respond to the reply. This leaves the first **packet** in the buffer so that other, legitimate connection requests can't be accommodated. Although the packet in the buffer is dropped after a certain period of time without a reply, the effect of many of these bogus connection requests is to make it difficult for legitimate requests for a session to get established. In general, this problem depends on the operating system providing correct settings or allowing the network administrator to tune the size of the buffer and the timeout period.

Teardrop Attack

This type of denial of service attack exploits the way that the Internet Protocol (**IP**) requires a packet that is too large for the next router to handle be divided into fragments. The fragment packet identifies an offset to the beginning of the first packet that enables the entire packet to be reassembled by the receiving system. In the teardrop attack, the attacker's IP puts a confusing offset value in the second or later fragment. If the receiving operating system does not have a plan for this situation, it can cause the system to crash.

Smurf Attack

In this attack, the perpetrator sends an IP ping (or "echo my message back to me") request to a receiving site The ping packet specifies that it be broadcast to a number of hosts within the receiving site's local network. The packet also indicates that the request is from another site, the target site that is to receive the denial of service. (Sending a packet with someone else's return address in it is called **spoof**ing the return address.) The result will be lots of ping replies flooding back to the innocent, spoofed host. If the flood is great enough, the spoofed host will no longer be able to receive or distinguish real traffic.

Viruses

Computer **virus**es, which replicate across a network in various ways, can be viewed as denial-of-service attacks where the victim is not usually specifically targetted but simply a host unlucky enough to get the virus. Depending on the particular virus, the denial of service can be hardly noticeable ranging all the way through disastrous.

Physical Infrastructure Attacks

Here, someone may simply snip a fiber optic cable. This kind of attack is usually mitigated by the fact that traffic can sometimes quickly be rerouted.

There are ways of preventing many forms of DoS attacks.

Digital Subscriber Line, DSL

DSL (Digital Subscriber Line) is a technology for bringing high-**bandwidth** information to homes and small businesses over ordinary copper telephone lines. xDSL refers to different variations of DSL, such as ADSL, HDSL, and RADSL. Assuming your home or small business is close enough to a telephone company **central office** that offers DSL service, you may be able to receive data at rates up to 6.1 megabits (millions of bits) per second (of a theoretical 8.448 megabits per second), enabling continuous transmission of motion video, audio, and even 3-D effects. More typically, individual connections will provide from 1.544 **Mbps** to 512 Kbps downstream and about 128 Kbps upstream. A DSL line can carry both data and voice signals and the data part of the line is continuously connected. DSL installations began in 1998 and will continue at a greatly increased pace through the next decade in a number of communities in the U.S. and elsewhere. Compaq, Intel, and Microsoft working with telephone companies have developed a standard and easier-to-install form of ADSL called **G.lite** that is accelerating deployment. DSL is expected to replace **ISDN** in many areas and to compete with the **cable modem** in bringing multimedia and 3-D to homes and small businesses.

Digital Versatile Disc, DVD

DVD (digital versatile disc) is an optical disc technology that is expected to rapidly replace the **CD-ROM** disc (as well as the audio compact disc) over the next few years. The digital versatile disc (DVD) holds 4.7 **gigabyte** of information on one of its two sides, or enough for a 133-minute movie. With two layers on each of its two sides, it will hold up to 17 gigabytes of video, audio, or other information. (Compare this to the current CD-ROM disc of the same physical size, holding 600 **megabyte**. The DVD can hold more than 28 times as much information!)

DVD-Video is the usual name for the DVD format designed for full-length movies and is a box that will work with your television set. DVD-ROM is the name of the player that will (sooner or later) replace your computer's CD-ROM. It will play regular CD-ROM discs as well as DVD-ROM discs. DVD-RAM is the writeable version. DVD-Audio is a player designed to replace your compact disc player.

DVD uses the MPEG-2 file and compression standard. MPEG-2 images have four times the resolution of MPEG-1 images and can be delivered at 60 interlaced fields per second where two fields constitute one image frame. (MPEG-1 can deliver 30 noninterlaced frames per second.) Audio quality on DVD is comparable to that of current audio compact discs.

Domain Name Service, DNS

The domain name system (DNS) is the way that Internet **domain names** are located and translated into **Internet Protocol** addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Because maintaining a central list of domain name/IP address correspondences would be impractical, the lists of domain names and IP addresses are distributed throughout the Internet in a hierarchy of authority. There is probably a DNS server within close geographic proximity to your **access provider** that maps the domain names in your Internet requests or forwards them to other servers in the Internet.

Dynamic Host Configuration Protocol, DHCP

Dynamic Host Configuration Protocol (DHCP) is a communications **protocol** that lets network administrators manage centrally and automate the assignment of Internet Protocol (**IP**) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique **IP address**. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It's especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

DHCP is an alternative to another network IP management protocol, Bootstrap Protocol (**BOOTP**). DHCP is a more advanced protocol, but both configuration management protocols are commonly used. Some organizations use both protocols, but understanding how and when to use them in the same organization is important. Some operating systems, including Windows NT/2000, come with DHCP servers. A DHCP or BOOTP client is a program that is located in (and perhaps downloaded to) each computer so that it can be configured.

E

Electronic Mail, Email

E-mail (electronic mail) is the exchange of computer-stored messages by telecommunication. (Some publications spell it *email*; we prefer the currently more established spelling of *e-mail*.) E-mail messages are usually encoded in **ASCII** text. However, you can also send non-text files, such as graphic images and sound files, as attachments sent in **binary** streams. E-mail was one of the first uses of the Internet and is still the most popular use. A large percentage of the total traffic over the Internet is e-mail. E-mail can also be exchanged between **online service provider** users and in networks other than the Internet, both public and private.

E-mail can be distributed to lists of people as well as to individuals. A shared distribution list can be managed by using an **e-mail reflector**. Some mailing lists allow you to subscribe by sending a request to the mailing list administrator. A mailing list that is administered automatically is called a **list server**.

E-mail is one of the protocols included with the Transport Control Protocol/Internet Protocol (**TCP/IP**) suite of protocols. A popular protocol for sending e-mail is **Simple Mail Transfer Protocol** and a popular protocol for receiving it is **POP3**. Both Netscape and Microsoft include an e-mail utility with their Web browsers.

F

File Transfer Protocol

File Transfer Protocol (FTP), a standard Internet **protocol**, is the simplest way to exchange files between computers on the Internet. Like the Hypertext Transfer Protocol (**HTTP**), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (**SMTP**), which transfers e-mail, FTP is an application protocol that uses the Internet's **TCP/IP** protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their **server** for everyone on the Internet. It's also commonly used to **download** programs and other files to your computer from other servers.

As a user, you can use FTP with a simple command line interface (for example, from the Windows MS-DOS Prompt window) or with a commercial program that offers a graphical user interface. Your Web browser can also make FTP requests to download programs you select from a Web page. Using FTP, you can also update (delete, rename, move, and copy) files at a server. You need to **logon** to an FTP server. However, publicly available files are easily accessed using **anonymous FTP**.

Basic FTP support is usually provided as part of a suite of programs that come with TCP/IP. However, any FTP clientprogram with a graphical user interface usually must be downloaded from the company that makes it.

G

H

I

Information Technology, IT

IT (information technology) is a term that encompasses all forms of technology used to create, store, exchange, and use **information** in its various forms (business data, voice conversations, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived). It's a convenient term for including both telephony and computer technology in the same word. It is the technology that is driving what has often been called "the information revolution."

Intrusion Detection System, IDS

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses *vulnerability assessment* (sometimes referred to as *scanning*), which is a technology developed to assess the security of a computer system or network.

Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

ID systems are being developed in response to the increasing number of attacks on major sites and networks, including those of the Pentagon, the White House, NATO, and the U.S. Defense Department. The safeguarding of security is becoming increasingly difficult, because the possible technologies of attack are becoming ever more sophisticated; at the same time, less technical ability is required for the novice attacker, because proven past methods are easily accessed through the Web.

Typically, an ID system follows a two-step process. The first procedures are host-based and are considered the *passive* component, these include: inspection of the system's configuration files to detect inadvisable settings; inspection of the password files to detect inadvisable passwords; and inspection of other system areas to detect policy violations. The second procedures are network-based and are considered the *active* component: mechanisms are set in place to reenact known methods of attack and to record system responses.

In 1998, ICSA.net, a leading security assurance organization, formed the Intrusion Detection Systems Consortium (IDSC) as an open forum for ID product developers with the aim of disseminating information to the end user and developing industry standards.

Internet

The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers). It was conceived by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 and was first known as the **ARPANET**. The original aim was to create a network that would allow users of a research computer at one university to be able to "talk to" research computers at other universities. A side benefit of ARPANet's design was that, because messages could be routed or rerouted in more than one direction, the network could continue to function even if parts of it were destroyed in the event of a military attack or other disaster.

Today, the Internet is a public, cooperative, and self-sustaining facility accessible to hundreds of millions of people worldwide. Physically, the Internet uses a portion of the total resources of the currently existing public telecommunication networks. Technically, what distinguishes the Internet is its use of a set of protocols called **TCP/IP** (for Transmission Control Protocol/Internet Protocol). Two recent adaptations of Internet technology, the **intranet** and the **extranet**, also make use of the TCP/IP protocol.

For many Internet users, electronic mail (**e-mail**) has practically replaced the Postal Service for short written transactions. Electronic mail is the most widely used application on the Net. You can also carry on live "conversations" with other computer users, using Internet Relay Chat (**IRC**). More recently, Internet telephony hardware and software allows real-time voice conversations.

The most widely used part of the Internet is the **World Wide Web** (often abbreviated "WWW" or called "the Web"). Its outstanding feature is **hypertext**, a method of instant cross-referencing. In most Web sites, certain words or phrases appear in text of a different color than the rest; often this text is also underlined. When you select one of these words or phrases, you will be transferred to the site or page that is relevant to this word or phrase. Sometimes there are buttons, images, or portions of images that are "clickable." If you move the pointer over a spot on a Web site and the pointer changes into a hand, this indicates that you can click and be transferred to another site.

Using the Web, you have access to millions of pages of information. Web browsing is done with a Web **browser**, the most popular of which are Microsoft Internet Explorer and Netscape Navigator. The appearance of a particular Web site may vary slightly depending on the browser you use. Also, later versions of a particular browser are able to render more "bells and whistles" such as animation, virtual reality, sound, and music files, than earlier versions.

J

K

L

Local Area Network, LAN

A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or many as thousands of users (for example, in an FDDI network).

The main local area network technologies are:

- **Ethernet**
- **token ring**
- **ARCNET**
- **FDDI** (Fiber Distributed Data Interface)

Typically, a suite of application programs can be kept on the LAN server. Users who need an application frequently can download it once and then run it from their local hard disk. Users can order printing and other services as needed through applications run on the LAN server. A user can share files with others at the LAN server; read and write access is maintained by a LAN administrator.

A LAN server may also be used as a Web **server** if safeguards are taken to secure internal applications and data from outside access.

M

N

NOC

A network operations center (NOC) is a place from which a telecommunications **network** is supervised, monitored, and maintained. Large **enterprise**s with large networks as well as large network service providers typically have a network operations center, a room containing visualizations of the network or networks that are being monitored, workstations at which the detailed status of the network can be seen, and the necessary software to manage the networks. The network operations center is the focal point for network troubleshooting, software distribution and updating, **router** and **domain name** management, performance monitoring, and coordination with affiliated networks.

O

P

Personal Computer Memory Card International Association, PCMCIA

The PCMCIA (Personal Computer Memory Card International Association) is an industry group organized in 1989 to promote standards for a credit card-size memory or I/O device that would fit into a personal computer, usually a notebook or laptop computer. The PCMCIA 2.1 Standard was published in 1993. As a result, PC users can be assured of standard attachments for any peripheral device that follows the standard. The initial standard and its subsequent releases describe a standard product, the PC Card.

Personal Data Assistant, PDA

PDA (personal digital assistant) is a term for any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business use, often for keeping schedule calendars and address book information handy. The term handheld is a synonym. Many people use the name of one of the popular PDA products as a generic term. These include Hewlett-Packard's Palmtop and 3Com's PalmPilot.

Most PDAs have a small keyboard. Some PDAs have an electronically sensitive pad on which handwritng can be received. Apple's Newton, which has been withdrawn from the market, was the first widely-sold PDA that accepted handwriting. Typical uses include schedule and address book storage and retrieval and note-entering. However, many applications have been written for PDAs. Increasingly, PDAs are combined with telephones and paging systems.

Some PDAs offer a variation of the Microsoft Windows operating system called Windows CE. Other products have their own or another operating system.

Q

Qmail

qmail is a modern SMTP server which makes sendmail obsolete, written by Dan Bernstein, who also has a web page for qmail. qmail is a secure package. You can download qmail 1.03 (Redhat RPMs, Mandrake RPMs, and Debian .debs) and redistribute qmail for free. You can get the "big picture" of how qmail is organized. You should read Life with qmail.

R

RSA

RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. It's also part of Lotus Notes, Intuit's Quicken, and many other products. The encryption system is owned by RSA Security. The company licenses the algorithm technologies and also sells development kits. The technologies are part of existing or proposed Web, Internet, and computing standards.

How the RSA System Works

The mathematical details of the algorithm used in obtaining the public and private keys are available at the RSA Web site. Briefly, the algorithm involves multiplying two large prime numbers (a prime number is a number divisible only by that number and 1) and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key. Once the keys have been developed, the original prime numbers are no longer important and can be discarded. Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet.

The private key is used to decrypt text that has been encrypted with the public key. Thus, if I send you a message, I can find out your public key (but not your private key) from a central administrator and encrypt a message to you using your public key. When you receive it, you decrypt it with your private key. In addition to encrypting messages (which ensures privacy), you can authenticate yourself to me (so I know that it is really you who sent the message) by using your private key to encrypt a digital certificate. When I receive it, I can use your public key to decrypt it. A table might help us remember this.

S

Simple Mail Transport Protocol, SMTP

SMTP (Simple Mail Transfer Protocol) is a **TCP/IP** **protocol** used in sending and receiving e-mail. However, since it's limited in its ability to **queue** messages at the receiving end, it's usually used with one of two other protocols, **POP3** or **Internet Message Access Protocol**, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving messages that have been received for them at their local server. Most mail programs such as Eudora let you specify both an SMTP server and a POP server. On **UNIX**-based systems, **sendmail** is the most widely-used SMTP server for e-mail. A commercial package, Sendmail, includes a POP3 server and also comes in a version for **Windows NT**.

SMTP usually is implemented to operate over **Transmission Control Protocol** **port** 25. The details of SMTP are in **Request for Comments** 821 of the Internet Engineering Task Force (**IETF**). An alternative to SMTP that is widely used in Europe is **X.400**.

SNORT

Snort is an **open source** network **intrusion detection** system (NIDS) created by Norman Roesch. Snort is a **packet** **sniffer** that monitors network traffic in **real time**, scrutinizing each **packet** closely to detect a dangerous **payload** or suspicious anomalies.

Snort is based on *libpcap* (for library packet capture), a tool that is widely used in **TCP/IP** traffic **sniffer**s and analyzers. Through **protocol** analysis and content searching and matching, Snort detects attack methods, including **denial of service**, **buffer overflow**, **CGI** attacks, **stealth** **port** scans, and **SMB** **probe**s. When suspicious behavior is detected, Snort sends a real-time alert to *syslog*, a separate 'alerts' file, or to a **pop-up** window.

NSS Group, a European network security testing organization, tested Snort along with intrusion detection system (IDS) products from 15 major vendors including Cisco, Computer Associates, and Symantec. According to NSS, Snort, which was the sole open source freeware product tested, clearly out-performed the proprietary products.

Squid

SQUID is a program that **cache**s Web and other Internet content in a **UNIX**-based **proxy server** closer to the user than the content-originating site. SQUID is provided as open source software and can be used under the **GNU** license for **Free Software Foundation**.

T

U

V

Virtual Local Area Network (VLAN)

A virtual (or logical) LAN is a local area network with a definition that maps workstations on some other basis than geographic location (for example, by department, type of user, or primary application). The virtual LAN controller can change or add workstations and manage loadbalancing and bandwidth allocation more easily than with a physical picture of the LAN. Network management software keeps track of relating the virtual picture of the local area network with the actual physical picture.

VLANs are considered likely to be used with **campus** environment networks. Among companies likely to provide products with VLAN support are Cisco, Bay Networks, and 3Com.

There is a proposed VLAN standard, **Institute of Electrical and Electronics Engineers** 802.10.

Value Added Reseller (VAR)

In the computer and other industries, a VAR (value-added reseller) is a company that takes an existing product, adds its own "value" usually in the form of a specific application for the product (for example, a special computer application), and resells it as a new product or "package." For example, a VAR might take an operating system such as IBM's **OS/390** with **UNIX** services and, adding its own proprietary UNIX application designed for architects, resell the package to architectural firms. Depending on sales and installation requirements, the VAR could choose whether or not to identify OS/390 as part of the package.

Also see **OEM** (original equipment manufacturer), a company that includes hardware components from other companies in its own product.

Virtual Private Network, VPN

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a **tunneling** **protocol** and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company. The idea of the VPN is to give the company the same capabilities at much lower cost by using the shared public infrastructure rather than a private one. Phone companies have provided secure shared resources for voice messages. A virtual private network makes it possible to have the same secure sharing of public resources for data. Companies today are looking at using a private virtual network for both **extranet**s and wide-area **intranet**s.

Using a virtual private network involves encrypting data before sending it through the public network and decrypting it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. Microsoft, 3Com, and several other companies have developed the Point-to-Point Tunneling Protocol (**PPTP**) and Microsoft has extended **Windows NT** to support it. VPN software is typically installed as part of a company's **firewall** server.

W

Wide Area Network, WAN

A wide area network (**WAN**) is a geographically dispersed telecommunications **network**. The term distinguishes a broader telecommunication structure from a local area network (). A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks. An intermediate form of network in terms of geography is a metropolitan area network (**MAN**).

Wireless Equivalent Privacy, WEP

Wired Equivalent Privacy (WEP) is a security protocol, specified in the **IEEE** Wireless Fidelity (Wi-Fi) standard, **802.11**b, that is designed to provide a wireless local area network (**WLAN**) with a level of security and privacy comparable to what is usually expected of a wired LAN. A wired local area network (**LAN**) is generally protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but may be ineffective for WLANs because radio waves are not necessarily bound by the walls containing the network. WEP seeks to establish similar protection to that offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. Data **encryption** protects the vulnerable wireless link between **client**s and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (**VPN**s), and **authentication** can be put in place to ensure privacy.

A research group from the University of California at Berkeley recently published a report citing "major security flaws" in WEP that left WLANs using the protocol vulnerable to attacks (called *wireless equivalent privacy attacks*). In the course of the group's examination of the technology, they were able to intercept and modify transmissions and gain access to restricted networks. The Wireless Ethernet Compatibility Alliance (WECA) claims that WEP - which is included in many networking products - was never intended to be the sole security mechanism for a WLAN, and that, in conjunction with traditional security practices, it is very effective.