

Canaudit Perspective

December 2003
Volume 4, Issue 12

Points of Interest:

- Building Strong Network Security
- Securing the Databases
- Securing the Operation Systems
- External Security
- Securing the Applications
- Upcoming Professional Development Weeks

Achieving Your Security Objectives



Recently, I received multiple requests for my views on information security. While I often write and teach on many security issues, several clients requested that I describe the components of a security IT environment to enable them to plan their security reviews and audits for the coming year. I believe that Information security is an ever-illusive goal, much like the search for the Holy Grail. No matter how hard you work, no matter how much you spend, perfect security can never be achieved. That said, there is much we can do to protect the IT environment, critical software and, of course, important data.

When I look at security, I break it down into seven components, which I call the seven cornerstones of basic security:

- Network security
- Database security
- Operating system security
- External security
- Application security
- Physical security
- Business continuance and disaster preparedness

Building Strong Network Security

Let's start with network security. I break this down into the internal network and external security. I'll cover the internal network first since recent statistics demonstrate that most network security events originate from the internal network. Since the only secure network is one that has no users, you can bet that there will be a major network incident one or more times a year. Given that, the most important control is to segment the network. This is achieved by implementing access control lists on existing routers or switches, or by installing internal firewalls.

A thorough analysis must be performed to identify sensitive information assets prior to segmenting the network. Once this is done, it is a simple matter to cluster related assets together so that they can be properly protected. One cluster might be the machine that enables wire transfer or electronic payments. I would expect these to be in the most secure network segment, protected by one or more firewalls, as well as router or switch access controls lists.

Depending on the circumstances, I might cluster several important assets into a single network segment so that they can be cost-effectively protected. For instance, I would place the human resources and payroll, mergers and acquisitions, legal services, and possibly internal audit into a firewall protected network segment. I would then use access control lists to protect each resource in the segment from other resources in the segment.

The largest network segment, the main network, should contain the core business assets that are shared by others. This might include items in the sales-to-cash and purchasing-to-fulfillment cycles, banking or claims, or policy and claims management, depending on the business. Where possible, access control lists should be used to restrict access within the segment.

After network segmentation, my next control is intrusion prevention and detection software. Many vendors provide a variety of intrusion detection software (IDS), which is used to detect a successful network penetration. I believe that IDS is comparable to closing the barn door after the horse has been stolen. I prefer that Intrusion Prevention Software (IPS) be implemented as the first line of defense, with IDS as the second line of defense. Prevention should always be first; then, detection should be the secondary control.

In addition to IPS and IDS, I like to use a series of honey pots in the network to detect insiders who are "exploring" the network. Honey pots are quite useful in catching hackers, as hackers tend to go for the low hanging fruit, the weakest machines. By carefully placing honey pots throughout the network, I will know when someone attempts to compromise security.

All network devices should be up to patch level. This sounds easy; however, with the plethora of network devices (routers, switches, hubs, wireless access points, firewalls, multiplexers, etc.), this is not an easy task. A multiple vendor environment complicates patch and version management; therefore, strong procedures are required to ensure that all network gear is at the current vendor release level.

If you would like more information on network controls, you can attend my seminar on Control and Security of Telecommunications Networks or purchase my book. If this is not possible, then send me an opt-in email to gordon@canaudit.com by January 15, 2004, and I will send you an electronic copy of my network security and audit guide.

Securing the Databases

Database security is my next line of defense. While others place operating system security first, I place a higher priority on database security, as it is sorely lacking in most organizations I audit. Database security is normally a part-time job of a database administrator. This places the administrator in a conflict of interest, as their primary function is to facilitate access. By saddling them with the security function, they are also responsible for restricting access. This creates a conflict that usually results in poorly protected databases, as they cannot effectively grant and restrict access at the same time.

The biggest threat to database security, in my mind, is access accounts. These are very powerful DBA accounts. This is prevalent in the Oracle / PeopleSoft environments. Users log into the application with a normal operator account and password. They use the various application panels to enter the required information. The database access account is used by the application to log into Oracle and update the database. The password to the access account is seldom changed and is often the same one the integrators used when implementing the application. Changing the access password frequently is a critical, yet often ignored, control.

Next on my database hit list is DBA access. Account authentication using a password is simply not effective given the tools available to a hacker. I strongly urge each of you to require secondary authentication using tokens (SecurID, etc), digital certificates, or biometrics for all DBA accounts. In addition, these techniques should be required for all users with access to sensitive information or who perform critical functions.

Access restrictions also need to be revamped. Usually there is a large number of individuals with DBA and SYSDBA access. In just about every database security review I perform, I find that DBA access is too widely distributed. Remove access from those who do not truly require it on a day-to-day basis. I recognize that occasional DBA access may be required. When it is, have a procedure to grant DBA access on an emergency basis.

Access restrictions also have to be tightened at the user level. When I look at menu, view, and panel security, I often find that most users have far more access than they need to perform their function. As an example, let us look at banking. Who has access to your account balance? The answer is every teller in every branch, loan offices, branch supervisory staff, customer service representatives, auditors, and investment services personal. A simple control would be to require the user to swipe their ATM card before the information is available to the bank staff member.

Before a telephone CSR could view your information, you would have to provide your account number or ATM number, then answer a challenge question such as password, favorite object, etc (not mothers maiden name or last four digits of the Social Security Number). If the answer to the challenge is correct, the CSR could view your data. Strong view and menu restrictions are required to limit the information available to staff. In addition, periodic database access reviews should be conducted to ensure that terminated employees no longer have access and that the view and menu access for all users is properly restricted.

Do not forget to secure your exports and backup files. In our penetration audits, we usually find that the databases themselves are protected from direct access by a normal user. Unfortunately, the export or backups are usually world readable. This enables a hacker to download the export copy then import it into a database where they have DBA access. As a result, the data can be readily compromised.

Securing the Operating Systems

Operating system security is the third cornerstone of information security. Our penetration audits reveal that the Windows operating system is the easiest to penetrate. Failure to properly secure workstations, accounts without passwords, and missing patches make Windows the preferred target. NetBIOS is fraught with security issues. By upgrading all Windows operating systems to Windows 2000, XP, or Windows 2003 Server, NetBIOS can be eliminated.

The next machine that is relatively easy to penetrate is the mainframe. Quite frankly, there is an over-reliance on the RACF, ACF2, and Top Secret security tools. Another factor is that many of the people who truly understand OS/390 and Z/OS are retiring. Our approach in a penetration audit is to crack Windows accounts and passwords first. We hold off on attacking the mainframe until an hour before the exit interview. Using a free tool called Brutus (available on the Canaudit Website), we automate a password attack against the mainframe FTP port with all of the cracked accounts and passwords. We usually crack 20 or 30 passwords within the first five minutes.

We then log into TSO using the compromised accounts and run our proprietary password cracker from a normal user account. We also search for, and normally find, a poorly secured library. Eldon Quast, our mainframe security analyst, normally has operaudit capability by the time we start the exit interview. Most of our clients are not monitoring the FTP port carefully. In the mainframe environment, the secret is to ensure that all libraries are properly secured, as well as all members of critical libraries.

Mainframe security auditing is a dying art. It has been many years since most of our clients have performed a proper, technical mainframe security review. Well, the mainframe has not gone away as many thought it would. In fact, mainframes are coming back into vogue as clients realize the labor and costs in managing and securing a dispersed server environment. Clearly, a mainframe security review should be on your radar in 2004. Email me if you would like Canaudit to assist you with this review.

UNIX and Linux operating systems also have many vulnerabilities. Some, such as the Sun integer overflow, can give a hacker unauthenticated access to the machine; in some cases, root access. You must keep up on all security bulletins for the UNIX and LINUX versions installed in your organization.

All operating systems need to be hardened to ensure that they remain secure. Patches should be applied quickly and universally. Accounts should be reviewed to ensure that they all have complex passwords (alpha, numeric, and special characters) and that every account has a password.

Secondary authentication should be used on all accounts (tokens, biometrics, and digital certificates). The majority of our clients do not want to incur the cost of these measures and they are severely exposed because of the extended use of an outdated control, the password. If your organization is not ready to accept secondary authentication techniques for all users, then implement it selectively. All administrators should be authenticated using the token, or biometrics.

External Security

External security is next on my hit list. Most of my clients believe they are secure if they have a firewall and restrict modems. These controls only cover a small fraction of the total external risk. In addition to internet and modem attacks, your organization may be attacked from trading partner networks that connect to your network. In a recent client visit, I asked a simple question and found that it could not be answered. **WHO CONNECTS TO YOUR NETWORK?** No one had a list. Within about 30 minutes, we identified about 20 trading partners that have a direct connection to the network. We expect that there may be 10 to 20 more. In many cases, these connections are not monitored, and, in some cases, they bypass the firewall. Trading partners are often trusted, and, once in the network, they may be able to freely roam the internal network.

I am also concerned about the number of Virtual Private Networks (VPN) that are poorly secured. VPNs are useful in permitting remote users to access the network using an encrypted and secure communications path. Unfortunately, account and password authentication is used by most of our clients instead of secondary authentication, as mentioned previously in this article.

When you question the VPN administrator, they often say that each VPN user must have a software client on their machine to enable them to connect. While this is true, it is also true that many of the clients can normally be freely downloaded from the VPN vendors' web site, negating the effectiveness of this control.

On VPNs, which do use proper secondary authentication, we often find several accounts that are permitted to connect to the internal network without using secondary authentication. When questioned, the administrators usually state that they need these accounts in case the authentication server fails and they need to log into fix it. Some things should not be fixed from home. If the authentication server fails, I think someone should go into the facility, find out what is wrong, and fix it. These "emergency" accounts, which do not require secondary authentication, are a ticking time bomb. We have special techniques for identifying and compromising these accounts during our penetration audits. If we can do it, then it is only a matter of time until hackers will guess the account password combination and use them to penetrate the network.

My next concern with external threats are wireless connections. I am constantly amazed to find customers with unsecured or very poorly secured wireless connectivity. We literally sit in the parking lot and access the internal network. Wireless Equivalent Protocol, which some clients use to "secure" wireless communications, is easily cracked using WEPcrack or AirSnort. These tools are available free on the internet. I strongly suggest that you use Cisco Leap and RADIUS or other tools to secure your wireless connections.

Once your authorized wireless connections are secured, the rogue user who sets up their own unofficial wireless access point poses a significant risk. Again, I strongly recommend that you perform regular wireless sweeps on a surprise basis to identify and eradicate unsecured or rogue wireless connections to your network.

Poorly secured modems continue to be a serious exposure. When our penetration team performs a war dial, we invariably find poorly secured modems that give us access to the internal network or critical business assets. To properly secure modems, you will need to identify all inbound analog circuits. Do not forget to include central office (CO) lines in your list. These lines bypass the PBX.

Our penetration team uses a tool called PhoneSweep from SandStorm Industries to perform a modem hunt (war dial). We find that this tool is both safe and effective. You should use this or a similar tool to perform periodic surprise modem hunts. Unauthorized modems, like unauthorized wireless, can place your network at great risk.

Many of our clients think they are safe because they have a firewall. In my books and classes, I demonstrate just how easy it is to bypass a firewall. Our penetration team is often successful in obtaining Internet access to a firewall-protected client network. We believe that each of our clients should have a quarterly surprise external penetration test. In the course of updating the network or the firewall, it is possible that holes could be created in your external security. In addition to the quarterly tests, all clients should have an annual surprise penetration test.

Securing the Applications

Application security is a critical cornerstone of a total security philosophy. User access should be limited using the rule of least access. Each transaction should be analyzed to determine who needs access to the transaction and the level of access they should have (read, update, delete, etc).

Process protocols should also be reviewed to ensure that application triggers are used to detect unusual items. In most of our audits, we find that triggers are underutilized. This results in a failure to automatically detect unusual items, as well as potentially fraudulent transactions. In addition, the failure to use triggers increases the work factor of the application. Manual reviews are not only inefficient, but often are ineffective as suspect transactions may fall through the cracks.

Do not forget to review the routings to ensure that there are no unnecessary routings and that the correct level of transaction review is in place. Most ERP systems use electronic transaction routing. This ensures that the transactions are moved through the process quickly. While unnecessary routings can cause excessive delay, condensing routings may result in a failure to properly review and scrutinize transactions.

While passwords may be passé as a control, when passwords are used, there are often accounts with no passwords or accounts with default passwords. These items can easily result in application data being compromised, altered, or harvested by electronic espionage specialists. Many of our clients do not purge user accounts as quickly as they should. In a recent review, we found that there were over 12,000 user accounts active in the application; yet, the client had only 3,500 staff! Not only were employee accounts not purged upon termination or transferred to another division, but all of the accounts for temporary staff brought in for the conversion were still active after three years. Worse still, the integrators still had powerful accounts that enabled them to access the application remotely, even though it was over two years since the last consultant worked on the application.

Physical Security is a Must

Physical security is still a very important part of the total security package. While hackers may be able to defeat your firewall, server, and application security from afar, it is more likely that a determined person could social engineer his or her way into your building. In every physical security test we have performed, we have defeated the controls and gained access to facilities and secure areas within facilities. Card access systems are easily defeated by creating a fake access badge, then piggy backing in behind a "smoker" after lingering in the "Butt Hut" (the area outside the building where the smokers congregate).

Other tricks, such as finding a modem on the access control computer to unlock doors after hours, are also very effective. One of my favorites is to call a regional office in a smaller town using the name of the network administrator or web master in the domain registration. This public document can be viewed by anyone. I like to use time zones to my advantage when I do this. If the head office is in California, I will call the network administrator or webmaster at 5:30 am (Pacific Time zone) to ensure that I get his or her voicemail. Then, I will call the local office in Newark (Eastern Time zone), and say that we need to perform a network loopback test to ensure that the new routers, which we spent all night installing, are working properly. We then let the regional facilities person know that John Doe will be arriving in 45 minutes to perform the test. If access to the network area is not available, he can perform the test from any conference room that has an active network connection. This is a simple, yet effective, way to get internal network access by breaching physical security.

It is very important that you perform a full physical security audit annually. In addition, you should perform several social engineering tests a year on a surprise basis. This will keep your staff on their toes so that physical security breaches can be minimized.

Business Continuity and Disaster Preparedness

The last security corner stone is business continuity and disaster preparedness. I am a strong believer in business continuity. Using several data centers with fully integrated server and application redundancy, your organization can survive most disasters and, like the energizer bunny, keep on going. Not only should there be redundant servers, but distributed databases are necessary, not only for business continuity, but also for improving transaction processing response.

Do not forget to build redundancy into the Extranet. You definitely need multiple firewalls, but multiple ISPs with completely separate access paths are also essential. Ensure that your business continuance plan is well documented and is tested frequently. To be effective, it should be stored offsite and copies should be distributed to key employees to keep in a secure location at home. No point having a great disaster plan stored in the burning building. It will go up in smoke like everything else.

Conclusion

Information security needs to be maintained and monitored. We believe that information security and client support staff should ensure that basic housekeeping is performed to ensure that hackers will not be able to use "low hanging fruit" to easily defeat your security. Our penetration audits are very successful because clients lack basic security. Examples include the following:

- Ensure all machines are at the current patch level.
- Ensure all accounts have complex passwords.
- Ensure that local security settings are in place on workstations and that all local workstation accounts have passwords.
- Reduce the number of domain administrator or root account access to the absolute minimum (this is normally the square root of the number of administrator root accounts that are "absolutely required").
- Permit accounts with restricted administrator rights for support and account maintenance.
- Ensure that all administrator or root accounts require secondary authentication.
- Eliminate the use of the NetBIOS ports or remove the ability to connect through null sessions in the Windows environment.
- Review and secure all remote access.
- Document all trading partner access, and ensure that all access is properly authenticated, including the use of digital certificates or other secondary authentication techniques.
- Conduct regular security reviews of all servers and several surprise penetration tests each year.
- Review the articles on the Canaudit website (www.canaudit.com) for more detailed information.

In addition to the above, your internal audit department should have a strong IT audit review schedule. This program should ensure that general controls are audited annually. In addition, there should be a full network audit at least once every three years. UNIX and Windows audits should be conducted every two or three years. In addition, new servers should be audited before they are placed into production to ensure that they are secure and that the application is controlled. External firms, such as Canaudit, should be used on a regular basis to perform penetration and mainframe audits. There should be one full penetration audit each year with quarterly Internet and modem penetration tests to ensure that controls remain in place between penetration audits.

In closing, I would like to thank each of you for supporting Canaudit. This year has been a record year of growth for us, both in staff and in revenues. As we move into the New Year, I would like to offer more than just a thank you; I would like to give you an opportunity to attend our upcoming Classes in San Diego and San Francisco at half price. This includes our IT AUDIT AND SECURITY BOOT CAMP and the ULTIMATE NETWORK PENETRATION classes in San Diego, as well as the PROFESSIONAL DEVELOPMENT WEEK in San Francisco. To qualify for the discount, you must register and pay for the classes by December 31, 2003.

I wish each of you a successful and safe New Year. As always, the opinions in this article are mine and mine alone. Please send any comments you may have to gordon@canaudit.com. I look forward to hearing from you.

[Register](#) for the Professional Development Week February 2-5, 2004 in San Francisco, CA.

[Register](#) for the IT Audit & Security Boot Camp or the Ultimate Network Penetration Class March 1-5, 2004 in San Diego, CA.

For more information please contact Jennifer Hoffman at 805-583-3723 or jennifer@canaudit.com



Mr. Smith is listed in the WHO'S WHO OF LEADING AMERICAN EXECUTIVES and has published 2 books titled [Network Auditing: A Control Assessment Approach](#) and [Control & Security of E-Commerce](#), both published by John Wiley and Sons.

A handwritten signature in black ink that reads 'Gordon Smith'.

Gordon Smith
President, CEO

Please feel free to forward this article to your co-workers.

In accordance with CA state laws, as of January 1, 2004 we must have a record that you opted-in to our mail list. If you would like to receive future Canaudit articles please select the opt-in option below.

[Opt-in](#) to our mail list
[Opt-out](#) of our mail list

Happy Holidays!