

The Canaudit Perspective

Volume 4 - Issue 6
(part 1)
June 2003

Special points of interest:

- [Identity theft](#)
- [Entry points into the network](#)
- [Securing your confidential data](#)
- [Part 2 of the Canaudit Perspective](#)
- [Learn more at our Boot Camp](#)
- [Upcoming events](#)



Protecting your customers, protecting your data.

Identity theft is a booming and growing business with plenty of customers willing to pay to become someone else. Recently, we have seen several news stories about hackers breaking into systems and taking personal information. This information can be used to obtain credit cards and loans. It can also be used to assume someone else's identity. A person with a criminal record or an illegal immigrant may want a new identity so that they can get a decent job. A terrorist may want a passport so that they can enter the country. An estranged parent may want a new identity to avoid paying alimony or support, similar to debtors who may want to avoid paying their obligations. Whatever the reason for the new identity, there is a large market waiting to be filled. With this type of demand, it is no wonder that hackers are constantly probing networks looking for weaknesses. When they find poorly secured systems, they exploit them in the hope that they can penetrate the defenses and reach their goal, the personal information of your customers, clients and/or business partners.

A common misconception is that this data is "stolen" from the Internet, making many people fearful of using the Internet. In fact, most electronic identity theft or the theft of financial information is not through the Internet. Rather it is usually taken from servers on the inside of the network where it is often stored unencrypted. Once on a server, hackers or your own employees seeking additional income can harvest data at will, normally without detection.

In [previous articles](#), we have emphasized the need for strong firewalls and controls over the Extranet. In this article, I want to make the assumption that the network will be breached at some point in time. When this occurs (not if it occurs), multiple defenses are necessary to protect your data and program files.

Entry points into the network. The first and most understood is from the Internet. Here, the control is a strong defense consisting of several firewalls, intrusion detection software and honey pots to attract the successful hackers. This will increase the likelihood of early detection. Another popular way to beat the network is through wireless access points. Here the control is to use Cisco leap and RADIUS technology to create a secure, encrypted tunnel for your data. Also, ensure to test for rogue access points on a regular basis. These items have been covered in past articles, so I won't expand on them here. In this article, I would like to build the defenses from the inside out, rather than the traditional outside in methodology.

Let's start this process with the most critical item you want to secure, **your confidential data**. Your data should be classified to determine whether it is public, confidential or private. I define public data as data that could be printed on the front page of the Wall Street journal and the CEO would not be upset. Confidential data is data that should be protected from general distribution. This may include

customer information, medical records, production data, or pricing information. Federal and state laws such as HIPAA, mandate that personal data be protected. The first way to protect it is to encrypt it when it is transmitted and when it is stored. Most of our clients understand the need for encryption during transmission, however most think that encrypting stored data is going too far. Also the cost of encrypting data is higher than not encrypting it. I believe that in a decade or so, data encryption will be commonplace. In the meantime, you may not want to fight the encryption battle in your organization.

So what can we do **if encryption is not an option?** Well, the first thing is to ensure that all databases and files are protected. Access permissions are generally available on your servers. These permissions break down one way or another in to three basic groups. The first is the owner of the data, who can usually read, write, alter, delete or execute the files. Users are often placed into groups and are able to access information available to that group. Normally this access would be restricted to the ability to read the data or execute the programs. In some cases, the group may need to write, alter or delete the data or records within the data. The third set of users is what "everyone" or the "world" can do. These are people with a normal user or guest account on the system, who are not granted access by virtue of being the owner or a manager of a group. Everyone who accesses a system should only be able to read public data. They should not have the right to alter, delete or write to the data. If data is properly protected, then when the server is compromised with a normal user account, the damage will be limited to the access that the user has. By ensuring that non-public databases and files are not world readable, we are defeating the hacker or unauthorized employee or contractor's ability to easily steal information.

Right about now, I suspect that you are wondering how to determine if data is properly protected. This depends on the operating system, which in many cases is UNIX based. In the UNIX world, we run a simple command from the root directory (`ls -alBRF >/tmp/outputfile.txt`). This produces a list of all of the file permissions. We load this into a Microsoft Access database, and then run some preformatted queries. Two of these provide us with a list of the world readable and world writeable files as well as a count for world readable and writeable files. These are the files that can be harvested by a hacker or unauthorized employee, or in the case or worlds writable, altered and changed using a normal account.

Using another query, we seek out the database files and the database backups (usually called exports). In most cases, the exports are world readable. Since we now know the location of this file, we can easily download it just as a hacker would. All we have to do now is import the exported database into our own database and your data, including identity related information, is our data.

There are two simple things you can do to **prevent hackers** from stealing the database in this manner. The first is to ensure that the owner or the database administrator group can only access the database export. There should be no world access at all. This will protect the export. To reduce the number of world readable files, set the umask (a parameter that defines the default file permissions when a file is created) to 027. Now when files are created, they will be better protected. *continued...[part 2](#)*

If you would like to learn more about how to protect your data including your customer and client information the Canaudit IT Audit and Security Boot Camp is a five-day workshop that covers all the items in this article in greater depth. There are over 1300 pages of material as well as several hands on exercises. This workshop will provide you with the concepts, tools and methodologies you need. We are holding public classes for this course in Fairfax, VA July 21-25, 2003 and Minneapolis, MN October 6-10, 2003. We look forward to seeing you there. For any questions or to register please contact Jennifer@canaudit.com or 805-583-3723 or visit us at www.canaudit.com

[Click here for part 2 of the June 2003 Canaudit Perspective](#)

Topics will include:

- Gordies top sixteen things to do to protect the UNIX operating system
- Network Segmentation

This article is based on our new seminar Control and Security of Enterprise Wide E-Commerce. An expanded version will be available in my new book, Control and Security of E-Commerce, which is currently in the process of being published by John Wiley and Sons. IT will include a full set of Risk / control tables and audit checklists to assist you with your audit or security review. When you attend one of my Canaudit or Chapter events, I will be pleased to dedicate and sign your copy of this book if you bring it to the class.

Best regards, Gord

UPCOMING EVENTS

It's time to register for one of Canaudit's public classes

**The Ultimate Network Penetration Class
(5-day)**

[Lake Tahoe, CA - September 15-19,2003](#)

**IT Audit & Security Boot Camp
(5-day)**

[Fairfax, VA – July 21-25, 2003](#)
[Minneapolis, MN – October 6-10, 2003](#)

Professional Development Weeks:

Simi Valley, CA - August 11-14, 2003

- [Understanding & Preventing Electronic Fraud](#)
- [Control & Security of Telecommunication Networks](#)
 - [Control & Security of Web Applications](#)
 - [Cyberterrorism and Electronic Espionage](#)
- [Computer Forensics For Security and Audit Professionals](#)
 - [Control & Security of Wireless Networks](#)

Minneapolis, MN – October 6-10, 2003

- [Control & Security of Windows 2000](#)
- [Control & Security of Wireless Networks](#)
 - [Control & Security of Unix](#)
 - [Control & Security of the Internet](#)
- [IT Audit & Security Boot Camp](#)



Canaudit, Inc.
AUDITS • SEMINARS • CONSULTING

P.O. Box 2110 – Simi Valley – California – 93062-2110 - Phone: 805-583-3723 Fax: 805-582-2676 www.canaudit.com