Introduction to Intrusion Protection and Network Security

Jennifer Vesperman

jenn@linuxchix.org

Megan Golding

meggolding@yahoo.com

2002-02-24

Revision History

Revision 0.1 2002-02-17 Revised by: MEG
Converted from text file. Modified wording.
Revision 0.2 2002-02-23 Revised by: MEG
Incorporated Jenn's suggestions.
Revision 0.3 2002-02-24 Revised by: MEG
Conforming to LDP standards. Added abstract.

In this introduction to protecting your computers from intrusion, the author discusses concepts of computer security. Selecting good passwords, using firewalls, and other security concepts are introduced.

1. Introduction

1.1. Copyright Information

1.2. Overview

If your computer is not connected to any other computers and doesn't have a modem, the only way anyone can access your computer's information is by physically coming to the computer and sitting at it. So securing the room it's in will secure the computer[1]. As soon as your computer is connected to another computer you add the possibility that someone using the other computer can access your computer's information.

If your network (your connected computers) consists only of other computers in the same building you can still secure the network by securing the rooms the computers are in. An example of this would be two computers sharing the same files and printer, but not having a modem and not being connected to any other computers.

However, it's wise to learn about other ways to secure a network of connected computers, in case you add something later. Networks have a tendency to grow. If you have a network, an intruder who gains access to one computer has at least some access to all of them.

2. The Locked Front Door

As soon as your network connects to somewhere outside your building, you need the virtual equivalent of a locked front door. If you don't have that, all the information you have on your computers is vulnerable to anyone who wants to gain access.

Like real doors, virtual doors come in a wide variety of types, security levels, and expense.

The simplest, but not the safest, way to secure your network is to keep 'moving' - if you're connected to the internet through a modem and have a 'dynamic IP address' (ask your service provider), your address keeps changing. If your address keeps changing, and you're never on the internet for very long, it's very hard for someone to deliberately intrude on you. However, many computer intruders are like teenagers - they will go to great lengths for what they perceive as 'fun'. I recommend at least some security beyond this, even if all you ever do is read and write email.

As soon as you have a stable address and a permanent connection, you lose the 'obscurity' advantage that a dynamic IP and sporadic connection provides. You must install a real 'front door'.

3. Passwords

The most basic lock for your front door is a password. Ensure that every computer on your network requires a password before anyone from the network can read your information or write to your hard

drive. If a password isn't required, there is no front door at all. If you're not sure how to ensure that passwords are necessary, I strongly recommend getting hold of a computer expert, or at least a very good manual.

> **Note:** Most computer systems will not password-lock someone sitting at the computer itself. There are ways to do it, but there's usually a way that someone at the computer itself (not on the network) can get in and change the passwords. This is to prevent the computer from becoming an expensive doorstop if the passwords are forgotten. This does, however, mean that you still need physical security.

Changing forgotten passwords isn't easy, however. It's better not to forget them in the first place. If your system has a 'master password' that has access to everything, make sure two people in your company or household know that password. If there's only one, what happens when that person is on vacation on that tropical island with no phones?

Passwords are only as secure as they are difficult to guess - if your password is your name, for instance, or the word 'password', it's like putting a lock on the front door and never bothering to actually lock it.

There are a lot of suggestions for how to make passwords difficult to guess - here're a few of them:

- no less than eight characters long
- include both upper and lower case letters, numbers and punctuation marks
- don't use anything which can be guessed by someone who knows you or has your information - no names of family members or pets, no licence numbers or passport numbers or phone numbers or similar, not a street address (current or past!), not any words which are visible from your desk (like the brand of monitor)
- no legitimate words in any language, brand names or logos
- no swear words
- not a simple substitution (ABC as 123, to as 2, Ziggy as 2166Y)
- not the same password as on as another computer, or the same one you had last year. ANY password can be figured out in time, and if someone guesses one of your passwords they might try the same thing for another computer
- not a common misspelling of a word

Suggestions for good passwords include

- take something you'll recognise - a line from a book or a line of poetry - and use the third letter of each word. Include punctuation (but not spaces)
- a really, REALLY bad misspelling of a word
- two words from different languages stuck together with punctuation marks
- a short phrase

Think up other suggestions. For passwords, weird and idiosyncratic is good.

4. Permissions

Passwords usually come with usernames as well. A good username-and-password system will enable you to set up several roles for your computers. Each role will need different types of access, will use different programs and different data.

If an intruder guesses or finds out one person's username and password, they will have access to any programs or data that person usually has access to. For this reason, you might like to limit what each person is allowed to access.

Most computer systems have something in place which does this. Under most systems, it is called 'permissions'. Your computer manual or local expert can help you set it up on your computers.

Give each person what they need to do their jobs, plus a little personal space of their own. That personal space is often used to 'to-do' lists and other minor things which make their job easier or more comfortable.

5. Firewalls

If passwords provide a 'door' to cover the 'doorway' into your 'house', then firewalls provide 'shutters' to cover the 'windows'. Bear with me, we're extending the metaphor further than we probably should.

Your network has a lot of windows. These aren't just casual windows that let you see out, the metaphor is closer if you think of them as service windows, like at a drive-through of them have people (programs) at them to provide service, some of them are empty.

A firewall provides shutters to close the empty service windows.

A firewall does absolutely nothing to protect the windows you leave open - that's the job of the programs which provide the services at those windows. But if you don't have a firewall, there's all those empty windows that an intruder can use to break in through.

The firewall is ideally a separate computer which is between your network and the internet. It can be a purpose-built device - there are some available which are small black boxes which look like network hubs. Or it can be your brother's old 486, with a highly secure operating system that provides an inbuilt firewall. Whatever you choose, ensure that your local computer expert approves of it, and do your best to ensure that he knows how to make sure it really is secure.

None of your computers should be able to access the internet or be accessed from the internet without going through the firewall.

> **Note:** The technical term for the windows is 'ports'.

6. Other security measures

6.1. Unused programs

At each 'service window' that your firewall leaves open (technical term: 'open port'), you should have a computer program. This program should be providing some sort of service to your users.

Any program which isn't being used, but which has a connection outside your network, should be shut down and the 'service window' (port) closed at the firewall. Every port which isn't specifically in use should be shut down. Admittedly, this is a 'paranoia' position - the rationale for shutting them down being that a closed port is safer than an open one, regardless of how good the program is.

6.2. Bugs & patches

Programs which you are using need to stay operational, and their ports 'open'. However, occasionally programs are vulnerable to clever attackers.

Vulnerabilities are reported to organisations on the Internet which make a point of informing the companies or groups who write those programs, and distributing the modifications that these companies or groups produce to patch the vulnerabilities.

Every so often someone in your company should go to those sites, read their reports for your programs, and install the patches. Once a month is common, but you need to determine your own balance between security and convenience.

6.3. Monitoring

How do you know if someone has broken into your system? The only way to know for sure is to monitor it.

Some common types of monitoring tools are:

- The tripwire: On a read-only medium (like a write-protected floppy), store a program and a small database. The program checks every file in the database to find out when it was last changed, and sends the user the list of all the files which have changed since it first ran. To prevent false reporting, the database should only include files which should never be changed.

  If any of the files have been changed, you may have been broken into. (Or your system administrator installed a new version of the operating system and forgot to warn whoever does the monitoring!)

- The sniffer: This tool checks all the traffic which goes through the network, looking for suspicious activity. It's usually installed on the firewall, or on a special box just to one side or the other of the firewall - though it would be more useful on the outside.

  It doesn't attempt to block any activity, only to report it when it finds it.

- The honeypot: One for special circumstances - this system has most of the useful programs (like directory listers or file removers or editors) removed and replaced with special programs that shut the computer down as soon as they're run. The shutdown prevents the intruder from further intrusion, and also from modifying the honeypot's logs.

  These aren't very useful as working computers - they're simply traps.

- Log analysis: This is difficult - most intruders will be careful to wipe traces of their activity out of the logs. I don't recommend its use by laymen, and include it here only because it is an important tool for more experienced administrators.

  Most operating systems keep a set of logs of their network activity. This usually consists of things like 'opened this port', 'sent mail to this person', 'closed the port'. The content of the mail is not kept, but the fact of its being sent is. This sort of information is a useful tool for intrusion analysis (and for checking whether the system is running correctly).

  Log analysis involves whoever does the monitoring going through the logs and looking for strange occurrences. Logs look something like this:

```
May 13 09:57:03 gondwanah dhclient-2.2.x: DHCPDISCOVER on lo to 255.255.255.255 port
May 13 09:57:05 gondwanah dhclient-2.2.x: No DHCPOFFERS received.
May 13 09:57:05 gondwanah dhclient-2.2.x: No working leases in persistent database -
May 13 09:57:05 gondwanah dhclient-2.2.x: No DHCPOFFERS received.
May 13 09:57:05 gondwanah dhclient-2.2.x: No working leases in persistent database -
May 13 10:00:21 gondwanah dhclient-2.2.x: DHCPREQUEST on eth0 to 10.0.3.1 port 67
May 13 10:00:21 gondwanah dhclient-2.2.x: DHCPACK from 10.0.3.1
May 13 10:00:21 gondwanah dhclient-2.2.x: bound to 10.0.1.1 -- renewal in 3500 secon
```

You're not expected to understand what this is! It's an attempt by my computer to get an IP address (a number address) from the master computer on our home network. Log analysis involves reading a lot of stuff like this, knowing what's normal and what isn't, and dealing with the abnormalities.

Which is why I don't recommend it for laymen.

6.4. What do I do if I think I've been broken into?

If it was a physical break-in, call the police.

If it was a network break-in, either call the police or:

- Shut your computer down.
- Call your trusted computer-expert friend, or hire specialists in computer security.
- Consider calling the police. Consider preserving the evidence.
- Let the experts take your computer off the network, reboot it, and take a look at the logs. They will hopefully be able to figure out what type of attack it was.
- If you chose to preserve the evidence, make sure your computer experts know this before they change anything.
- Let the experts check your files for damage. They may recommend reinstalling the operating system, they may recommend restoring your data from your latest backup. Ask them for the pros and cons of each option they offer, and each recommendation they make. It's your data, but you hired them for their knowledge. So lean towards their advice, but you make the decision.
- Get their advice on further securing your system. Listen to it.

6.5. Final words

Your security system is only as strong as its weakest part. A determined intruder will keep looking until they find a vulnerability.

Security through obscurity is weak. A hidden thing is more secure than a highly visible one, but don't trust hiding on its own to protect your data. A hidden safe is more secure than a sock under the floorboards.

7. Links and further information

- WWW Security FAQ (http://www.w3.org/Security/Faq/www-security-faq.html)

- CERT (http://www.cert.org/), one of the major centres for vulnerability reporting and patch coordination
- About.com's Security page (http://netsecurity.about.com/)
- O'Reilly security books (http://security.oreilly.com/)
- Security Focus (http://www.securityfocus.com), another centre for security news

Notes

1. Note that once someone has physical access to your computer, there are a number of ways that they can access your information. Most systems have some sort of emergency feature that allows someone with physical access to get in and change the superuser password, or access the data. Even if your system doesn't have that, or it's disabled, they can always just pick up the computer or remove the hard drive and carry it out. More on this in the physical security article.