

iTCO

Linux Security
Foundation

White Paper

Why Do We Need Security?

In the ever-changing world of global data communications, inexpensive Internet connections, and fast-paced software development, security is becoming more and more of an issue. Security is now a basic requirement because global computing is inherently insecure. As your data goes from point A to point B on the Internet, for example, it may pass through several other points along the way, giving other users the opportunity to intercept, and even alter, it. Even other users on your system may maliciously transform your data into something you did not intend. Unauthorized access to your system may be obtained by intruders, also known as "crackers", who then use advanced knowledge to impersonate you, steal information from you, or even deny you access to your own resources.

How Secure Is Secure?

First, keep in mind that no computer system can ever be completely secure. All you can do is make it increasingly difficult for someone to compromise your system. For the average home Linux user, not much is required to keep the casual cracker at bay. However, for high-profile Linux users (banks, telecommunications companies, etc), much more work is required. Another factor to take into account is that the more secure your system is, the more intrusive your security becomes. You need to decide where in this balancing act your system will still be usable, and yet secure for your purposes. For instance, you could require everyone dialing into your system to use a call-back modem to call them back at their home number. This is more secure, but if someone is not at home, it makes it difficult for them to login. You could also setup your Linux system with no network or connection to the Internet, but this limits its usefulness. If you are a medium to large-sized site, you should establish a security policy stating how much security is required by your site and what auditing is in place to check it.

What Are You Trying to Protect?

Before you attempt to secure your system, you should determine what level of threat you have to protect against, what risks you should or should not take, and how vulnerable your system is as a result. You should analyze your system to know what you're protecting, why you're protecting it, what value it has, and who has responsibility for your data and other assets.

- **RISK** is the possibility that an intruder may be successful in attempting to access your computer. Can an intruder read or write files, or execute programs that could cause damage? Can they delete critical data? Can they prevent you or your company from getting important work done? Don't forget: someone gaining access to your account, or your system, can also impersonate you. Additionally, having one insecure account on your system can result in your entire network being compromised. If you allow a single user to login using a .rhosts file, or to use an insecure service such as tftp, you risk an intruder getting 'his foot in the door'. Once the intruder has a

user account on your system, or someone else's system, it can be used to gain access to another system, or another account.

- **THREAT** is typically from someone with motivation to gain unauthorized access to your network or computer. You must decide whom you trust to have access to your system, and what threat they could pose.

There are several types of intruders, and it is useful to keep their different characteristics in mind as you are securing your systems.

- 🚩 **The Curious** - This type of intruder is basically interested in finding out what type of system and data you have.
- 🚩 **The Malicious** - This type of intruder is out to either bring down your systems, or deface your web page, or otherwise force you to spend time and money recovering from the damage he has caused.
- 🚩 **The High-Profile Intruder** - This type of intruder is trying to use your system to gain popularity and infamy. He might use your high-profile system to advertise his abilities.
- 🚩 **The Competition** - This type of intruder is interested in what data you have on your system. It might be someone who thinks you have something that could benefit him, financially or otherwise.
- 🚩 **The Borrowers** - This type of intruder is interested in setting up shop on your system and using its resources for their own purposes. He typically will run chat or irc servers, porn archive sites, or even DNS servers.
- 🚩 **The Leapfrogger** - This type of intruder is only interested in your system to use it to get into other systems. If your system is well-connected or a gateway to a number of internal hosts, you may well see this type trying to compromise your system.
- **VULNERABILITY** describes how well-protected your computer is from another network, and the potential for someone to gain unauthorized access. What's at stake if someone breaks into your system? Of course the concerns of a dynamic PPP home user will be different from those of a company connecting their machine to the Internet, or another large network. How much time would it take to retrieve/recreate any data that was lost? An initial time investment now can save ten times more time later if you have to recreate data that was lost. Have you checked your backup strategy, and verified your data lately?

Developing A Security Policy

Create a simple, generic policy for your system that your users can readily understand and follow. It should protect the data you're safeguarding as well as the privacy of the users. Some things to consider adding are:

A generally-accepted security policy starts with the phrase "That which is not permitted is prohibited". This means that unless you grant access to a service for a user, that user shouldn't be using that service until you do grant access. Make

sure the policies work on your regular user account. Saying, "Ah, I can't figure out this permissions problem, I'll just do it as root" can lead to security holes that are very obvious, and even ones that haven't been exploited yet.

Means of Securing Your Site

iTCO Linux Engineers have many strategies, technologies and best practices which will help you secure the assets you have worked hard for: your local machine, your data, your users, your network, even your reputation. What would happen to your reputation if an intruder deleted some of your users' data? Or defaced your web site? Or published your company's corporate project plan for next quarter? If you are planning a network installation, there are many factors you must take into account before adding a single machine to your network. Even if you have a single dial up PPP account, or just a small site, this does not mean intruders won't be interested in your systems. Large, high-profile sites are not the only targets -- many intruders simply want to exploit as many sites as possible, regardless of their size. Additionally, they may use a security hole in your site to gain access to other sites you're connected to. Intruders have a lot of time on their hands, and can avoid guessing how you've obscured your system just by trying all the possibilities.

Host Security

Perhaps the area of security on which administrators concentrate most is host-based security. This typically involves making sure your own system is secure, and hoping everyone else on your network does the same. Choosing good passwords, securing your host's local network services, keeping good accounting records, and upgrading programs with known security exploits are among the things the local security administrator is responsible for doing. Although this is absolutely necessary, it can become a daunting task once your network becomes larger than a few machines.

Local Network Security

Network security is as necessary as local host security. With hundreds, thousands, or more computers on the same network, you can't rely on each one of those systems being secure. Ensuring that only authorized users can use your network, building firewalls, using strong encryption, and ensuring there are no "rogue" (that is unsecured) machines on your network are all part of the network security administrator's duties.

Security Through Obscurity

One type of security that must be discussed is "security through obscurity". This means, for example, moving a service that has known security vulnerabilities to a non-standard port in hopes that attackers won't notice it's there and thus won't exploit it. Rest assured that they can determine that it's there and will exploit it. Security through obscurity is no security at all. Simply because you may have a small site, or a relatively low profile, does not mean an intruder won't be interested in what you have.

Conclusions

Hopefully this document has educated you into some of the areas you will need to address to increase security in your Linux deployment. If you would like to know some more about how iTCO might improve Linux security within your organization please contact your local iTCO representative.



iTCO Solutions Corporation
P.O. Box 610090
Redwood City, CA 94061
United States

<http://www.itcosolutions.com/>

Enterprise Sales Team Contact
Ryan Edwards
National Accounts Manger
Tel: 650-367-0514
E-Mail: redwards@itcosolutions.com