Global Information Assurance Certification Paper

It's Not Your Network
(and it's only as secure as they want to make it)

Rick Ammenheuser
March 8, 2001

Abstract

So, you think you have a secure network. You've implemented all the latest security patches, hardened up your equipment and installed layers of defenses to give you the safest environment…right?

Wrong, even though countless hours are spent each week pursuing log after log, reading reports and monitoring change management controls, there still is a vulnerability lurking in the shadows of every hallway and cubical within your organization. The vulnerability that you think you have control over is your network's end users.

In my opinion, end users present the biggest threat to security vulnerabilities that exist for your network—considering both external and internal vulnerabilities.[1]

This paper will highlight some of the potential security risks that a company insider can introduce into your network. I will also provide some insight of what the information security team for my employer's enterprise has done to combat these risks.

My Company's Profile

I am part of an Information Security team for a worldwide company that comprises of approximately 25,000-networked users. These user IDs are distributed across the Enterprise and broken up into a NT 4.0 multi-master account domain architecture. The master account domains are primarily distributed geographically by continental region.

Additionally, this Enterprise entails approximately 500 resource domains, which have a one-way trust pointing back to each master account domain. These resource domains average in size anywhere from 3,500 users down to 10 users each.

WAN circuits range from dual T1 pipes and Frame Relay Circuits servicing the larger sites down to multi-linked asynchronous modem sites providing around 80 kbps service on demand to the smallest locations.

As imagined, an enterprise architecture of this magnitude is very difficult to manage, monitor and control network users from an information security standpoint.

Build the foundation to protect you, your network and your company

Policy is the first line of defense you have to protect yourself, your network and to help mold user habit to conform to the results desired. While the process will

not happen overnight, the trek to a tighter network can be achieved through enforced **policy** and being aware of the human aspect of such an endeavor. It is paramount that senior management provides support for such initiatives. During the **policy** development phase, ensure that representation from each level of users – management down to the receptionist – have a voice in the creation of the primary information security **policy** document.

For a very large corporation in which I work, there is one guiding document, which will dictate direction and overall philosophy for the security of the organization's information assets. Smaller more concise policies are borne from this corporate document and tailored to fit departmental or functional needs on a site or regional basis. This level of document is what is needed to have the kick required to align user psyche and also manageability for implementation and audit ability. This level of document also provides the necessary granularity to accommodate ethical, language and political differences inherent of a global enterprise.

Several issues where users pose potential risk are mentioned below. While this list is by no means complete, I hope to demonstrate that picking the low hanging fruit can help tighten your networking environment to a point where you might be able to sleep a little easier at night.

Unaware users = risk

Passwords

There have been numerous papers and articles describing the mechanisms used (and the vulnerabilities introduced) by NT for password handling.[2, 3] While all these issues have merit, the single most vulnerable is the user's own handling of their credential. This problem appears to be so easy to fix but is actually very difficult to monitor to ensure compliance. In my environment, I routinely run across one or so instances a week where a user is violating existing password policy. The problem is primarily rooted from a couple key points:

1) Lack of user awareness – no matter how much attention is given to education and awareness about risks for sharing passwords, a few will never comprehend the potential of risk.
2) Temporary employees – users think that it is easier to share a credential for a day or so than wait for the new user's ID to be created.
3) Time – user doesn't have access to a resource and therefore "borrows" ID from another coworker to get temporary access to the desired service.

While some of these acts are intentional, most involve users who state that they were never informed of such risks. I use these occurrences as opportunities to educate the end user on a one-on-one basis.

Create ironclad password **policy** and have management backing and

enforcement and semi-annually publicize the existence of such a document. Also, provide the **policy** as part of all new hire orientation training sessions.

Ensure that your **policy** allows the use of password crack utilities to ensure that privileged accounts are not abused and take a firm decisive action if required.

Biometrics, Smart cards, and Kerberos all have great potential to help close the gap in user password handling. Currently, these implementations are still cost prohibitive for a large corporation and have large dollar investment with no immediate ROI. The implementation of Win2k migrations and the use of the inherent Kerberos will probably become the de facto standard for the windows platform and will provide a new level of protection.[4, 5]

Helpdesk/social engineering

Do you know what the current rate of password-reset calls your local helpdesk receive? Is your helpdesk staff trained to discern between a suspicious caller from a legitimate one? Monitor those call logs. Educate the helpdesk on all the latest social engineering tactics.[6] Create a work process to not give passwords over the phone, if possible. One great recommendation is to tell the caller that the reset password will be left on the caller's voice-mail system.[7] Incorporate this work process into **policy** and make the helpdesk accountable.

Disgruntled employees

Work with your Human Resources department and choreograph the disabling of network accounts with the termination of users. Have the user escorted out of the building and do not give the opportunity to "clean up a few loose ends" on the workstation. This level of caution is critically important for users with elevated access on the network.[8, 9, 10] Ensure that these steps are included in your **policy**.

Privileged (Admin) accounts

Create **policy** to ensure that network or machine administrators can't use Remote Access Service (RAS) to access the network remotely. Ensure that reading e-mail and surfing the web are grounds for loosing elevated privileges.

Any user that has administrator rights can change local server admin accounts. Often this has created an environment of uncertainty of whether the local admin password has been changed – either intentionally or by error. Rename the local administrator account to something that would appear to be a normal network user ID. Create a **policy** to proactively, on a routine basis, run a script to maintain known credentials across all servers. Maintain the credentials within an envelope and lock in a safe within the data center.[11]

Create a dummy "Administrator" account and ensure that is has no rights. Audit this account and actively investigate any evidence of tampering.

Resource ACLs (share access)

If your network entails a large sum of transient users moving from department to department or project to project, ensure that access to shares follow that user on a need-to-know basis. This can be performed from group policy and managed via 3rd party tools. Ensure that you local **policy** requires that the data owner of the resource actively manage such access.

Deleted/dead accounts

As mentioned earlier, the company in which I work posses over 25,000 network accounts across multiple account domains. Due to the transient nature of these employees, HR's status of these workers change when moving from one subsidiary to another. As a result, HR records cannot be relied on to manage network ID validity. Keeping track of all these IDs is a huge undertaking even with automated tools. To lessen this exposure, create a **policy** to ensure passwords expire after a set amount of time (we use 30 days). The tool to manage this task is integral to any NT system.

After an additional 30 days, a script is run to disable any ID where the password has not been reset. The intent here is to still retain the ID but have the owner contact an appropriate administrator to reactivate it. A second script is routinely run after an additional 30 days to delete any ID that was not re-enabled during the interim. This last script is designed to delete the user's personal share, mailbox and associated network account.

Modems

Ensure that your **policy** includes a section on disallowing any modem use while having a machine connected to the network. Enforce this edict by war-dialing your entire block of public phone numbers. Believe me, in a large corporation, rouge modems do exist and will be exploited by hackers if found. Generally, as expected, the user of the modem is unaware of the risk associated with such a configuration.

If a business case does support dial-out use, ensure all other available options are exhausted before approving it's use. Configure the modem to use a "dial-out only" port on the PBX if possible. Also, ensure that the particular box does not have any type of routing enabled and monitor all installed configurations on a routine basis.[12]

Remote Access Service (RAS)

Protect those RAS numbers - consider them Intellectual property! Ensure that administrator accounts do not posses such access. Only grant the user RAS access if a business case truly exists. Ensure that **policy** states such positions.

PcAnywhere and other remote control tools

Limit use of remote control tools at the administrator level. End users customarily use default installs, which pose security risks to known vulnerabilities and fail to maintain upgrades or patches for change management. When needed, ensure that **policy** states that all approved installations are to be locked down to a minimum of users, which have a true business case for such usage. Ensure that **policy** requires you to audit such installations and take appropriate actions, if violations or abuse exist.

Shareware/internet access

Internet surfing -- the great corporate pastime (waste of time). Implement mechanisms to minimize or stop the downloading of trial installations of commercial software, shareware or freeware. These types of software distribution mechanisms, usually (in many cases) EXCLUDE corporations of such limited use. Most users are unaware of this fact and could potentially pose substantial liability risk to your employer.

Create **policy** to ensure that machines are locked down locally to disallow software installation and/or shut the door at the proxy using content based filtering and reporting tools. Send these reports to your HR contact for appropriate disciplinary action.

Internet e-mail and risk to company image[13]

Educate the user when it is appropriate and required by **policy** to encrypt messaging.[14] Use content filtering at the mail gateway for all out-going mail to block (from a customizable word list) any sensitive information that could potentially expose the company. Automatically attach a “trailer” to all Internet destined e-mail with a disclaimer to minimize company risk from the content.

Virus

Lessen the potential of damage at the desktop by disabling scripting. Force the user via **policy** to not disable or prevent DAT updates. Inform all users about hoax e-mails and the intent of such mass distributions.

Laptops

Ensure that **policy** requires the encryption of all hard drive data on all laptops. Use corporate approved encryption tools to ensure intellectual property, RAS numbers, user profile information and cached passwords are adequately protected from possible theft. Inform users that the immediate notification of stolen machines would help minimize potential access to the network. Educate users to be aware of their surroundings; “shoulder surfing” at the airport terminal or on the plane could lead to potential leaks of trade secrets or hacks into the network.

Software Developers and other IT personnel

Finally, I have yet to meet a developer that does not need a test environment for the troubleshooting of their products. Ensure that data used in their testing is comprised of junk info. If real data is required to check data integrity mechanisms, ensure that environment is appropriately locked down. Often, developers have their test environment wide open to help troubleshoot bugs. Create a **policy**, which requires the registering of all servers not physically isolated from the floor and ensure change management mechanisms are installed, if possible. Also monitor and ensure virus utilities are installed and kept up to date.

Summary

The intent of this paper was to expose to the reader the level of risk introduced by your "normal" network users. The above recommendations should only prevent the novice user inside the organization from creating much havoc.

True seasoned hackers, and to a limited extent "script-kiddies", are another story. From a hacker/kiddie standpoint, each of the above items is large enough to warrant individual papers investigating their inherent vulnerabilities against such a threat.

Even though, I view uninformed network users as the weakest security link in any network system, having no network would most likely equate to me flipping hamburgers at a local fast food joint.

While it is becoming quite common to read about the latest virus outbreak or the recent dot.com break-ins, most users have the "it will never happen to us" perception. They need to realize that security is everyone's business. If your company is the next victim to hacker activity, you might be out of a job; but also your users, as well as the demise of your employer may also be at risk.

"The most secure fortress in the corporate world will crack if employees – from the corner office to the reception desk – aren't made aware of the dangers." [15]

The best a network security administrator can do is to ensure that security **policy** reflects your current network environment and raises the awareness of your end user.

Policy, no matter how boring it is compared to implementing a new piece of hardware, is the fundamental foundation for protecting your company's network infrastructure. Without **policy**, you can't monitor your user's activities. Without **policy**, management will not support any of your decisions. Without **policy**, HR will not help you control your users.

Without appropriate policies, it is you against them – the users.

Bibliography

[1] Stanley, Chris, "Network Security by Design", SANS Institute, October 9, 2000, URL: http://www.sans.org/infosecFAQ/securitybasics/netsec_design.htm, (February 25, 2001)

[2] Smith, Randy Franklin, "Protect Your Passwords", *WindowsNT Magazine, October 1998, URL:* http://www.win2000mag.com/Articles/Index.cfm?ArticleID=3844, (February 26, 2001)

[3] Edwards, Joeseph Edwards; LeBlanc, David, "Where NT Stores Passwords", *WindowsNT Magazine, August 1999, URL:* http://www.win2000mag.com/Articles/Index.cfm?ArticleID=5705, (February 26, 2001)

[4] Smith, Randy Franklin, "Why NT Passwords are Weak", *Windows2000 Magazine, November 6, 2000, URL:* http://www.win2000mag.com/Articles/Index.cfm?ArticleID=3844, (February 26, 2001)

[5] Kaplan, Ray; Kovara, Joe; Zorn, Glen; Krause, Micki (editor); Tipton, Harold F. (editor), Handbook of Information Security Management, Implementing Kerberos in Distributed Systems, Auerbach, 1999, URL: http://secinf.net/info/misc/handbook/115-117.html, (February 24, 2001)

[6] Fennelly, Carole, "The human side of computer security", Unix Insider Online, July, 1999 URL: http://www.sunworld.com/unixinsideronline/swol-07-1999/swol-07-security_p.html (February 22, 2001)

[7] Thaddeus, Jude, "Security Managers Journal, Week 26: From credit cards to corporate passwords, users are blissfully unaware of today's security issues", SANS Institute, February 5, 2001, URL: http://www.sans.org/newlook/resources/SMJ/week26.htm, (February 26, 2001)

[8] Radcliff, Deborah, "Internal employees - not outside hackers - can be a time bomb waiting to blow", InfoWorld, April 20 ,1998, URL: http://www.findarticles.com/m0IFW/n16_v20/20524682/p1/article.jhtml, (February 24, 2001)

[9] Ohlson, Kathleen, "Disgruntled employees: the newest kind of hacker", ComputerWorld, Online News, March 11, 1999, URL: http://www.idg.net/crd_brewer_69413.html, (February 24, 2001)

[10] Georgia, Bonny, "On the firing line", NetworkWorldFusion news, November 11, 2000, URL: http://www.nwfusion.com/careers/2000/1106man.html, (February 25, 2001)

[11] Wells, Bob, "How to Manage Your Enterprise's Passwords the Easy Way", Windows2000 Magazine, August 1, 1998, *URL:*

http://www.win2000mag.com/Articles/Index.cfm?ArticleID=3687, (February 26, 2001)

[12] Fisch, Eric A.; White, Gregory B., "Secure Computers and Networks – Analysis, Design and Implementation", CRC Press, 2000

[13] Reh, John F., "You Have to Have an E-mail Policy", Management, an About.com GuideSite, URL: http://management.about.com/smallbusiness/management/library/weekly/aa071299.htm?COB=home&terms=email+policy+liability&PM=112_300_T (February 22, 2001)

[14] Boustani, Eric Bakri, "An Employer's Approach to Email policies", CyberCouncel, URL: http://iplawyers.com/CyberCounsel/an_employer.htm (February 22, 2001)

[15] Radclif, Deborah, "Physical Security: The danger within (internal threats to data security)", InfoWorld, April 20, 1998, URL:http://www.findarticles.com/cf_0/m0IFW/n16_v20/20524682/p1/article.jhtml (February 24, 2001)