Hardening Authentication

On many networks, in order for users to be granted access to network resources, they must prove that they are who they say they are. This is the process of **authentication** of a user. The user can be authenticated by what he has (e.g., an ID card or token), what he knows (e.g., a password or PIN), or what he is (e.g., biometric data). More robust authentication processes use two or more of these factors.

Your network likely has an authentication mechanism in place to make sure that your network resources cannot be accessed by unauthorized users. However, your authentication process may not be as robust as it should be, or your authentication mechanism itself may be vulnerable to attack. The following are some suggestions for hardening this critical piece of your infrastructure.

1. Limit Remote Access

Limiting remote access to your network is likely the most effective mitigation step you can take, because it will reduce your attack surface. Remote access should only be allowed for those users who truly need it to perform their duties; it should not be standard for all users.

- Do not allow remote access clients to connect directly to the internal network – they should connect to a DMZ (demilitarized zone) and their traffic should be monitored.
- Restrict remote access to only authorized IP addresses.
- Limit concurrent logins to one per user.
- Audit login activity – verify suspicious logins with users, look for successful logins from unusual IP addresses, and look for spikes in failed logins.
- On each login, notify users of their last login date/time – if a user sees a suspicious last login, he should inform your network security personnel.

2. Augment Authentication Measures

If you are only using one factor to authenticate your users, consider using two or more. Other suggestions:

- Avoid transmitting authentication information using cleartext/weak protocols (e.g., telnet, ftp, http, pop3, ssh-1, etc.).
- Consider requiring users to do additional authentication (e.g., an additional password) in order to access protected resources and applications.
- Set login restrictions by time (e.g., no logins outside of normal work hours).
- For users who intermittently log in remotely, consider setting their accounts to be disabled by default – require them to first call in and have their accounts reactivated before they can log in. The accounts should automatically revert back to disabled after a defined amount of time.
- Implement a Network Access Protection/Control (NAP/NAC) solution to check the characteristics of a client machine before allowing it access to your network resources.

3. Educate Users

Your users should be alerted that they might receive phishing e-mails that ask them for their user name, PIN, password, etc. To prevent their credentials from being stolen, users should never send any of this information in an e-mail, and they should immediately inform your network security personnel if they ever receive such requests.

Users should never use high-privilege administrator accounts to browse the Internet or read e-mail. A malicious website, e-mail, or e-mail attachment could hijack the user's credentials, allowing an intruder to masquerade as the high-privilege user and do severe damage to the network.

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

The Information Assurance Mission at NSA

June 2011

4. Harden Authentication Server

Your authentication server should be hardened to prevent compromise of your authentication mechanism. If possible, build a new, hardened server from the ground up and once it is ready, transition to it and take the old server off line. The new authentication server should:

- Only do authentication, with no other services running and no file sharing.
- Have only software verified as valid installed on it – software can be verified by checking its hash against the vendor-provided value, or by using digital signatures. If digital signatures are used, be sure to enable checking for revoked certificates using Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) checking.
- Have its baseline install documented and periodically rechecked, either manually or with a system integrity checking application.

Even if you don't stand up a new server, do the following:

- Change the default passwords on the server.
- Prohibit Internet access to/from the server.
- Be sure the database of users that can be authenticated is up-to-date – old user accounts should be removed so they cannot be improperly used.
- Be sure that user passwords are stored securely – both on the server and on the clients – and transmitted securely (e.g., do not use Windows LanMan or any type of reversible encryption).
- Be sure all information about your authentication infrastructure (e.g., spreadsheets that link users to authentication data or that correlate different pieces of authentication data) is stored securely – preferably offline, or at least encrypted.
- If you are using a third party authentication solution, put that server in a separate security domain isolated from the rest of your network (e.g., for Windows Active Directory, the third party authentication server should not be part of the same forest as the rest of the network). An intruder on your network could use a temporary vulnerability to obtain domain credentials; isolating your authentication server reduces the risk that this intruder will then be able to obtain authentication information that would give him more persistent access to your network.
- Enable logging of all administrative actions done on your authentication server. Review these logs often, looking for any suspicious actions – especially any suspicious accesses of data used to authenticate users.
- Set firewall rules to restrict network and user access to the authentication server as much as possible. Only allow administrative access to the server from defined IP addresses.
- Consider requiring physical access in order to administer the authentication server. Restrict physical access to only authorized administrators.

5. Establish Robust Password/PIN Policy

Although establishing a draconian password policy may be the easiest thing to do, it is also the least likely to be effective. Such a policy will only annoy your users and inspire them to develop ingenious ways to get around it. It is important, however, to have a robust yet reasonable policy.

- Enforce selection of robust passwords/PINs.
- Lock out a user after a reasonable number of failed login attempts. Consider not doing automatic unlocks – your network security personnel should conduct a review before unlocking the account. This policy may allow a determined adversary to perform a Denial of Service attack against you, however, so weigh the risks.

The Mitigations Group
"One Voice"
www.nsa.gov/mitigations
OneVoice@radium.ncsc.mil
Creative Imaging 49948CG