Hardening Authentication

A text message can be sent to a husband to remind him to please pick up milk at the grocery store.

If the husband recognizes the sender's phone number to be his wife, he inherently trusts that it is his wife who sent this message and therefore purchases the milk.

But, beyond grocery lists, what about situations where you must be absolutely sure you know the message was sent from a trusted source?

What if a fighter pilot receives an urgent message to bomb an installation 200 miles away? Can it be trusted?

Or could it be a devious adversary hacking into military communications sending a message a message to destroy an allied bunker?

The process of determining that the original sender is he or she claims to be is called authentication.

Authentication can be broken down into three factors: something the user knows, such as a password or PIN, something the user has, such as a token or an ID card or something the user, such as a fingerprint or iris pattern, commonly known as biometric data.

Weak authentication can give a false sense of security.

Just because access to your data is protected with a password does not mean that the data is secure.

Relying on only one factor of authentication, such as a password, can be risky.

Security can be increased by using two or more factors of authentication.

For instance, requiring both a smart card and a password.

The National Security Agency's Information Assurance Directorate, or IAD, released a fact sheet of strong authentication recommendations called Hardening Authentication.

It provides a number of suggestions for strengthening your authentication process.

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.

Of course, any system used for remote access must be properly secured.

Do not allow remote access clients to connect directly to the internal network.

They should connect to a demilitarized zone, or DMZ, and their traffic should be monitored.

Restrict remote access to only authorized clients. (for example, filtering by IP address).

Only company owned systems with approved baselines should be allowed remote access.

Limit concurrent logins to one per user.

Audit login activity.

Verify suspicious logins with users.

Look for successful logins from usual IP addresses and look for spikes and failed logins.

On each login, notify users of their last login date and time.

If a user sees a suspicious last login, he should inform your network security personnel.

If you are only using one factor, such as just a password to authenticate your users, consider using a multi-factor mechanism, such as PKI or using a hardware token, especially for access to sensitive or critical resources and applications.

Avoid transmitting authentication information using cleartext or weak protocols, such as telnet, ftp, http, pop3, or ssh-1.

Instead use only secure protocols as recommended by NIST-FIPS or special publications, which are available at the following URL: http://csrc.nist.gov/publications/

Configure the host to minimize the number of locally credentials.

The number of cached credentials should be set to 0 for desktops and servers, and 1 for laptops.

Set login restrictions by time and user type, such as 'no employee login outside of normal work hours'.

For users who intermittently login in remotely, consider blocking their access by default.

Require them to first call in to be allowed access. Access should then automatically be blocked again after a defined amount of time.

Implement a network access protection, or NAP, solution to check the characteristics of a client machine before allowing it access to your network resources.

Consider segmenting your network to isolate high value assets and services, sensitive information, and privileged processes.

If an intruder gains access, this will limit the damage that can be done.

Alert your users that they might receive phishing emails that ask them for their user name, PIN, password or other personal information, or that direct them to an unknown or untrusted website.

To prevent their credentials from being stolen, users should never send any sensitive information in an email.

They should immediately inform their network security personnel if they ever receive such requests.

If hardware credentials such as ID cards are used for authentication, remind your users to physically remove these credentials when not in use. This prevents an intruder from masquerading as an authenticated user.

Your users should never use high privilege administrator accounts to browse the Internet or read email.

A malicious website, email, or email attachment could hijack the user's credentials, allowing an intruder to masquerade as the high privilege user and do severe damage to the network.

For suggestions on how to enforce this, see the "Enforcing No Internet or Email from Privileged Accounts" NSA fact sheet at the following URL:
https://www.iad.gov/IAD/library/ia-guidance/security-tips/hardening-authentication.cfm

In general, authentication credentials that provide access to sensitive resources should never be used on any system that is also used to access the Internet.

For example, the domain admin account should never be used to log onto and locally administer workstations.

Your authentication server should be hardened to prevent compromise of your authentication mechanism.

The authentication server should be used solely for authentication.

It should not also be used as a file server, web server, or anything else.

Only install software verified as valid on the server.

Software can be verified by checking its hash against the vender-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, or OCSP, or Certificate Revocation List, or CRL checking.

Document and periodically recheck the baseline install on the server, either manually or with a system integrity checking application.

Change the default passwords on the server and disable unnecessary accounts.

Prohibit Internet access to or from the server.

Handle patches and updates through an offline process.

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 all credentials are properly managed.

Passwords should be stored securely, both on the server and on the clients and transmitted securely.

For example, do not use Windows LanMan, or any type of reversible encryption.

Public key credentials should be validated to a known and trusted root, and should be checked for revocation.

Certificate trust stores and certificate usage should be minimized to those actually needed.

Seeds from one time password mechanisms should be protected with layered defenses.

For more information on password management, see NIST's special publication 800-118 Guide to Enterprise Password Management available at the following URL: http://csrc.nist.gov/publications/PubsSPs.html

Be sure all information about your authentication infrastructure such as 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 3rd party authentication solution, put that server in a separate security domain isolated from the rest of your network. For Windows Active Directory, for example, the 3rd 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 the intruder will be able to obtain authentication information that would give him 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 access 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 within protective enclaves.

Consider requiring physical access in order to administer the authentication server. Restrict physical access to only authorized administrators. Although establishing a Draconian password policy may be the easiest thing to do, it's 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.

Consider requiring public key based authentication, using FIPS-certified hardware tokens.

For password and PIN-based accounts, enforce selection of robust passwords and PINS.

Consider modeling user activity and setting thresholds to block anomalous login attempts.

At a minimum, lock out a user after a reasonable number of failed login attempts.

Consider a policy that requires your network security personnel to conduct a review before restoring access to a blocked account.

A more sophisticated lockout policy should set multiple incremental thresholds for failed authentications attempts to distinguish potential denial of service attacks from inadvertent activity.

Enforce the use of separate credentials for different accounts especially for administrator accounts.

If a user has administrator privileges, his administrative authentication credentials must be user specific and different from his non-administrative authentication credentials.

In general, the access allowed by a given credential should be minimized, both in terms of which assets can be accessed, and for how long they can be accessed. The latter can be accomplished by using a time-based access control mechanism, such as Kerberos.

While none of these steps will secure your network perfectly, implementing these tips will significantly harden your authentication protocols, and thus make your network more secure.

Preventing unauthorized users from access your sensitive systems is critically important, especially as technology improves and the number of skilled hackers increases.

It may not be as important when it comes to receiving a grocery list via text message, but when you're the pilot receiving a critical order, you want to make absolute certain it was sent from an authenticated source.

(music)