Social engineering

Remco Hobo

January 19, 2005

1 Social engineering, stealing passwords

Social engineering has his roots in the telephone system, with the so-called phone phreaks. By speaking the right jargon, it proved to be fairly easy to get information from people that wasn‘t supposed to be shared. The easiest way to break into a system is using a valid username and password. Getting your hands on a valid username and password might be much easier then breaking into a system using it‘s other security weaknesses. There are several ways to get a username and password from a person:

- Meeting them in a bar and chat them up, trying to reveal pieces of information.
- Impersonating another person and asking for information
- Phishing, sending an email of instant message, asking for personal information for "billing information"
- Eavesdropping, just get a job with the cleaning team and wait until you hear valuable information.

2 Try to gain access to several systems in the lab with social engineering

This excercise has no potential, no-one will tell any information that is of any use. This is because everybody knows the excercise, so is on "red alert". No information can be gained. Since I have done some work for Wouter's company in the past, I do know all of his passwords, and he also knows some of mine. However, I did gather information about a mail box, and it‘s password. With a little study (I need a last name to complete the username/password pair) I could get access to this mailbox. Since I am "white hat" I will not continue to get all this information and break into it.

3 coutermeasures

To remedy social engineering, there are several ways:

- Training has to be given to employees. Learn the employees how to identify social engineering. If they know when someone is fishing for information, they will less likely make the mistake of giving out sensitive information.
- Make sure new employees are always introduced. This way, a person impersonating a new hire will not get very far. If the organisation isn't too big, make sure everybody knows everybody.
- Create strict procedures about password resets, and account enabling and creating. Make sure everybody knows, sharing passwords is forbidden.
- Transfer the inquiry through to security personell, they might be able to trace where the caller is calling from. Also, a pattern might be uncovered and other counter measures might be taken if the pattern appears to be persistent.

4 Sending a PGP private key signed email

For this excercise we had to compose an email and send it to our lab assistant, signed with the PGP private key. In former excercises we have created and published a PGP public/private key pair. Therefore it was a simple manner of composing an email in KMail, in which I already had imported my PGP keys. Both systems PGP and openSSL rely on a system of certificates that are stored on a pubic place (normally a public webserver like cacerts.org). This way, a public key can be searched and added to the existing keys. A security flaw might be that a user can create a certificate with another person‘s name, and publicise this certificate. After this, the user might encrypt and send emails using this "forged" certificate. This might be remedied by letting your certificates be signed by trusted people (colleagues, friends, etc) and thus creating a chain of trust.

5 Sending a CAcert private key signed email

CAcert signed emails are another story. Below is a list of steps to enable Thunderbird to sign emails with the CAcert keys.

- First, create an account with cacert.org
- After this account is created, click in the right navigation bar on "Root Certificate".
- Click on "Root certificate (PEM Format)" and check all options.
- Click on "Root certificate (DER Fromat)" and save it to disk.
- Open an email client, open the email from cacert and click the link to activate the account.
- Log into cacert.org.
- Export your pgp key to a file; gpg –export –armor ¿ file.key
- Copy the data of file.key to the clipboard.

- In cacert.org, go to GPG/PGP keys.
- Select new and paste the data in the clipboard to the webpage.
- After this, a new key is shown, select this key and copy it to the clipboard.
- Browse to pgp.mit.edu and past the key in the box under "Submit a key". The key is now added to your PGP key.
- On the cacert.org page, click on client certificates, view, and click on the email address.
- Click on the "Click here" href to install the certificate.
- Open Thunderbird and configure your email account via the wizzard.
- Click on the compose a new mail button, click on the lock icon, and select sign. You will be shown a menu in which you can import the CAcert key.
- Click on import and select the key.
- Send the mail. If your'te lucky, you can now sign mails with your CAcert certificate.

Unfortunately, this didn't work for me. The step "Click on "Click here" href to install the certificate" has to be done with Firefox on the same OS etc as the Thunderbird mail client. This is because it ONLY works the FIRST time you click on it. Only the first time a private key is generated with the public key CAcert sends. Since I had installed the certificate in Firefox under Gentoo, and used the Thunderbird client under MacOS X, it didn't work. The webpage will not give any error report or hint. Thanks to some help from classmates, I found this out.

- I had to export the key from Mozilla under Gentoo by clicking on the backup button in the certificates menu, encrypt it with a password, and copy the .p12 file to firenze.
- I have imported this file under MacOS X, by going into the Thunderbird, preferences, advanced, certificates, manage certificates, import and selecting the .p12 file. I also had to import the DER file again from the cacert.org website.

After this, I could finally send signed emails.

6 Comparison GPG en CAcert

The most significant difference is that before you can send a CAcert email you first have to set up a GPG keypair. This first step is already quite difficult for most people, and after this step they already can send a GPG signed email (if the email client supports it). For CAcert, you have to do a lot more to get it working. This is a huge barrier for most users. I myself have had a lot of trouble getting it to work, and I am an "advanced" user. Also, the day after I have done this excercise, the GPG certificates could not be imported anymore on cacert.org due to a bug.

CAcert uses SSL, which also forces you to trust the root certificate of the cacert website. The root certificate is stored on the website, with it‘s pgp key to check it‘s authenticity, but the keys are stored on an non-secure web page. HTTPS is not used for this, which I find strange.

Is CAcert more secure? No, although Cacert has some added functionality, it isn’t more secure. Both rely on a secret key that has to be protected, both have a public key. With both techniques you can create a chain of trust and authenticate people by comparing a message, signed with a private key against the public key. The certificate‘s level of trust depends on the people it was signed by. With openSSL you can grade the level of trust for someone by handing out points. This is not possible with PGP/GPG.

My preference is with GPG, because of it‘s ease of use compared to CAcert.

7 Sending secure email to an SMTP server

For sendmail, a module [5] STARTTLS exists. This module will authenticate with openSSL certificates both client and server. Also data will be encrypted using the openSSL certificates.

Main functionality is:

- Server and Client openSSL certificates.
- Certificates are published on an CA.
- Rules can be written who to let in, and who to deny
- Relaying can also be done using openSSL.
- Extended debug and configuration options are available.

This means a client will still use SMTP, but the data is encrypted and signed using openSSL. The server identifies the client and authorises it and forwards the message. If the next SMTP server doesn’t understand the openSSL certificates, the data can be send on using normal SSL. With rules you can also disallow the message being forwarded plain-text.

This is one solution for the problem. Due to the fact I don’t have a sendmail server and don’t have time to install it and test this module, this part is purely theoretical.

References

[1] http://www.cacert.org, The CAcert website

[2] http://pgp.mit.edu, MIT PGP Public Key Server

[3] http://www.rhce2b.com/clublinux/RHCE-38.shtml, A site comparing the techniques used in both schemes.

[4] A lot of the information in this report was gathered questioning other students in the SNB lab.

[5] http://www.sendmail.org/ ca/email/starttls.html, The STARTTLS webpage