Safer hex in public places and at home

Holger Levsen

5th Debian Conference, Helsinki, Finland
Introduction

Security - the buzzword of the 21st century

Privacy enhancing tools

Data integrity and reliability
Outline

1. Introduction
2. Security - the buzzword of the 21st century
3. Privacy enhancing tools
4. Data integrity and reliability
Participate!

- This talk was announced as a BOF
- Therefore I’ll set up a wiki page :)"http://wiki.debian.net/SaferHex"
- So that everyone who is more experienced in $whatever can contribute easily
A general advice...

- Be safe - don’t play frisbee!
Introduction

2 Security - the buzzword of the 21st century

3 Privacy enhancing tools

4 Data integrity and reliability
You have no privacy, get over it (Scott McNealy, 1999)

Security is an illusion, data security twice

Or a little less dramatic: security is a chain, the weakest link breaks

So, why bother??

I think rather not. You cannot get perfection, but you can always make some links stronger and raise the barrier

At FOSDEM I met a guy who used no local passwords, whatsoever, because it’s so easy anyway to get the hard disc out of a thinkpad...
Things I learned over the time

- I was on the internet, before I knew that I was on the internet
- Privacy feature in mail and news clients of that time to set the send time to 00:00 always
- Today we have google etc. - and you are still able to find traces from me of that time
- Sometimes this alone is nice and useful, on the other hand it’s scary
Data traffic analysis from public data: IRC, mailing lists, GPG web of trust

3.000.000.000.000 minutes of voice traffic in Germany per year (most of it interceptible with echelon etc.), that’s 300TB disc storage (at 2kbit/s), the cost of doing it is neglectable

Then there is internet surveillance and data retention requirements (in the EU, all communication meta data shall be stored for .5-2 years (sid))

Tools to analyse those data exist
What does security mean to you?

- Privacy / secrecy
- Data integrity / reliability
- Classify and organize your data (private, specific audiences, public)
- This also applies to meta-data: don’t use your gpg passphrase for your webmail account
It all starts with physical security

- Ibooks are very secure :)
- Encrypt your /home, /var/ and swap partitions (rootfs also doesn’t hurt), leave a unencrypted partition for unclassified stuff
- Also encrypt your usbkey, where you should store your gpg-key. Better use a smartcard crypto usb-key
Tools that help you realize you are vulnerable

- dsniff, dnsspoof, mailsnarf, sshmitm, webspy
- driftnet
- ethereal can also capture VOIP streams and save them as .au files
- all are in Debian and there are a lot more available
- use them with care :-)

Safer hex in public places
Privacy enhancing tools

- ssh, ssh port forwarding, openvpn, ipsec
- imaps, pop3s, ssmpth
- gnupg
- ctrlproxy/screen
- tor, tor, tor!
- mixmonion
Outline

1. Introduction
2. Security - the buzzword of the 21st century
3. Privacy enhancing tools
4. Data integrity and reliability
Data integrity and reliability

- Do backups!
- Do backups more often, e.g. daily and even in HEL
- Encrypt your backups
- Running sid gives you no reliability, although you still can mostly rely on ssh and X11 to work as they should
Final words

- RTFM :-) It really helps...
- http://wiki.debian.net/SaferHex
- Thanks for your participation