Increased security standard or paranoia?

digmia
expert computing

30.11.2010

Tomáš Zaťko

About me

- Linux/unix sysadmin
- Penetration tester
- Co-founder of hackerspace progressbar.sk
- Member of The Society for Open Information Technologies
- Amateur paraglider pilot

Just because you're paranoid doesn't mean they're not after you.

Reasons

- Privacy
- Security fetish
- New experience
- Hobbies and activities on the borderline of law
- Cybercrime is not sci-fi anymore

What can be targeted in an attack?

- Physical access
  - Data on media
  - Installation of malware (backdoors, rootkits)
  - Firewire/USB memory dump attack
  - HW keyboard sniffer

What can be targeted in an attack?

- Physical access
  - Eavesdropping (of any kind)
    - Audio (remote/hidden microphones)
    - Video (remote/hidden cameras)
    - Emissions (Screen, cables, keyboard, ...)

What can be targeted in an attack?

- Network access (client)
    - Whole OS and installed software
        - Web browser
        - Mail client
    - Sniffing / modifying traffic

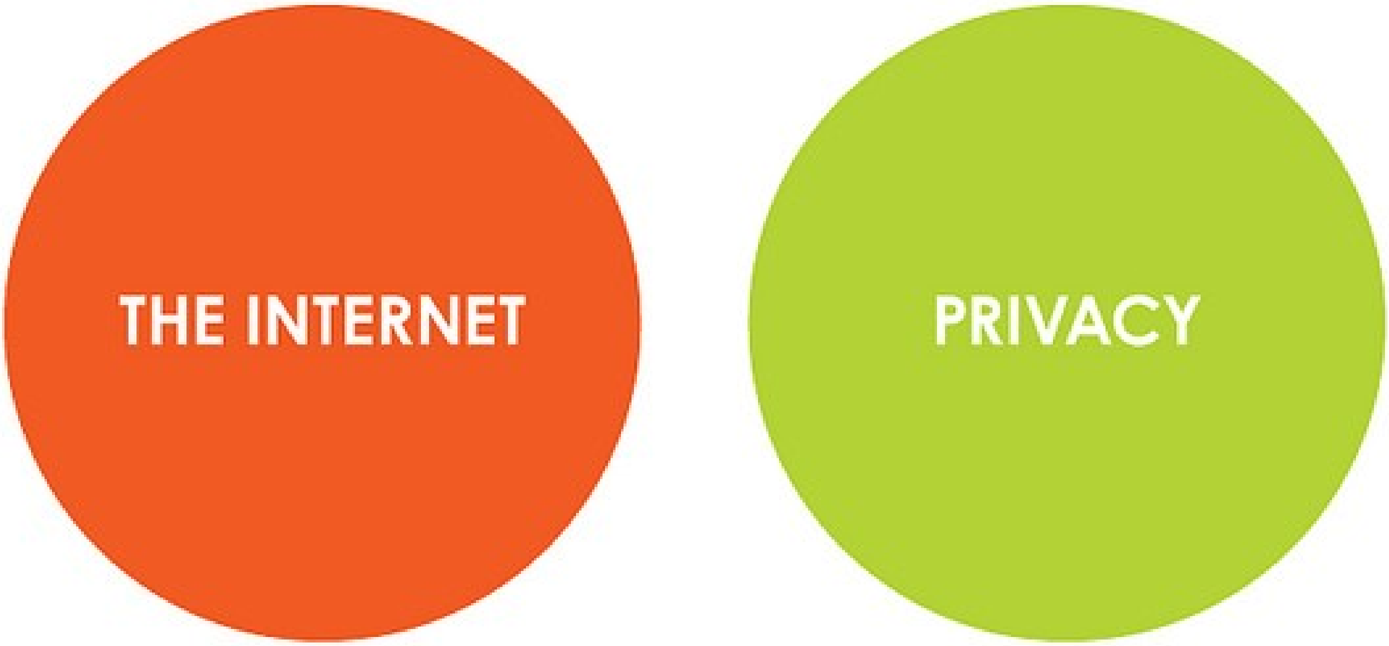
What can be targeted in an attack?

- Social engineering + Data mining
  - Social networks
  - Robots (google, archive.org, shodan)
- Human factor

So what?

- Security is about lowering the risk
- Degree of risk depends
- Conditions are changing

- And still there is real world... :)
  - (apt-get install real-life)



A HELPFUL VENN DIAGRAM

Data on media

- Encrypt, encrypt, encrypt
- ~/crypto || Crypto ~
  - Temporary files
  - System modification
  - Swap

Data on media

- Encrypt, encrypt, encrypt
- Full disk encryption
- HW encryption devices
  - Black box
- SW Implementations
  - Depend on chosen sw and it's configuration
  - Cold boot / evil maid attack

Data on media

- Evil maid
  - USB boot
- Cold boot
  - Alzheimer hook
- Rather don't give up physical control of your computer
  - Don't trust your drunk geeky friends :)
  - Be aware of your girlfriend :)

Data on media

- Removable media
  - Encryption is not always easy
  - Undelete
    - Shred
- Backups

Network access – web client

- You are actually running strange code
  - Enabled noscript, forcetls
  - Disabled unnecessary plugins
- Anonymization
  - UserAgent, IP, Referrer
  - Panopticlick.eff.org
- Cookies

Network access - MUA

- User-agent: / X-Mailer: / Other equivalents
- References:
- In-Reply-To:
- Received:
- Use VPN
- Delete unwanted headers

Human factor

- ”I can do it better”
  - Custom kernel with security patches (grsec+pax)
  - Slackware style fetish
  - In general – modifying takes time
- Backups
- Temporary / forgot *

Operating system

- Install only what you really need
- Use trusted software sources and check signatures
- Have separate environments for separate tasks
  - Restrict them as much as possible (fs,fw)
  - Rutkowska's qubes-os looks nice to me
- Mainstream is more interesting for attackers

General advice

- Use strong passwords
    - And store them securely
- Use different password for every service
- Encrypt all your data and traffic
- Always lock your screen

- Don't forget they are after you :)

Paranoia again

- Eavesdropping (of any kind)
- .mil / .gov 0days
- Girlfriend

My setup

- Full disk encryption with dm-crypt
  - Additional encryption of ultra-sensitive data credentials – decrypted only when needed
- Booting from USB
- Different users for different tasks
  - Multiple Firefox instances running as different users
- Noscript extension, Forcetls

My setup

- Using VPN all the time
- Hiding unwanted email headers
- Deleting data of “dangerous” accounts (pentest)

Questions

?

Thank you for listening!