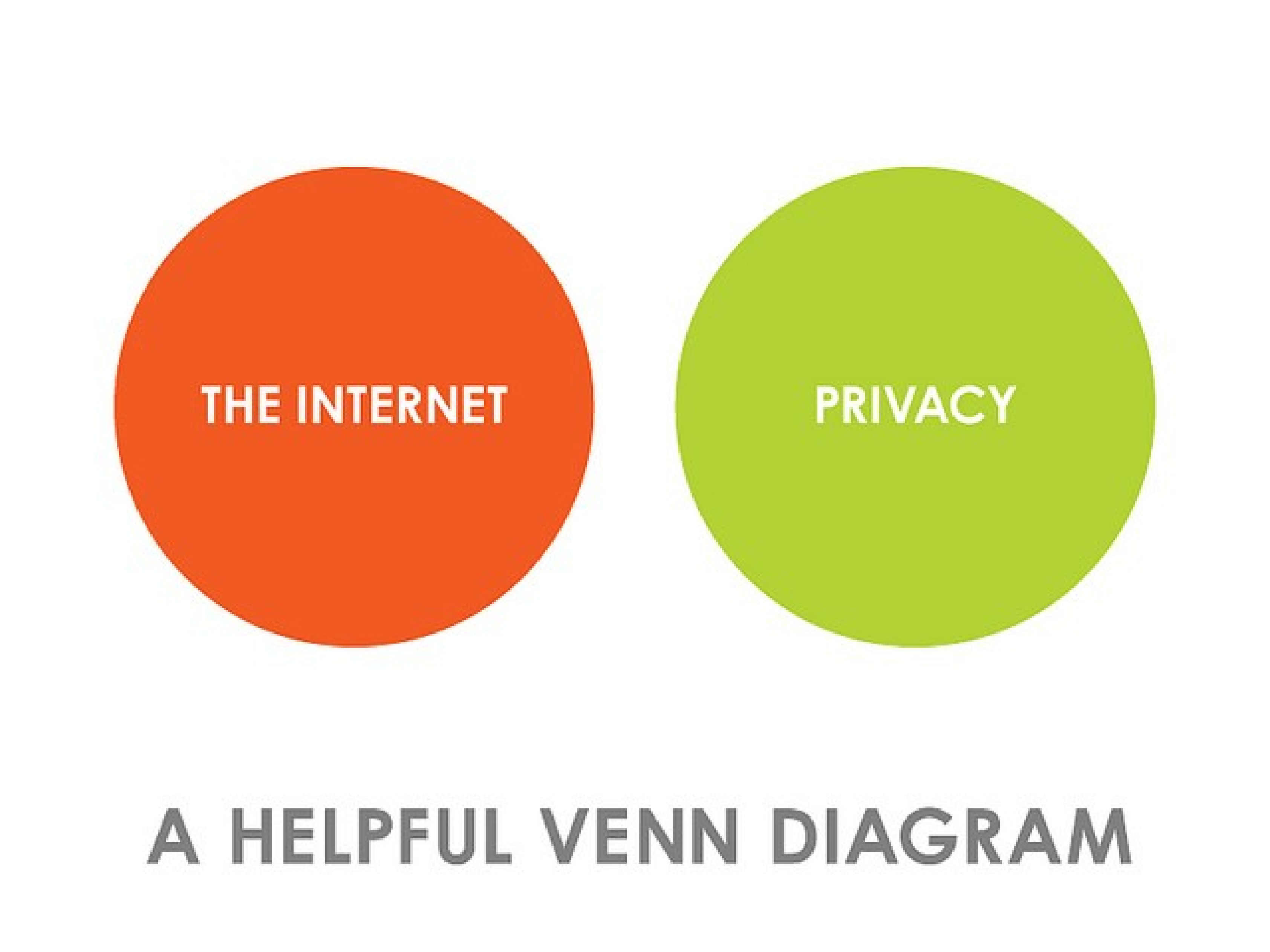
Increased security standard or paranoia?

tomas.zatko@digmia.com

Everyday paranoia

- Just because you are paranoid, it does not mean they are not after you
- The only secure system is unplugged from network, shut down, buried 20 meters under ground and guarded by angry army guards.
  - Even then I would not trust it enough


THE INTERNET
PRIVACY
A HELPFUL VENN DIAGRAM

Reasons

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

What do we want to protect?

- lorem ipsum dolor sit amet
- consectetur adipiscing elit
- nullam in mauris quam
- nulla facilisi
- vestibulum accumsan ligula
- sed nulla tincidunt sagittis
- in at lectus ac leo dictum pretium

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

What can be targeted in an attack?

- Network access
    - Server
    - Client
    - Configuration errors
    - Trust

What can be targeted in an attack?

- Social engineering
- Data mining (internet never forgets)
    - Social networks
    - Robots (google, archive.org, shodan)
- Side channels
- Human factor
- Coherences

So what?

- Security is about lowering risks
- Degree of risk depends
- Dependencies are changing
- And still there is real world... :)
    - (apt-get install real-life)

Data on media

- Encrypt, encrypt, encrypt
- ~/crypto
- Crypto ~
- Cryptoroot / full disk encryption
- HW encryption devices
  - Black box
- SW Implementations
  - And configurations in use

Data on media

- How much do we need to protect?
  - physical_security++
  - availability--
- Removable media
  - Dump + undelete

Data on media - attacks

- ~/crypto && crypto~
  - Temporary files
  - System modification
  - Swap
  - Side channels

Data on media - attacks

- Full disk encryption
    - Swap – it can be still easily forgotten
    - Wordlist / Brute force
        - Header / headless
    - Evil maid
        - USB boot
    - Cold boot
        - Alzheimer hook

Physical access

- Eavesdropping
  - Audio - jamming
  - Video - physical barriers
  - Emissions - maybe jamming+faraday fence ??
- Trust
  - Always lock your screen
  - Be aware of your girlfriend :)
    - Be aware who met your girlfriend and if it's Samy, be very, very concerned

Network access

- Server
  - Hardened firewall
  - Denyhosts
  - Port knocking (resistant to replay attack)
  - VPN
  - One time passwords
  - Banners of services

Network access

- Client – Web
  - You are actually running strange code
  - Anonymization
    - UserAgent
    - IP
    - Referrer
  - Cookies
  - Known software vulnerabilities

Network access

- Client – mail
  - User-agent: / X-Mailer: / Other equivalents
  - References:
  - In-Reply-To:
  - Received:
  - Known software vulnerabilities

Network access

- Misconfiguration
  - Access rights
  - Default config
  - Forgotten accounts, config files, whatever
    - Maybe not so big problem individually but linked with other pieces can cause more harm
- Trust
  - System accounts for friends
  - Friendly systems:
    - Proxy, firewall rules

- Human factor
    - ”I can do it better”
        - Cusom kernel with security patches (grsec+pax)
        - Slackware style fetish
        - In general – modifying takes time
    - Backups
    - Forgetting
    - Mistakes
    - Temporary (everything)
- Relations with other info

How to live with that?

- Restrictions
- Isolation
- Don't forget they are after you :)

How to live with that?

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

Get a life!

Questions

?

Thank you for your patience