heig-vd

HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD

www.heig-vd.ch

Cyber security challenges

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale

Security in « medical world »?

- A (too) complex system!

- Information systems
  - Standard services (storage, emails, websites, etc.)
  - Patient data (personal, treatment, images, etc.)
  - Electronic patient records
- Medical devices

- Cloud? Mobile?
- Laws and privacy regulations

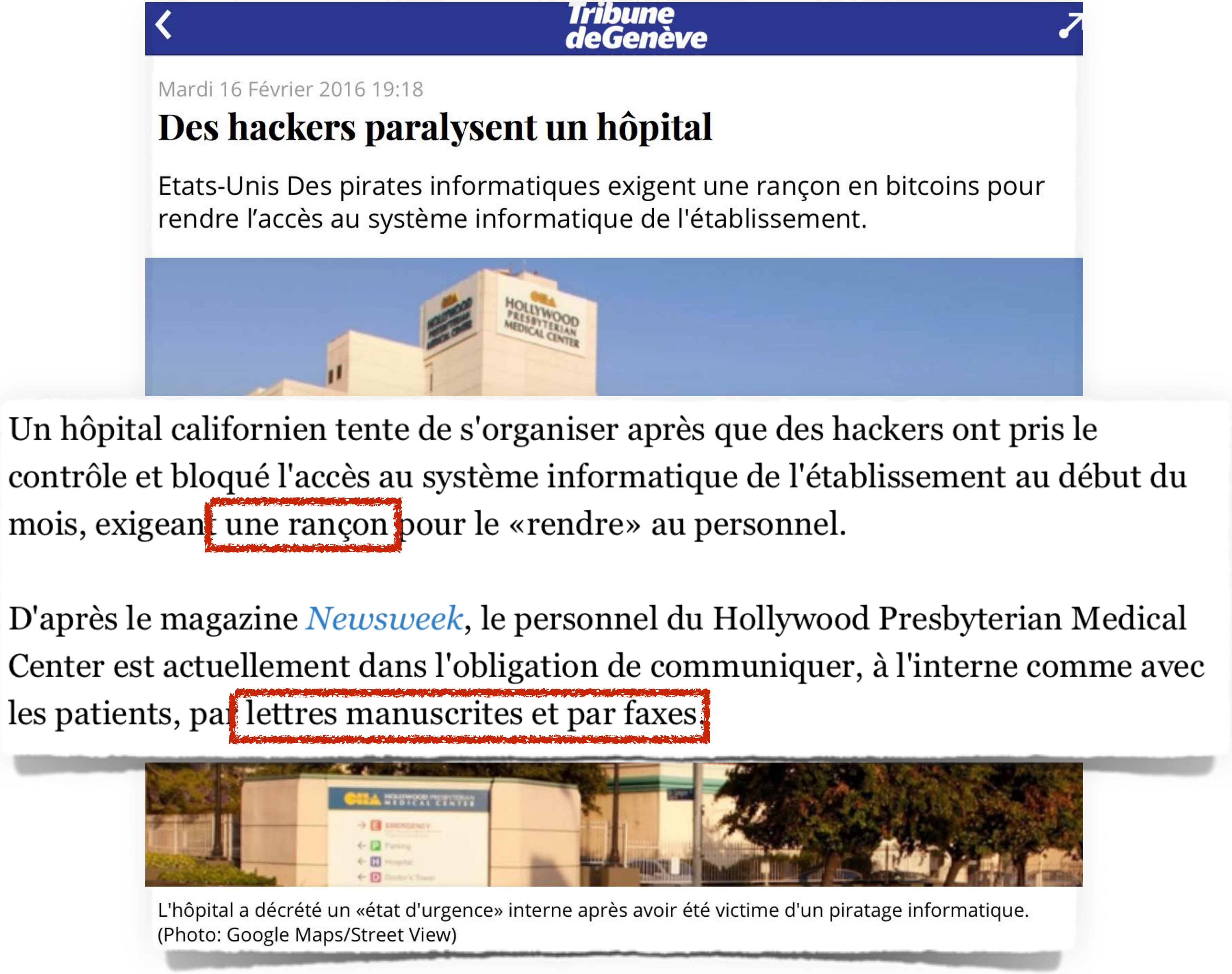
heig-vd

What about security of the information systems?

Switzerland: threats and « trends »

[Source] : MELANI reports (Melde- und Analysestelle Informationssicherung)

- Phishing
- Social engineering (attacks exploit user vulnerabilities)
- Cyber extortions
  - Ransom on data theft
  - Ransomware (e.g. crypto lockers)
  - Ransom on availability (e.g. denial of services)
  - Sex-torsion
- Targeted attacks (for instance RUAG)
- Governments involved in attacks (Stuxnet, PRISM, etc.)



Tribune deGenève

Mardi 16 Février 2016 19:18

Des hackers paralysent un hôpital

Etats-Unis Des pirates informatiques exigent une rançon en bitcoins pour rendre l'accès au système informatique de l'établissement.

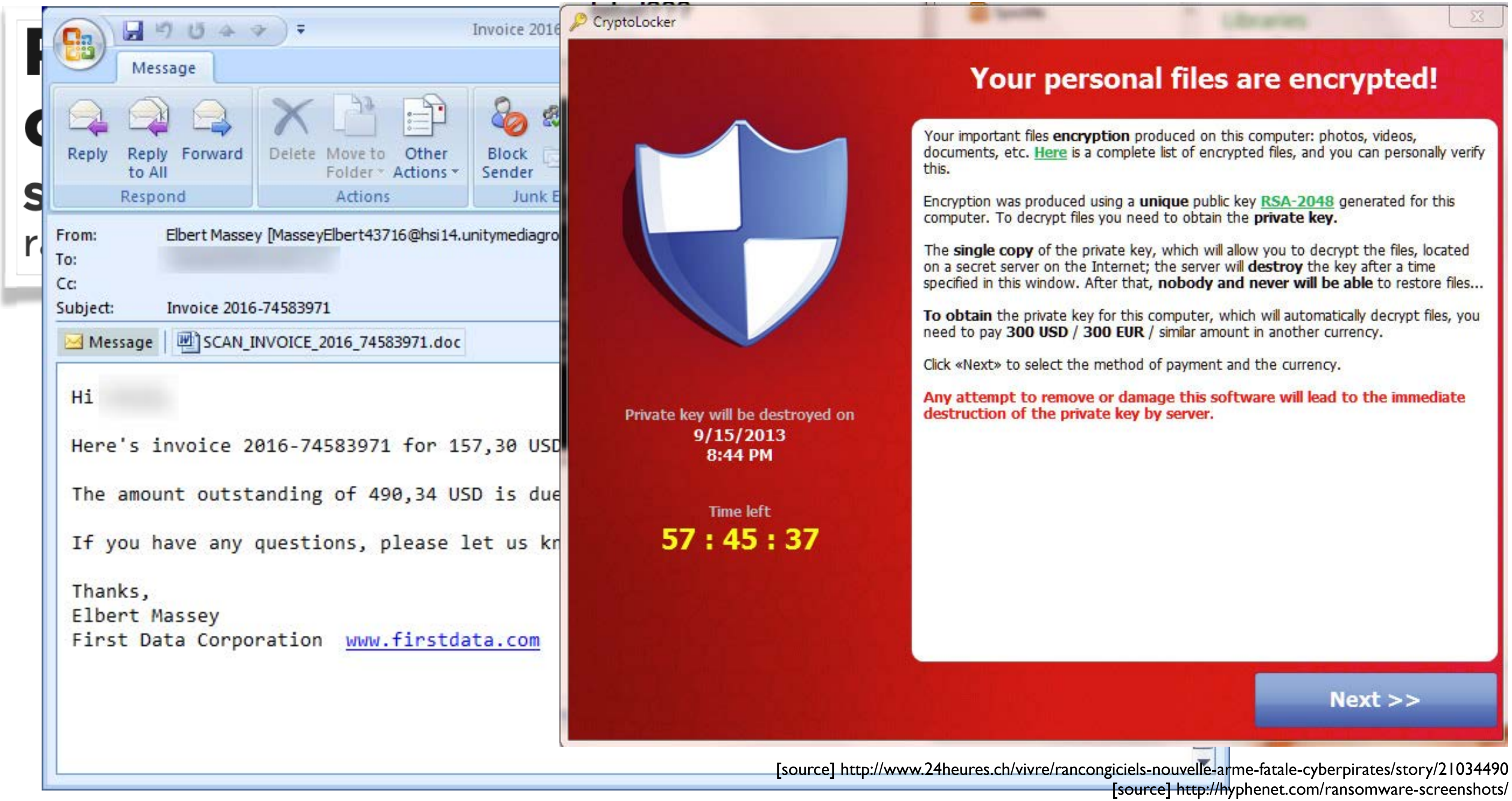
Un hôpital californien tente de s'organiser après que des hackers ont pris le contrôle et bloqué l'accès au système informatique de l'établissement au début du mois, exigeant une rançon pour le «rendre» au personnel.

D'après le magazine *Newsweek*, le personnel du Hollywood Presbyterian Medical Center est actuellement dans l'obligation de communiquer, à l'interne comme avec les patients, par lettres manuscrites et par faxes.

L'hôpital a décrété un «état d'urgence» interne après avoir été victime d'un piratage informatique. (Photo: Google Maps/Street View)

[source] http://mobile2.tdg.ch/articles/56c36775ab5c370bfa000001

Locky, cyptolocker, and others



From: Elbert Massey [MasseyElbert43716@hsi14.unitymediagro

To: [redacted]

Cc:

Subject: Invoice 2016-74583971

SCAN_INVOICE_2016_74583971.doc

Hi [redacted]

Here's invoice 2016-74583971 for 157,30 USD

The amount outstanding of 490,34 USD is due

If you have any questions, please let us kr

Thanks,
Elbert Massey
First Data Corporation www.firstdata.com

Your personal files are encrypted!

Private key will be destroyed on
9/15/2013
8:44 PM

Time left
57 : 45 : 37

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

[source] http://www.24heures.ch/vivre/rancongiciels-nouvelle-arme-fatale-cyberpirates/story/21034490
[source] http://hyphenet.com/ransomware-screenshots/

Cyber extortion

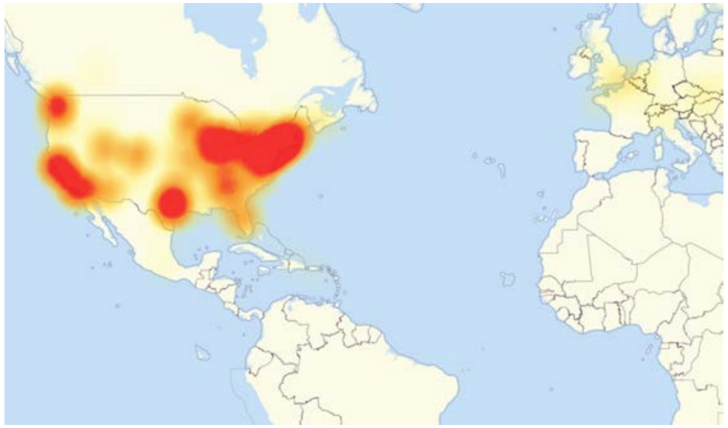
- First advantage:
  - No need to target systems with money
  - **Any system or data is appropriate** (owner is ready to pay)
- **Any form**: data/files, systems, network, etc.
- **Money laundry** is easier; virtual currencies (e.g Bitcoin)
- **Mass attacks: huge gains** (325 M$ for cryptowall, 2015)
- Vicious circle: victims pay, **criminals improve**, …
- Customer service (chat online, etc.)

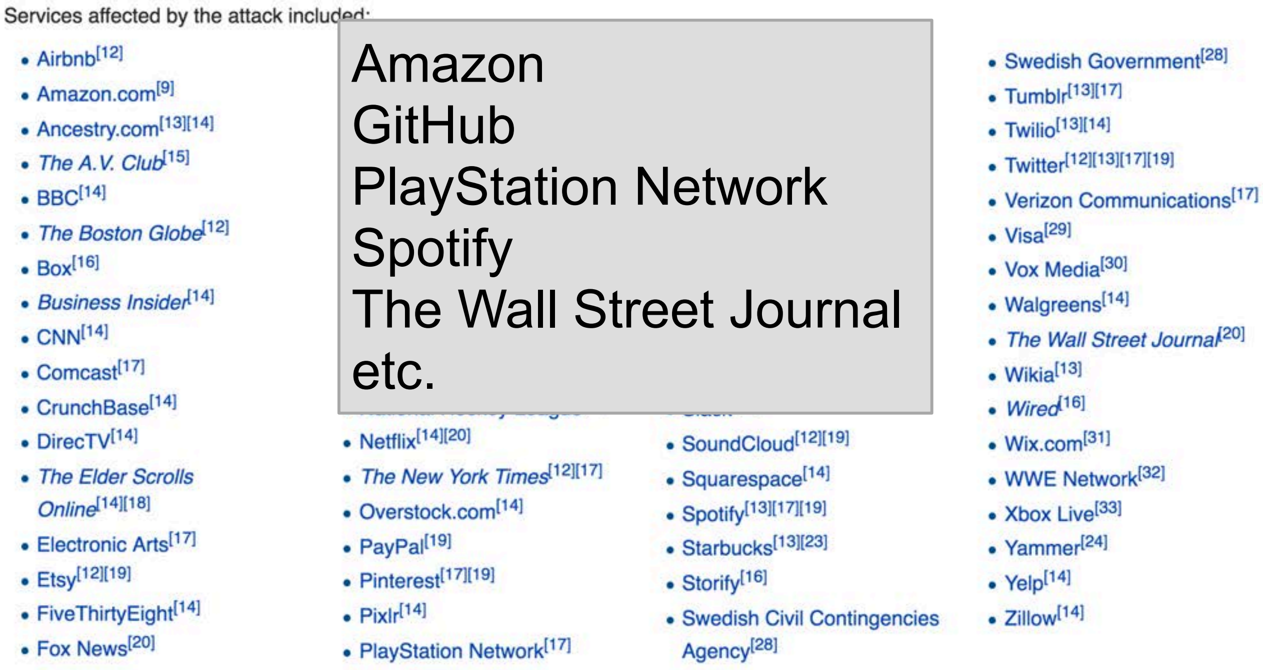
CNN (21 October 2016)

Unavailable services

Distributed Denial of Service (DDoS)

October 2016 :





Services affected by the attack included:

- Airbnb[12]
- Amazon.com[9]
- Ancestry.com[13][14]
- *The A.V. Club*[15]
- BBC[14]
- *The Boston Globe*[12]
- Box[16]
- *Business Insider*[14]
- CNN[14]
- Comcast[17]
- CrunchBase[14]
- DirecTV[14]
- *The Elder Scrolls Online*[14][18]
- Electronic Arts[17]
- Etsy[12][19]
- FiveThirtyEight[14]
- Fox News[20]

- Netflix[14][20]
- *The New York Times*[12][17]
- Overstock.com[14]
- PayPal[19]
- Pinterest[17][19]
- Pixlr[14]
- PlayStation Network[17]

- SoundCloud[12][19]
- Squarespace[14]
- Spotify[13][17][19]
- Starbucks[13][23]
- Storify[16]
- Swedish Civil Contingencies Agency[28]

- Swedish Government[28]
- Tumblr[13][17]
- Twilio[13][14]
- Twitter[12][13][17][19]
- Verizon Communications[17]
- Visa[29]
- Vox Media[30]
- Walgreens[14]
- *The Wall Street Journal*[20]
- Wikia[13]
- *Wired*[16]
- Wix.com[31]
- WWE Network[32]
- Xbox Live[33]
- Yammer[24]
- Yelp[14]
- Zillow[14]

Amazon
GitHub
PlayStation Network
Spotify
The Wall Street Journal
etc.

1.2 Tbps

(equivalent to 261 DVD/s, DVD=4.7GB)

Cause?

Malware Mirai (camera vulnerability)

Industrial automatization

E-health

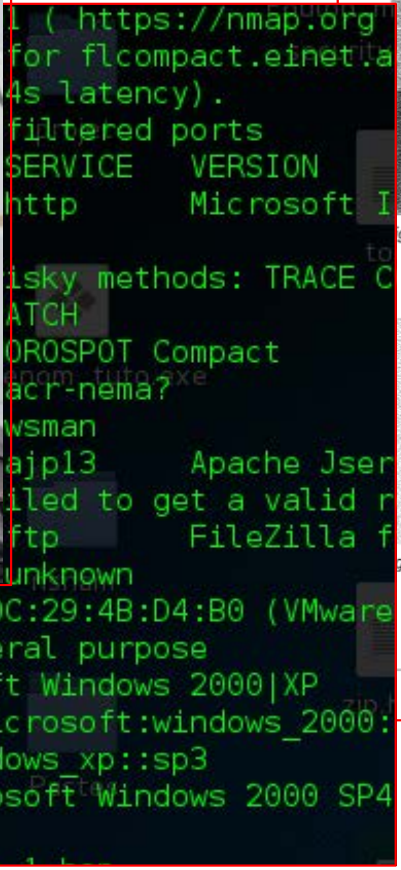
Smart Home

Smart Cities

What about security of medical devices?

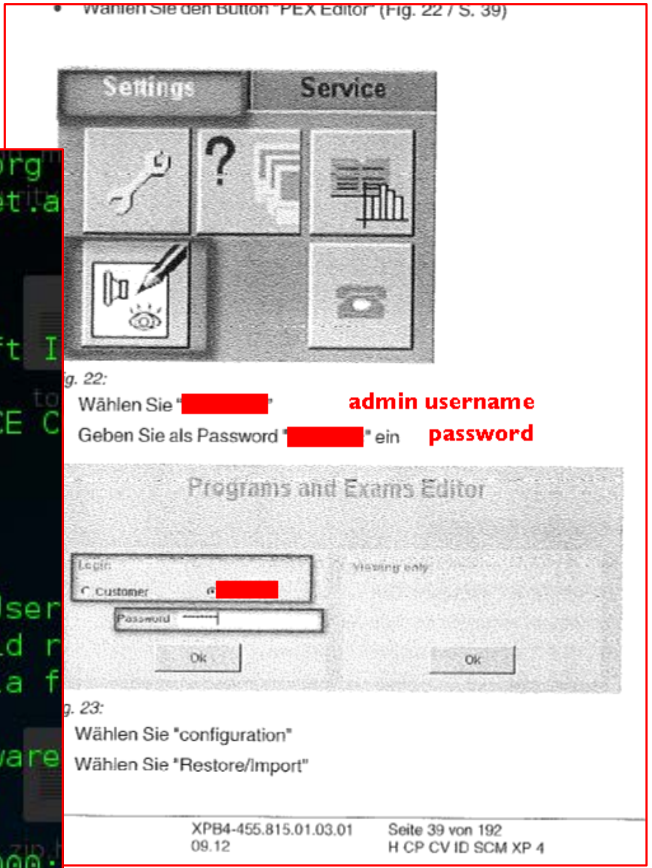
MedicAl SCAnneR POwNagE (MASCARPONE)

Project @ HEIG-VD



```
l ( https://nmap.org
for flcompact.einet.a
4s latency).
filtered ports
SERVICE    VERSION
http       Microsoft I

isky methods: TRACE C
ATCH
OROSPOT Compact
acr-nema?
wsman
ajp13      Apache Jser
iled to get a valid r
ftp        FileZilla f
unknown
MAC Address: 00:0C:29:4B:D4:B0 (VMware
Device type: general purpose
Running: Microsoft Windows 2000|XP
OS CPE: cpe:/o:microsoft:windows_2000:
/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows 2000 SP4
ws XP SP2
```



- Wählen Sie den Button "PEX Editor" (Fig. 22 / S. 39)

Settings
Service

g. 22:

Wählen Sie "[redacted]" **admin username**

Geben Sie als Password "[redacted]" ein **password**

Programs and Exams Editor
Login
Customer
Password
Viewing only
Ok
Ok

[redacted]

g. 23:

Wählen Sie "configuration"

Wählen Sie "Restore/Import"

XPB4-455.815.01.03.01
09.12

Seite 39 von 192
H CP CV ID SCM XP 4

Pacemakers: Hacking risk (August 2017)

- Recall of 500,000 due to patient death fears

- « lax cybersecurity »
- « run the batteries down »
- « even alter the patient’s heartbeat »

- « the recall won’t see the pacemakers removed »
- « issued a firmware update »

theguardian

Perfect murder? (July 2017)

Hackers can hijack DRUG PUMPS to kill hospital patients

© Tom Vickers/MOVI INC

© Shutterstock / Bravo_Roger

MailOnline

eHealth security trends

- Context:
  - Increasing **technologies**
  - Increasing **connectivity** in all medical devices, everything is connected!
  - Relatively easy or unattended **physical** access
  - **Legacy** software and technologies (Windows XP is born in 2001…)
- **Privacy vs. availability**
- **Interoperability**, security for new vs. legacy systems
- **Costs** pressure / business survival
  - functionalities are the priorities, security is not a concern
- **Security awareness is a priority** (at all levels)
  - doctors, operators, managements, admin, developers, etc.

Security engineers from HEIG-VD

- Bachelor degree: **« information security engineers »**
  - 3 years full-time
  - 180 ECTS credits
    40+ fully dedicated to infosec, **e.g. 1 year**
  - To date, **unique** such degree in Switzerland

- History
  - First student registrations in 2009-2010
  - First degrees awarded in 2013 (40 graduated since 2013)
  - Currently 60 students in formation

HEE: a multi-disciplinary research group

HEALTH
ENGINEERING
ECONOMICS

HEE platform fosters sustainable partnership to address unmet needs

HESAV
HAUTE ÉCOLE
DE SANTÉ VAUD

heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

heig-vd

Thank you

for your attention

sylvain.pasini@heig-vd.ch

LinkedIn http://ch.linkedin.com/in/sylvainpasini

http://secu.famillepasini.ch

@sylvainpasini