Infosec

karel@kubat.nl

Myself

- Karel Kubat
- Application development / architecture
- Security
- Financial services
- Presently Go2SEPA.nl / WAPP.nu

Agenda

- What to protect (against), opponents
- Recent examples
- Most notorious hacks
- How to protect
- Security & privacy

What to protect (against)

- Traditional losses
  - Loss of continuity (data / downtime)
  - Intellectual property
  - Reputational damage
  - Financial damage
- Opponents
  - Anonymous unknowns
  - Known outsiders, customers
  - Known insiders, staff

Target selection

- Dragnet fishing
- Spear fishing
- Drive by infections

Daily routine

- Apache proxy logs, bots
- SSL offloader logs, weak algorithm requests
- Firewall logs, portscans
- Injection attacks
- Infected customers (Zeus kit)
- Fraudulent customers or employees
- Software (re)engineering, code reviews

Rules of thumb

- Can’t lose what you don’t have
- Non-repudiation
- Multi-channel
- Keep tech up
- Increase security only if also increasing usability

Data / processing separation

- 1990’s: Crusty the Clown .ps
- Outlook mails with .scr
- Word doc macros
- Javascript + origin checks
- Java applet security model
- .asp active components

Simple data?

- PDF / Adobe Acrobat
- jpeg / gif / png buffer overflow problems
- font rendering & buffer overflow problems
- No known browser survives fuzzing
- 2012: Chrome & Firefox yield no useful fuzzing results
- 2013: Chrome & Firefox hacked within minutes

Google hack

- Targeted spoofed emails
- PDF infection vector
- Trojan
- Mothership command centre & updates
- Code repo theft
- Probably Chinese

Dalai Lama’s office

- Targeted spoofed emails
- PDF infection vector
- Trojan
- Mothership command centre & updates
- Surveillance
- Probably Chinese

Stuxnet worm

- Many infection vectors
- Mothership command centre & updates
- Windows shares, autorun.inf
- Last transmission via USB stick
- Targeted Siemens SCADA controllers
- Probably Israeli / USA

SQL injection

- Typical live data
- Most common cause of data loss due to hacking
- Soup nazi Gonzales: 170mio credit cards
- Heartland

Traffic interception

- Man in the middle
- Pseudo-WiFi
  - DHCP + gateway, ARP poisoning, DNS poisoning (Kaminski attack)
- Diginotar hacks
- Hong Kong Post Office
- Mostly surveillance

What to protect (against)

- Traditional losses
  - Loss of continuity (data / downtime)
  - Intellectual property
  - Reputational damage
  - Financial damage
- Opponents
  - Anonymous unknowns
  - Known outsiders, customers
  - Known insiders, staff

What to protect (against)

- Losses
  - Privacy
- Opponents
  - Ridiculously rich organisations

Snowden leaks

- NSA / GCHQ
- Spearfishing: anyone can be hacked
- Dragnet fishing
  - Weaken algorithms
  - Weaken implementations
  - Commandeering of Internet companies
  - Patriot Act / National Security Letters
- $250mio yearly budget, approx 10% R&D

Commandeering

- Likely Skype
- Possibly Google, Yahoo, Facebook
  - gag orders
- Not lavabit
- Not groklaw

How to fight back

- Do not trust closed source
  - Truecrypt or Bitkeeper?
  - OpenSSL or Windows Crypto API?
- Increase cost of cooperation

NL

- GCHQ
  - 7 out of 10 westbound Internet lines
  - Landfall in UK mentioned in leaks
- Verizon
  - Will probably offer telecom to the Dutch government
  - Falls under UK law
- KPN
  - Will collect & sell customer data
  - No opt in / opt out

Bayes

- DNA test with 1 : 1.000.000 false positive ratio
- Schiphol passenger movements
  - 43mio/yr (2007)
  - Assume 1% false positive alarms = 1178/day
  - Assume background check takes a few hours
  - 500+ extra security personnel needed only for false positives
- Surveillance cameras on highways

TSA 2012

- Some fireguns intercepted
- Top result: stopped turtles transport
- Pretty certainly also without TSA
- No fly list massively polluted
  - 100 names in 2001
  - 870k names in 2013

Thank you