Security through Openness

I. Background

Position

- Professor of Software Security and Correctness at Nijmegen since 2002...
- ... with 15 member (top) security group on smart cards, software security, protocols, auditing etc.
- Occasional role in discussions in the media on security in society topics:
  - bank cards
  - privacy
  - phone tapping
  - open source software
  - E-voting
  - ...
Involvement in OSS

- Participant in relevant discussions, inaugural speech, interviews, publications, ...
- Contributor to national E-Voting Experiment *Kiezen op Afstand* that went open source
- Active user, since many years.

II. Open Source Software (OSS)

What is OSS?

- **Minimal interpretation:** computer programs (software, source code) is available for public inspection
- **Stronger (official, see opensource.org):** code may be adapted & redistributed by everyone

Successful applications so far especially in:

- backoffice, notably webservers (apache)
- embedded software—to cut costs

Open/closed source essentials

- Programs are written as *source code*, which is still understandable (*if..then..else*)
- are “compiled” to *executable code* that:
  - actually runs on computers (as .exe)
  - is not readable for humans (0s and 1s)
- **Closed source distribution** means
  - the “binary” executable code is distributed
  - only the programmers know & check what code really does (too little or too much)
  - heavy dependence on supplier
Why would you want OSS?

1. **Economic** motives: cost & dependence
2. **Security** reasons: resilience
3. **Political** reasons: transparancy

Emphasis in this talk on points 2 & 3 (while ignoring legal & business issues)

---

**Economic reasons, briefly**

- OSS is often *free*—but installation & maintenance costs remain.
- No consensus on ultimate cost:
  - **optimistic**
  - **pessimistic**
  - **realistic?**

- No dependence on single supplier (lock-in)

---

**III. Openness & Security**

*Code comparison: Lock*

Would you have most **trust** in the locksmith who:

- keeps the working of his locks **secret**, so that thieves cannot exploit this knowledge?
- *publishes* the workings of his locks, so that:
  - everyone can judge how good/bad they are,
  - one relies on the complexity of the keys for protection?
Arguments pro openness

- Fast bug detection and correction—for actively used & supported OSS
- Programmers produce better code when everyone can read their work
- Reduced risk of backdoors
- Flexibility:
  - Minimal & trimmed installations
  - Independence of supplier, also for patching
  - Everyone can assess quality

Closed source beneficial?

- Closedness gives false sense of comfort: “security by obscurity” does not work.
- Implicitly used assumption: what is hidden is correct
- Bugs are found in closed source every day!
- General trust in what is really happening is problematic.

Public security

- Much emphasis currently on:

  State must protect citizens from harm

- More basic:

  State itself must not harm citizens

IV. Openness & Public Administration
Limitations to state power

- Prosecution & police must follow strict rules
- State can be held accountable (can be sued)
- **Freedom of Information Acts** (*WOB* in NL):
  - traditionally focussed on data
  - processes also relevant, esp. when automated
  - Open Source Software (OSS)
  - very natural

Example projects in NL

- Electronic voting: important test case!
  - Voting machines: *closed*, since early 90s
  - Online voting: *Kiezen op Afstand open*, via [www.ososs.nl](http://www.ososs.nl)
  - Online voting: RIES water management.
  - Results & process (but not all code) *open*
- E-authentication
  - A-select from Surfnet *open*
- Phone tapping: *closed*
- Various Linux projects: *open*

Conclusions

- Open software in public administration contributes to:
  - *Security & trust* (if actively supported)
  - *transparency & trust* (inspection only)
- Using OSS is both *natural & appropriate* in public administration . . .
- . . . as is increasingly recognised, in NL and internationally (D, F, UK, China, Brasil, . . .)
- Active community (building) required
- Similar for open standards.
Thanks for your attention!

Questions / Remarks?