Security & Testing

Bart Jacobs

Institute for Computing and Information Sciences – Digital Security
Radboud University Nijmegen

4/11/10, Leiden

Outline

Who is this guy?

- Professor at Nijmegen in software correctness & security (0.0 also at Eindhoven)
- Mix of theoretical and practical work
- Focus on protection & abuse of ICT
- Security research with societal relevance, eg. in **e-passports**, **e-voting**, **road pricing**, **smart meters**, **e-ticketing**
- Occasional role in media
- Author of online book *De Menselijke Maat in ICT*, see `www.cs.ru.nl/B.Jacobs/MM`

Nijmegen involvement in "security testing"

- In the past occasional (commercial) involvement in penetration testing, of:
  - networks and operating systems
  - websites

  Specialised companies are better at this
- Several evaluation rounds for the Dutch e-passport
  - including conformance testing
  - trying out the whole chip command set is doable
- Mifare Classic (in OV-chip) well-known case of
  - "hacking" (as described in the press)
  - "academic security evaluation" (as we like to see it)

- Nowadays involvement in several (architecture) reviews
  - eNIK: electronic national identity card
  - smart metering
  - next generation OV-chipkaart

  More natural role for academia

About testing

- Software testing is "little brother" of software verification
- Testers hate Edsger Dijkstra:

  Testing can only reveal the presence of errors, not the absence of errors
- Traditional testing focus on functionality
- But security is non-functional in nature.

Safety and Security

- Important conceptual distincition. In Dutch more subtle
  - *veiligheid*
  - *beveiliging*
- Security is about
  - regulating access to assets
  - protection against an active, malicious attacker that deliberately wants to undermine a (computer) system
- Safety is about protection against unintended accidents or errors
  - safety involves following "the internal logic"
  - main focus of testing practice
- Think about the difference between eg.
  - Nuclear safety / security
  - Food safety / security

Penetration test example

KPMG Amsterdam has a good computer security group

Some time ago, KPMG was approached by a large firm that had its own secure facilty, with sensitive and strategic data. It had:

- strong physical & electronic security measures
- strict operational security guidelines
- well-trained staff

KPMG was asked/challenged to try and obtain access, either physically or electronically ("red teaming")

They managed to get in as Sinterklaas en Zwarte Piet

(an attack known as: *Trojaanse Schimmel*)

Yes, indeed ...

Computer security is the nicest part of computer science!

(met een hoog kwajongensgehalte)

Serious, difficult questions

1. How do you protect against a deliberate, well-motivated, malicious, resourceful, technically competent, intelligent, creative, socially skilful, patient attacker?
2. Assume you think you have such protection, how do you test it?
   - How to incorporate *out-of-the-box thinking* and *sick minds* into your testing;
   - how to do this systematically?

Rule number one

Security is not an add-on;
it must be in the design, right from the start

Towards proper protection in five steps

1. Make a list of your assets that need protection
   - include the relevant security goals (like CIA = *confidentiality*, *integrity*, *availability*)
   - possibly with an informal ranking of required protection levels (like *high*, *medium*, *low*)
2. Make a threat analysis
   - who may wish try to do undermine which security goal? (*attack trees* may be useful tool)
   - what attack resources are assumed? (eg. funding, strength)
   - what are the risks? (eg. risk = probability * impact)
   - non-technical approach, so far
3. Design a security architecture, describing how to counter the identified threats
   - Still at a high level of abstraction
   - Eg. use strong authentication for employees

Towards proper protection in five steps

5. Get your architecture implemented
   - At this stage the technicalities really matter
   - Software correctness/security often more critical than cryptography
   - Modular approach to be preferred (for easy updates and avoiding lock-ins)
   - Distrust closed/proprietary solutions (like Mifare Classic)
6. Assessment of all of the above points 1-4
   - by an independent party
   - repeated regularly: "security if like fruit: it goes off quickly"
   - what guarantees can you reasonably expect?

Security is not a static state of affaires, but is dynamic

Static versus dynamic evaluation

- Static evaluation, of a non-live system/process
  - Most similar to testing; see more below
- Dynamic evaluation, during live operation
  - Involves elaborate monitoring, incident response & adaptation
  - Necessary for large, open, 'always on' systems (like webbased services, such as e-banking)
  - Topic on its own, not covered here

Two extremes in static evaluation

- Check boxing
  - based on security standards, such as ISO 27000 / NEN 7510 / COBIT / Common Criteria, etc.
  - done by:
    - EDP-auditors, with background in accountancy (EDP = Electronic Data Processing)
    - Computer scientists etc, for instance in code reviews
  - useful, but can easily become a burocratic process in itself
- Penetration testing
  - often done by technically skilful (white hat) hackers
  - there is not really a systematic approach
  - outcome strongly depends on available experience/skills
  - "big picture" often missing

In practice, there is not much more than this

More on check boxing and pen testing

In evaluations the "big picture" is needed:

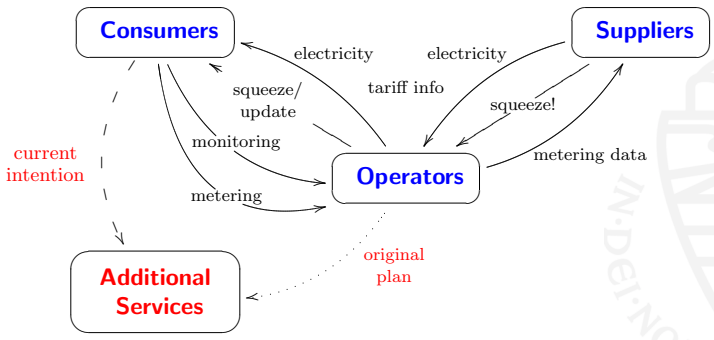
1. Check boxing must be risk based
   - with risks as existing in a particular situation
   - ...and identified in the five-step approach
2. Penetration testing must be threat based
   - Not every intrusion is necessarily harmful

New e-meter picture

Why smart electricity (and gas/water) meters?

- Basis in EC directive (2006/32/EC)
- Remote reading, to prevent expensive home visits
- Remote management (change supplier etc.)
- Remote disconnect:
  - to deal with arrears (non-payment/fraud)
  - emergency supply management ("code red")
- Intelligent grid management, for optimisation, esp. with eg.
  - electric car charging (sudden high demand)
  - clients who also produce, etc.
- Energy preservation, via better insight in own consumption
- Additional (commercial) services, based on customer profiles
  - typically by third parties

Flow schema essentials



Sensitive issues

How much/often metering / monitoring / control / services info

Old and new meters

- Traditional electricity meters have tamper proof hardware protection, so that:
  - customer cannot change meter (downwards)
  - supplier cannot change meter (upwards)

  Intuitively this two-way protection, with local data storage, is well-understood.
- New, smart meters offer no such protection. Operator can:
  - read/change data at a distance, at any moment
  - change all software (& cryptographic keys)
  - store all data centrally, out of context, and pass it on
- Energy sector reply: *we don't do such things; you can trust us!*
  - that is what Google/Apple/... used to say
  - what if the operator becomes Chinese (state) owned?
- What if a customer challenges his bill in court, claiming manipulation by the operator? How will the judge rule?

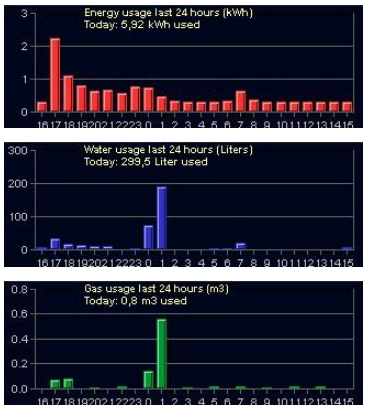
Timeline

1. **Summer 2008**
   New utility law adopted by Parliament (Second Chamber)
   - making smart meters compulsory,
   - meter recording *every 15 minutes* (daily read-out, with opt-in for every 15 min.)
   - remote squeeze/disconnect possible
   - clients can also supply energy (solar/wind/...)
2. **Spring 2009**
   Senate (First Chamber) objects with privacy/security concerns
   - asks for removal of compulsary character
   - positive impact: sector finally wakes-up
3. **Currently**
   Update of law (*novelle*) sent to parliament (debated yesterday)
   - obligation to accept meter will disappear
   - security requirements strengthened (in AMvB)

Privacy concerns: Pamphlets (in Dutch only...)

See also: `wijvertrouwenslimmemetersniet.nl`

Privacy concerns: example readings (`bwired.nl`)



Privacy concerns & personal security

With 15 minute & daily meter reading ...

- Operator/producer employees see when I'm at home or not
- Useful info for burglars
  (can use blackmail/bribery/infiltration/hacking to get such info)
- Why am I exposed to this new vulnerability?
- Privacy is important for personal security!

Unanswered questions

1. Do smart grid plans make sense with the current poorly mapped (partially unknown) infrastructure?
   - cables and wirings are not all known
   - part of the consumption is not measured (eg. public lighting)
2. How much aggregation can be done in a smart grid
   - at household level
   - at neighbourhood ("data concentrator") level?
3. How much behavioural data should operators get?
   - knowing when I want to charge my electric car is useful to them
   - knowing when I am (or will be) ill is also useful
   - ... and for how long (so why not give them my DNA??)

Data protection aspects of behavioural data poorly developed

Denial of service (DOS) concerns

- Nicely illustrated in *Delta Lloyd Hackman* Video advertisement (2005)


- National security / infrastructure risk
  (exploitable by blackmailers / terrorists / hostile nations; see stuxnet)
- Why do we introduce these vulnerabilities?

Approach of the sector & ministry

- Non-approval in Senate has been beneficial
  - sector has woken-up, cooperates, and takes privacy & security issues seriously
  - NL now thought leader in Europe (on this topic)
- Chosen approach: combination of
  - improved technical security
    (but meter manufacturers are slow/unwilling/incompetent)
  - organisational requirement: privacy paragraph in annual reports
  - transparancy of communication
  - Lots of evaluation and testing, of e-meters and infrastructure!!

Final remarks

- Little scientific theory available on security evaluation
  (in comparison to software evaluation)
- Dynamic evaluation becomes the norm
- Best practices in static evaluation are:
  - check boxing, based on international standards
  - penn testing
- Architecture is politics: design of information systems is highly sensitive
  - information is power
  - who has access to which information determines power relations & vulnerabilities
  - little understanding/consensus on dealing with behavioural data
- Privacy & security issues can make or break large ICT-projects (OV-chip, EPD, e-meters, road pricing etc)

Thanks for your attention! Any questions/remarks?