Research Workshop on Challenges for Trusted Computing

Tuesday 2nd September 2008

Workshop summary

Programme

16:00-16:10 Opening remarks

16:10-16:40 *Challenges for trusted computing*: Shane Balfe and Eimear Gallery (ISG, Royal Holloway, University of London, UK)

16:40-17:10 *Advances on PrivacyCAs*: Martin Pirker, Ronald Toegl, Daniel Hein, and Peter Danner (IAIK, Graz University of Technology, Austria)

17:10-17:40 *Attacking the BitLocker Boot Process*: Sven Tuerpe, Andreas Poller, Jan Steffan, Jan-Peter Stotz, and Jan Trukenmueller (Fraunhofer-Institute for Secure Information Technology, Darmstadt, Germany)

17:40-17:55 Discussion

17:55-18:00 Wrap-up

Proceedings!

- An electronic version of the workshop handout, including written-up versions of all three talks, is available via the ETISS 08 website.
- If the organisers allow, I plan to also make this final presentation available via the ETISS website.

Challenges for trusted computing:
Shane Balfe and Eimear Gallery

- Discussion of a range of practical obstacles to deployment of full range of TC functionality.
- Issues discussed include:
  - TC PKI problems, including bootstrapping and revocation issues;
  - practical attestation questions;
  - backwards compatibility issues;
  - usability problems.
- Observed in talk that many problem disappear in a single domain environment (e.g. for corporate use).
- Research questions:
  - would be interesting to do a study of one particular use of TC in a multi-domain environment – might be 'do-able' next step;
  - What level of 'retrofitting' of credentials to a trusted platform is possible, and how useful would it be?

Advances on Privacy CAs:

Martin Pirker, Ronald Toegl, Daniel Hein, and Peter Danner

- Experiences on building and operating open-source Privacy CA described.
- This was the first public Privacy CA service (part of OpenTC project).
- Some interoperation issues identified with parallel open source developments.
- New version of software (much easier to install and run) available soon.
- Problem identified that AIK certification request cannot use standardised certificate management syntax (e.g. PKCS/CMP), because of problems with providing proof of possession (POP) [private part of AIK cannot be used to sign arbitrary data, for obvious reasons].
- Research questions:
  - Can we modify restraints on AIK use to allow use of AIKs with standardised protocols?
  - What other issues arise in providing practical PKI services to support TC?

Attacking the BitLocker Boot Process:

Sven Tuerpe, Andreas Poller, Jan Steffan, Jan-Peter Stotz, and Jan Trukenmueller

- Goal of work described was to analyse security of BitLocker against *targeted attacks*.
- [BitLocker only claims to resist *opportunistic attacks*].
- Range of possible attacks described.
- Provides understanding of limits of BitLocker security.
- Planned work on realising some of the attacks.
- Research questions:
  - How might BitLocker be modified to better resist these attack scenarios?
  - Similar analyses of other applications of TC technology (implemented or just proposed) would be very interesting.