Energy Considerations in the Design of Secure Systems

N. Asokan

Security vs. Energy consumption

- Mobile devices are energy-constrained
  - New type of DoS: “Sleep deprivation torture”
- Security mechanisms are energy-intensive

- This conflict leads to nice research topics
  - How exactly does the conflict manifest? (Topic 1)
  - How to design for optimal tradeoffs? (Topic 2)
  - Can this conflict be a blessing-in-disguise? (Topic 3)

Topic 1: Energy Consumption Profiles

- What primitives/operations are expensive?
  - Computation
  - Memory access
  - Transmission and reception
- System issues

- Starting points: [1,2]

Topic 2: Energy-optimal design

- How to optimize software and hardware implementation of cryptographic primitives?
- How to design energy-optimal protocols and systems?
- Optimizing crypto implementations for energy consumption may open power-analysis vulnerabilities
  - Similarly, protections against side-channels may drive up energy consumption
- Starting points: [3,4] (software) [5,6] (hardware)

Topic 3: Energy constraint as a security measure

- Attackers have to live with the same constraints
- Unusual energy consumption pattern may imply an intrusion

- Starting points: [7,8]

References

1. Potlapally et al, “A study of the energy consumption characteristics of cryptographic algorithms and security protocols”, IEEE TMC, Feb 2006
   - http://ieeexplore.ieee.org/search/wrapper.jsp?arnumber=1563998
2. Haverinen et al, “Energy Consumption of Always-On Applications in WCDMA Networks”, IEEE VTC 2007
   - http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=4212428&arnumber=4212635&count=655&index=206
3. Potlapally et al, “Optimizing Public-Key Encryption for Wireless Clients”, ICC 2002
   - http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=997014
4. Großschädl et al, “Energy-Efficient Software Implementation of Long Integer Modular Arithmetic” CHES 2005
   - http://www.iaik.tugraz.at/research/publications/2005/CHES2005_EES.pdf
5. Goodman et al, “An Energy-Efficient Reconfigurable Public-Key Cryptography Processor”, IEEE JSSC 2002
   - http://ieeexplore.ieee.org/xpls/abs_all.jsp?tp=&arnumber=962304
6. Benini et al, “Energy-Aware Design Techniques for Differential Power Analysis Protection”, IEEE DAC 2003
   - http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1218775
7. Jacoby et al, “Using Battery Constraints within Mobile Hosts to Improve Network Security”, IEEE S&P Magazine, Sept-Oct 2006
   - http://ieeexplore.ieee.org/search/wrapper.jsp?arnumber=1704780
8. Martin et al, “Denial-of-Service Attacks on Battery-powered Mobile Computers”, PerCom 2004
   - http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1276868