Report from the "Smart Object Security Workshop 23rd March 2012, Paris"

Presenter: Hannes Tschofenig

Workshop Organizers

- Hannes Tschofenig
- Jari Arkko
- Carsten Bormann
- Peter Friess
- Cullen Jennings
- Antonio Skarmeta
- Zach Shelby

Thomas Heide Clausen
(Host)

Workshop Info

- Webpage: http://www.lix.polytechnique.fr/hipercom/SmartObjectSecurity/
- Papers and slides will be copied to this website after the meeting. Currently, they are temporarily here:
  - Position papers: http://www.tschofenig.priv.at/sos-papers/PositionPapers.htm
  - Agenda & slides: http://www.tschofenig.priv.at/wp/?p=874

Workshop Goals

- We had a gut feeling that we might have problems with securing smart object networks.
  - Had received input already in the March 2011 Prague IAB Smart Object workshop.
- Bring together implementation experience, application requirements, and researchers and protocol designers
- What deployment experience is there? What credential types are most common? What implementation techniques make it possible to use Internet security technology in these devices? What are the challenges?

Requirements & Economics

- Requirements for each application domain differ
  - also driven by the business models and number of devices that need to be provisioned
- Understanding of threats differs between the different communities:
  - Attacks are not just from neighbor's kids
  - Also, e.g., taking-the-grid-down attacks
  - Installation by regular people

Implementation Experiences

- We think we can use the existing crypto algorithms
- We probably can use the existing protocols (delta a few minor extensions).
- Lots of implementation work being done by the participants (e.g., TLS, DTLS, PANA, EAP, HIP) but still more investigations needed.
- Important aspect:
  - Focus on the system!
  - Look at the code size of the entire system (including provisioning, authorization, config)
- Focus on what to optimize for various among the different deployments
  - Energy consumption, code size, main memory size, over-the-wire bandwidth

Authorization Discussion

- Many questions were raised, for example:
  - Which device is authorized to talk wo which other device?
  - What is the role of the human?
  - Where is the policy decision point and the policy enforcement point in the network?
  - What is the granularity of the authorization decision?
  - What needs to be standardized?
- Seems to be the most challenging aspect.
- Not clear whether there is any IETF standards work needed?

Imprinting Discussion

- There is a limited set of solutions
  - Based on the hardware support of devices: buttons vs. labels vs. LEDs, multicast discovery, online network availability, ...
- Again, the threat assumptions matter and who is supposed to do the credential provisioning.
- A fun area to design protocols in
  - Detailed discussion about a specific proposal from Cullen Jennings.
  - http://www.tschofenig.priv.at/sos-papers/CullenJennings.pdf

Next Steps

- Document the implementation experience in the LWIG group.
- A few already ongoing security standards activities (e.g., TLS raw public keys, JOSE on JSON encryption and signing).
- Maybe discussions around imprinting protocols in the IETF in the future.
- There is no single security architecture for smart objects (not even a small number of them).