Hardware-rooted Trust for Secure Key Management and Transient Trust

J. Dwoskin, R. Lee, "Hardware-rooted Trust for Secure Key Management and Transient Trust", in *Conf. on Computer and Communications Security (CCS 2007)*, pp. 389-400, 2007.

Presented by:
Ali Al-Sarraf

Article Summary

- It propose a minimum new hardware that act as an addition to the microprocessor of any portable device and protect its cryptographic keys and secret information's.

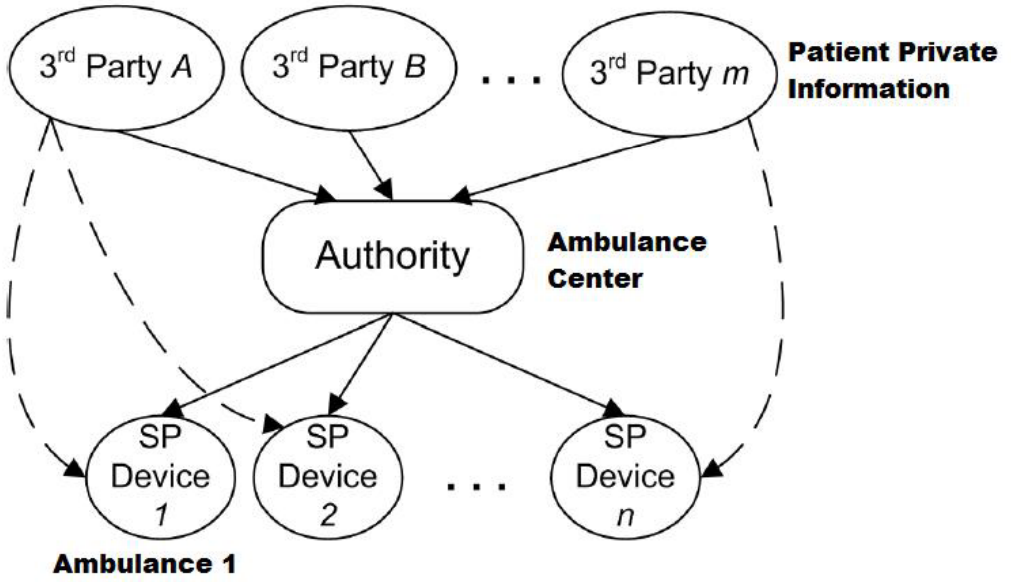
- The main idea is, the portable device are owned by a central authority that can give transient access to its users to the secret information in the device in certain times by using the propose hardware.

Appreciation 1

- A detailed technical explanation of the architecture and the functionality of the propose hardware "authority -*mode SP (Secret-Protecting)*" .

Appreciation 2

- They offered some good crisis scenarios that shows how their trust model work in these scenarios.



Criticism 1

The drawback about this article

- The threat model only covers operational threats and not development threats.
- Which means, the hardware was developed in a secure trusted environment.

Criticism 1(Continue..)

- For example:
  - The hardware has been initialized by a trusted authority.
  - They depend on other trustworthy system (e.g. a security kernel and secure I/O drivers) to assist with their system.

Criticism 2

- They considered their problems as "orthogonal issues" to their designs, for that they have not discuss it in this paper.
- But they claims that any attacks on their model is detectable but they have not provide a recovery solution.

Question?

- How do you define a trustworthy system?