Physically Restricted Authentication and Encryption for Cyber-physical Systems

Michael Kirkpatrick, Elisa Bertino
Purdue University

Frederick Sheldon
Oak Ridge National Laboratory

DHS: S&T Workshop on Future Directions in Cyber-physical Systems Security

July 23, 2009

Key Problems for CPS

- Data provenance and integrity
  - Origin of data is known
  - Changes are tracked
- CPS vs. traditional computing
  - Decentralized
  - Not desktop/server model
  - Continuous, not discrete
- Goal is to restrict access to trusted devices
  - First, one must identify the device!

Authorization Mechanisms

- Physical key
  - Continuous
  - "Clonable"
- Cryptographic key
  - Discrete
  - Clonable
- CPS identification
  - Based on continuous, physical properties
  - Can be discretized
  - Unclonable

OAK RIDGE National Laboratory

Physical Unclonable Functions (PUFs)

- One-way function
  - Given challenge C_i, response is R_i
  - R_i cannot be predicted or duplicated
  - R_i continuous, but can be made discrete
- SRAM-based PUFs
  - SRAM bits start in the same state (0 or 1) with high probability
    - Not affected by previous computation
  - C_i is a range of memory locations in SRAM

OAK RIDGE National Laboratory

Usage of Discretized PUFs

- Secure cryptographic key storage
  - Given key K, create and store X = K XOR R_i
  - X can be stored in plaintext (!)
- Cryptographic key generation
  - For ECC, point P, R_i is private key, $K_{pub} = R_i * P$
  - For Feige-Fiat-Shamir, public identity commitment is R_i^2 mod n

OAK RIDGE National Laboratory

Advantages of PUFs

- SRAM is everywhere
  - ASICs, processor caches, FPGAs, micro-controllers, embedded devices
  - Devices without TPM or tamper-proof hardware
- Cryptographic key exists only when needed
- Bound to the hardware itself
  - Uniquely identifies hardware instance

OAK RIDGE National Laboratory

Challenges and Open Problems

- No tool support
  - PUFs have been created just as proof-of-concept
- Delicacy of (C_i,R_i) and revocation
- New protocols designed specifically for PUFs
  - Use function as ZKPK secret
- Heterogeneous devices for CPS
  - PUFs for different types of hardware?
- Scalable identity management for large sensor networks

References

- B. Gassend, D. Clarke, M. van Dijk, S. Devadas, "Controlled Physical Random Functions." In *Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC)*, 2002.
- J. Guajardo, S. S. Kumar, G.-J. Schrijen, P. Tuyls, "Physical Unclonable Functions and Public-key Crypto for FPGA IP Protection." In *International Conference on Field Programmable Logic and Applications*, 2007.
- S. S. Kumar, J Guajardo, R. Maes, G.-J. Schrijen, P. Tuyls, "Extended Abstract: The Butterfly PUF Protecting IP on Every FPGA." In *IEEE International Workshop on Hardware-Oriented Security and Trust (HOST)*, 2008.
- G. E. Suh, S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation." In *Proceedings of the 44th IEEE Design Automation Conference (DAC)*, 2007.