Embedded Authentication

Patrick Schaumont, Circuit Cellar, January 2013

Jeremy Hines
UNCC Spring 2013
Advanced Embedded Systems

Agenda

- Introduction
- Motivation
- Security Obstacles
- Authentication Methods
- Implementation
- Conclusion

Introduction

- Circuit Cellar, January 2013
- Patrick Schaumont
- Three methods of implementing authentication protocols in embedded systems

Motivation

- Black Hat 2012 Hotel Room Door Hack - Cody Brocious
- 4 Million Locks Vulnerable
- Less than 1 second to unlock any door
- COTS Hardware

Motivation

- “Hackers can unlock cars via SMS” – 2011
- “Black Hat hacker details lethal wireless attack on insulin pumps” – 2011

Security Obstacles

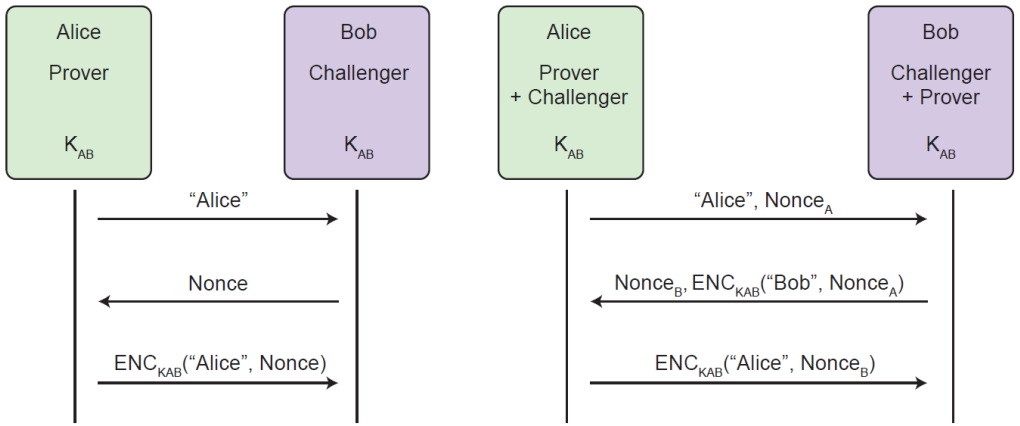
- Cost
- Lack of knowledge
- Memory Constraints
- No standard practice
- Difficult to implement after production

Authentication Methods

- HMAC-based protocol on chip
- HMAC-based protocol on separate chip
- Public-key Cryptography on separate chip

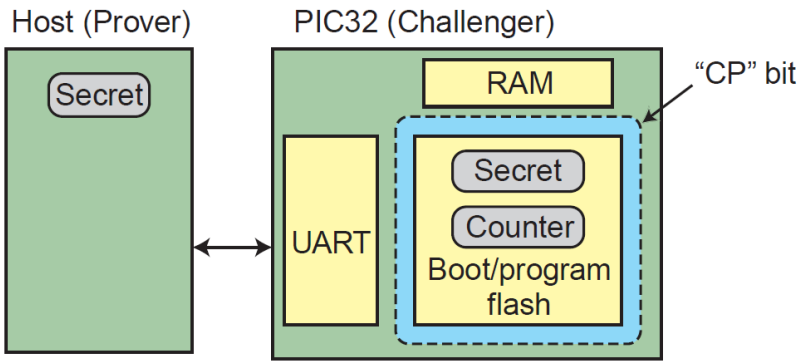
Basic Authentication

- One-way
  - Challenger/Prover have shared secret
  - Prover sends public identifier to Challenger
  - Challenger sends nonce
  - Prover encrypts public identifier and nonce using shared secret
  - Challenger performs same encryption and compares with Prover encrypted response
- Mutual
  - Both systems act as both Challenger and Prover



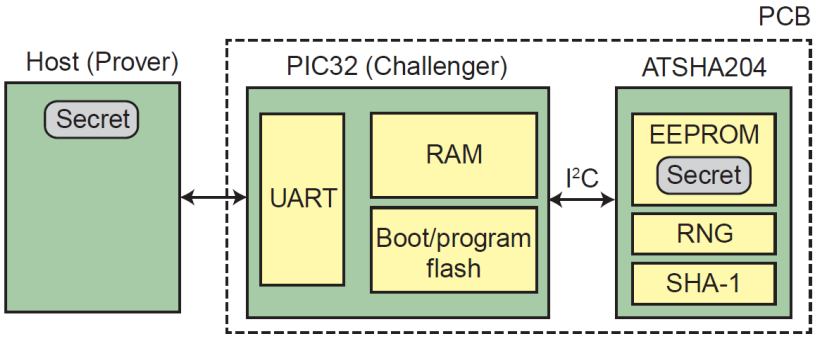
PIC32 Implementation

- HMAC protocol implemented on single chip
- Secret & Counter must be stored in flash
- Program memory can be read via software
- Vulnerable if secret is discovered



ATSHA204

- Read protected non-volatile memory
- Random Number generator
- SHA-1 algorithm hardware



Origa SLE95050

- Asymmetric key authentication device
- Chip contains secret key that never leaves the package
- Releases matching public key
- More scalable since challenger only handles public-key values

Conclusion

- Necessity of embedded security
- Obstacles to security implementation
- Basic authentication methods
- Implementation of authentication

References

- Schaumont, Patrick. "Embedded Security." *Circuit Cellar*, January 2013, 54-58.
- Koopman, Philip. "Embedded System Security." *IEEE Computer*. no. July (2004): 95-97. http://www.ece.cmu.edu/~koopman/security/koopman04_embedded_security.pdf (accessed February 18, 2013).
- Infineon, "Origa SLE95050." Accessed February 18, 2013. http://www.infineon.com/export/sites/default/media/press/Image/press_photo/ORIGA.jpg.
- Anthony, Sebastian. "Black Hat hacker gains access to 4 million hotel rooms with Arduino microcontroller."*Extreme Tech* (blog), July 25, 2012. http://www.extremetech.com/computing/133448-black-hat-hacker-gains-access-to-4-million-hotel-rooms-with-arduino-microcontroller (accessed February 18, 2013).
- Anthony, Sebastian. "Black Hat hacker details lethal wireless attack on insulin pumps." *Extreme Tech*(blog), August 5, 2011. http://www.extremetech.com/extreme/92054-black-hat-hacker-details-wireless-attack-on-insulin-pumps (accessed February 18, 2013).
- Anthony, Sebastian. "Hackers can unlock cars via SMS."*Extreme Tech* (blog), July 28, 2011. http://www.extremetech.com/extreme/91306-hackers-can-unlock-cars-and-meddle-with-traffic-control-systems-via-sms (accessed February 18, 2013).