Implementation Experiences on Public Key Crypto, Small Platforms, and CoAP

Mohit Sethi

Ericsson Research / Aalto University

Jari Arkko, Ari Keränen, Heidi-Maria Rissanen

Ericsson Research

www.arkko.com/publications/draft-aks-crypto-sensors-02.txt

PK Crypto on Tiny Devices?

- We set out to
  - Find out what public domain libraries exist
  - See how well they work in small platforms (Arduino)
  - Demonstrate the technology with COAP
- Doable on 8-bit CPUs? Definitely, at least for some apps
- Also definitely difficult in some other cases

What's hard and what's easy?

- **Libraries**: Easy. There are several. But with major variations!
- **Memory**: Easy. Can be very small but is at least reasonable
- **Speed**: Harder. Can be very fast with the right library, but can also be unreasonably long

Observations: 1) this gets easier with new CPUs 2) transmitting a bit over wireless is more expensive than any processing anyway

ECC and RSA on Arduino

Library	ROM
AvrCryptolib	3.6 KB
Wiselib	16.0 KB
TinyECC	18.0 KB
Relic	29.0 KB

Algorithm	Library	RAM	Time	
RSA-512	AvrCryptolib	320 B	25.0 s	
RSA-1024	AvrCryptolib	640 B	199.0 s	
ECC 128r1	TinyECC	776 B	1.8 s	
ECC 192k1	TinyECC	1008 B	3.4 s	
NIST K163	Relic	2804 B	0.3 s	← ~ RSA 1024!
NIST K233	Relic	3675 B	1.8 s	← ~ RSA 2048!

Example Application for CoAP