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

<table>
<thead>
<tr>
<th>Library</th>
<th>ROM</th>
</tr>
</thead>
<tbody>
<tr>
<td>AvrCryptolib</td>
<td>3.6 KB</td>
</tr>
<tr>
<td>Wiselib</td>
<td>16.0 KB</td>
</tr>
<tr>
<td>TinyECC</td>
<td>18.0 KB</td>
</tr>
<tr>
<td>Relic</td>
<td>29.0 KB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Library</th>
<th>RAM</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-512</td>
<td>AvrCryptolib</td>
<td>320 B</td>
<td>25.0 s</td>
</tr>
<tr>
<td>RSA-1024</td>
<td>AvrCryptolib</td>
<td>640 B</td>
<td>199.0 s</td>
</tr>
<tr>
<td>ECC 128r1</td>
<td>TinyECC</td>
<td>776 B</td>
<td>1.8 s</td>
</tr>
<tr>
<td>ECC 192k1</td>
<td>TinyECC</td>
<td>1008 B</td>
<td>3.4 s</td>
</tr>
<tr>
<td>NIST K163</td>
<td>Relic</td>
<td>2804 B</td>
<td>0.3 s</td>
</tr>
<tr>
<td>NIST K233</td>
<td>Relic</td>
<td>3675 B</td>
<td>1.8 s</td>
</tr>
</tbody>
</table>

~ RSA 1024! ~ RSA 2048!
Example Application for CoAP

Delegation:
- Delegate work to a mirror
- No need to stay awake

COAP GW
(mirror proxy)

Data-object security:
- Verifiable by all nodes
- Verifiable at any time
- JOSE, SENML, ECC

SSH-like leap of faith:
- No configuration!
- Supply PK in mirror registration
- Ensure data updates signed by the same key

Arduino sensor
(CoAP client)

Application Software
(CoAP client)