Optimized Resource Access Control in Shared Sensor Networks

Christophe Huygens, Nelson Matthys and Wouter Joosen

christophe.huygens@cs.kuleuven.be

Mobisec 2010
Quick overview

- Intro
- Problem domain: long-lived WSN settings
- Problem analysis
- Contribution
- Results and Q&A
Monolithic – security problem
Real-world – extra security issues

- Harbours
- Shipping Co.
- Sales Co.
- WAREHOUSE
- INTERNET
- APPLICATION ADMIN.
- SYSTEM CONTROL
- BACK END SYS.
Federating and sharing

- Current WSN research = single applications
- Typical business usage scenarios are different
  - Devices of different owners must cooperate to achieve objectives > federation - logistics
  - Devices must offer services to multiple applications of different owners > sharing – building management
- F/S security challenge complements scale, dynamics, device heterogeneity, locality
- Beyond monolithic security requirements
Contribution

- Analysis of the security gap of *sharing*
- Detailed requirements for WSN access control
- Solution for WSN access control
  - Operational model
  - Reference monitor
  - Integration strategy
- Evaluation
Shared WSN Security stack

- Access control
- Process isolation
- Controlled cooperation

- Secure routing
- Key management
- Crypto
- Physical

Done
Operational Model
Resource Access Control Req’s

- Traditional:
  - Complete mediation
  - Isolation
  - Verification

- Applications and infrastructure are decoupled

- New setting of long-lived WSN
  - Energy conservation

May 28, 10
Optimized Resource Access Control in Shared WSN – Mobisec 2010
Resource Access Control Req’s

- Decoupling
  - Stakeholder decoupling, transition to sharing
  - Segregation of duties (SE: separation of concerns)
  1. No impact on Application owner development

- Energy considerations
  2. Enable light-weight run-time change for Administrative owner
  3. Selective deployment
  4. Maximize work in resource-rich environment
Solution

1. No impact on Application owner development
   *Aspect-oriented instrumentation*

2. Enable light-weight run-time change for Adm. owner
   *Small policy-driven engines*

3. Selective deployment
   *Selective instrumentation*

4. Maximize work in resource-rich environment
   *Pre-deployment instrumentation*
Operational Model
Policy engine

- Match (object, operation) = reference monitor
- Decision tree = policy
- Trusted Computing Base implements RM
- TCB = policy engine + control flow + system sec.
- Control flow is easy to implement (WSN security)
- Policy engine is challenging on WSN nodes
Policy Statements

- ECA semantics
- Snippet

```
policy "example access control" {
  on accessrequest req
  if(req.applicationID == "iid7" &&
      req.resourceId == "lightsensor" &&
      req.operationId == "get")
  then allow
}
```
Instrumentation

- ... intercept request in original app code on node
- ... intercept communication of interaction
- Instrumentation of app code
  - Byte code instrumentation of app code
  - ... when submitted to Admin. Owner
  - ... before deployment on node
  - ... using AO techniques (AspectJ)
J2ME Instrumentation tool chain

```
package org.sunspotworld;
import com.sun.squaawk.*;
public aspect intercept {
    private Isolate isolate; private int iid;
    before(LightSensor ls): target(ls) && call (* getAverageValue(..)) {
        isolate = com.sun.squaawk.Isolate.currentIsolate();
        iid = isolate.getId();
        if (!engine.allow("iid"+iid,"lightsensor","get")
            {throw new IllegalAccessException();})
    }
```

May 28, 10
Optimized Resource Access Control in Shared WSN – Mobisec 2010
Evaluation

- **Policy engine**
  - Prototype on Sun SPOT (180 MHz ARM920T 512K)
  - Policy item = 142 Bytes on transmit
  - Policy item = 420 Bytes on node
  - Engine code = 28 kBytes (rich engine)
  - <> Atmel ATmega1284p Raven 16K
  - Evaluation = 1 to 2 ms

- **Instrumentation**
  - AspectJ run-time can be stripped to 2.3 kBytes
Results – Q&A

- Energy optimization
  - Life-cycle: selective pre-deployment activities are low-cost
  - Different abstractions for run-time and development: policy is suitable R/T abstraction at low-cost versus OO/CBSE

- SE perspective
  - Abstractions align well with different stakeholder views
  - Low coupling particularly for CBSE (=non-intrusive development)

- Elegant solution to Resource Access Control

- Challenges:
  - Equilibrium: resource consumption <> engine size
  - Choosing the right abstraction can be hard
Backup slides
Research background

- Middleware challenges for long-lived WSN
  - Each stakeholder in his part of the life cycle needs optimal abstraction
  - Abstraction > middleware mechanism
  - Mechanisms have different cost
  - One-size fits all is suboptimal
  - How can we integrate these multiple mechanisms

- Security problem presented is case study