
M. Pugliese\textsuperscript{1}, A. Giani\textsuperscript{2}, L. Pomante\textsuperscript{1}, F. Santucci\textsuperscript{1}

\textsuperscript{1}Center of Excellence DEWS
University of L’Aquila – ITALY
marco.pugliese@ieee.org, \{luigi.pomante, fortunato.santucci\}@univaq.it

\textsuperscript{2}Dep. of Electrical Engineering and Computer Sciences
University of California at Berkeley
Berkeley – USA
agiani@eecs.berkeley.edu
Outline

• Introduction
• Cross-Layer Platform-based Design
• The Cryptographic Scheme: TAKS
• The Intrusion Detection System: WIDS
• Secure Platform Architecture
• Conclusion and Future Works
Introduction

- Provide secure monitoring services, supported by flexible and cheap systems, in areas where ordinary networks are unsuitable is one of today interesting challenges.
- Wireless Sensor Networks (WSN) represent a promising technological solution but resource constraints and exposure to external attacks could limit their employment.
- **The problem:** design a secure execution environment over WSN.
- **Our solution:** smart adaptation into WSN of traditional security techniques and supply to performance degradation with the adoption of advanced system architectures (CL and PBD) and the application of optimization criteria in node deployment and network topology management (Topology Optimization, see poster “Optimal Wireless Sensor Networks Topologies for the support of Mobile Agent-based Monitoring and Alerting Applications”).
Cross-Layered Platform-Based Design

• Here Cross-layer (CL) results in the interplay between network layer (topology management and routing protocol) and presentation layer (mobile agent based execution environment for distributed monitoring applications). Applied to security, an important benefit of CL mechanism is the exploitation of the interplay between different security measures in different layers to provide a enforced security service to applications.

• Here Platform-based design (PBD) [21] results in the availability of a software platform where the internal structure is composed by “interconnected” SW Components which represent abstractions of the wired hardware components. At presentation layer, a platform behaves as a middleware, i.e. Application Execution Environment (AEE).

• In next slide the Secure Platform is a secure CL-BPD execution environment for applications over WSN.
Cross-Layered Platform-Based Design

• Architecture of the proposed framework:
Secure Platform Components

• Intrusion Detection System (IDS)
  – Based on \textit{Weak Process Models} (WPM-based IDS, WIDS).
  – WPMs are a non-parametric version of HMMs wherein state transition probabilities are reduced to rules of reachability.
  – The estimation of a threat in the case of weak processes is greatly simplified and less demanding for resources.
  – The \textit{most probable state sequence} generated by the Viterbi algorithm [8] for HMM becomes the \textit{possible state sequences} for WPM.

• Cryptographic Scheme (CS)
  – Based on \textit{Topology Authenticated Key Scheme} (TAKS).
  – TAK is a symmetric key computed using asymmetric mechanism.
    • TAK local component (private) and TAK transmitted component (public)
  – TAKS is supported by TGMP (TAK Generation Management Protocol).
WPM Model

State

Threat Observable

Score associated to WPM transition

State path associated to an abnormal behaviour

State class

Observation step

The corresponding (weighted) state trace

State class

Score associated to WPM transition

State path associated to an abnormal behaviour

State class
Security Analysis Results for WIDS

• **Test for alarm mis-detection (False Negatives, FN).**
  If WPM is structurally well-defined then virtually zero FNs because for each possible abnormal behaviour is associated a state path in WPM. *Normality modelled as the absence of abnormality*. To reduce FNs:
  – Design a number of state paths associated to abnormal behaviors starting from each state.

• **Test for false alarm detection (False Positives, FP).**
  If Anomaly Rules are logically well-defined then virtually zero FPs because no “undecidable” threat observables (therefore “undecidable” states) can be produced. To reduce FPs:
  – Insert truly (even trivial) states associate to “truly” threat observations in WPM branches where the leaf state is in UPA.
  – Introduce a further state class, the UPA class, and apply ad-hoc (lighter) countermeasures in case an alarm had been generated.
TAK Generation Mngt Protocol

\[ t_j \cdot k_{tj} = 0 \]
\[ \text{TAK}_i = f(k_{li}, k_{tj}) \]

\[ \text{SETUP}(k_{tj}) \]

\[ (1) \]

\[ t_i \cdot k_{ti} = 0 \]
\[ \text{TAK}_j = f(k_{lj}, k_{ti}) \]

\[ \text{SETUP}(k_{ti}) \]

\[ (2) \]

\[ \text{TAK-ciphered link} \]

\[ \text{RELEASE}_\text{ind}(n_i \neq \text{CH}) \]

\[ \text{REVOKE}\text{Key}(\text{TAK}) \]

\[ \text{TinySec} \]

\[ \text{TRANSMITTED Key Component} \]

\[ \text{LOCAL Key Component} \]

\[ \text{ARCHEA} \]

\[ \text{LCD}_i \]

\[ n_i \]

\[ \text{LCD}_j \]

\[ n_j \]
Security Analysis Results for TAKS

- The entropy per binit associated to TAK is \( \approx 1 \) (i.e. pseudo-random sequence) when \( q >> N \) [18] with \( q = 2^k \), where \( k \) is the key length in binit and \( N \) the nodes in WSN.

- **Single node security.** How difficult is to compromise a single node (single node security)? In [18] we show that this reverse problem is harder than solving the Discrete Logarithm Problem [15].

- **Network security.** How many nodes should be compromised to gain enough information to break TAKS (security level in the network)? In [18] we show that is \( \approx N \) when \( q >> N \).
Secure Platform Architecture

Applications

Application $A_1$  Application $A_2$  .......  Application $A_n$

Application Execution Environment (AEE)

Shared memory

MW services

SW component

TAKS  WIDS

Local memory

Underlying WSN Deployment

Conclusion and Future Works

This work is an intermediate result of the internal project WINSOME (Wireless sensor Network-based Secure system for structural integrity Monitoring and Alerting) being developed at DEWS labs aimed at the implementation of a CL-BPB secure framework for mobile agents applications (e.g. monitoring and alerting) supported by a MicaZ sensor network.
WIDS Component

- Shared Memory
- Comms
  - TGMP msgs
  - ARCHEA msgs
- AG
- WML
- TM
- ADL
  - AR
  - LCD
  - Net Manager

Connections:
- Shared Memory to AG: $o^k$, $al[s^k]$
- AG to WML: $Hp_x^k$
- WML to TM: $o^k$
- TM to Comms
- Shared Memory to Comms
- ADL to Net Manager
- LCD to Net Manager
Alarm Generation (AG) sub-Component

Shared Memory

al[s^k]

Score Computation

Hp_x^k

Trace Estimation

Free_x^{i<k}

AG

WML

TM

Hp_x^k

Free_x^k
Threat Model (TM) sub-Component
TAKS Component

TAKS

- Network Topology Authentication
- Key Generation
- ReplaceKey
- RevokeKey
- TinySec

TGMP

- TGMP msgs
- cm[s]

Shared Memory

AR

TAKgen
ok/ko

RELEASE_ind(n_i≠CH)

Net Manager

Comms

LCD

k_{tj} \sigma(j)

k_{lj}
References


AICA 2010, L'Aquila, Oct 1st 2010
References


