Agenda

- Intro
- What are MANETs and WSNs?
- Problem Space and Challenges wrt to Security

- Drinking @ BJ’s Restaurant & Brewary, across the street
Who am I?

- Senior Principal Engineer, Office of the CTO, Symantec
  - Approaching 10 years @ Symantec
- Development @ QA engineering background
- Prior to Symantec: operating systems & networking protocols
- OWASP LA board member
- Father of three (future world changing persons)
  - Note to self: robot programming and first Emails...
- Computer Science Ph.D. student
- Famous for long introductions
What are MANETs?
Mobile Ad-hoc Networks

- Do not rely on an existing infrastructure
- Wireless communications
- Mobile nodes (constantly changing topology)
- Nodes must be able to relay traffic, as communicating nodes might be out of range
- MANET can be self-forming and standalone or attached to other networks
MANET vs. "Traditional" Wireless Network

Mobile ad-hoc network

Wireless, fixed network
MANET Example: Vehicular Ad-Hoc Network (VANET)
LIKE ELEPHANTS marching trunk to tail, each vehicle in a platoon takes cues from the vehicle just in front of it. Unlike an elephant, though, the vehicle also communicates directly with the leader in order to anticipate any turns or braking action.

A driver finds a platoon that’s going the right way by selecting a destination and following the navigation system’s directions. The driver joins the platoon at the rear, and the system takes control.

When one car leaves the platoon, the followers automatically close the gap and continue until their drivers decide to peel off and go their own way.

Drivers in the following vehicles relax. When the platoon approaches their various destinations, each driver pulls to the side and drives on independently.

A professional drives the platoon’s lead vehicle, which communicates with the following cars by radio.
What are Wireless Sensor Networks?
Sensor Network

- Consists of a number of small nodes

- Each node is capable of:
  - Communications
  - Sensing
  - Computation

- Typically, measures physical phenomena
Wireless Sensor Network

- Each sensor node is equipped with a radio transceiver, microprocessor, sensors.

- Such nodes can autonomously form a network, through which sensor readings can be propagated.

- Data can be processed as it travels through the network, because nodes have some intelligence.
Wireless Sensor Network

Sensor Field
Self forming wireless network

Spaced at ~250 to 300 meters

Detection

Alternate access schemes

Remote Monitoring Facility

Local Monitoring Base Station
Typical WSN Applications

- Weather survey in hard-to-access geographical locations (e.g., mountains, ocean floor)

- Battlefield (e.g., surveillance and reconnaissance)
Security in MANETs and WSNs
Types of Attacks

- Application Layer:
  - Malicious code, Repudiation

- Transport Layer:
  - Session hijacking, Flooding

- Network Layer:
  - Black Hole, Worm Hole, Link Spoofing, Location disclosure etc.

- Data Link/MAC:
  - Malicious Behavior, Selfish Behavior

- Physical:
  - Interference, Traffic Jamming, Eavesdropping
Types of Attacks (cont.)

- Passive (difficult to detect)

- Active

- External
  - External malicious nodes attempting to DoS the network

- Internal
  - A (compromised) node that’s already an authorized part of the network, performing malicious actions
  - Compromised nodes can use security measures to protect their attacks
Security Challenges

- Resource scarcity

- Highly susceptible to physical attacks (e.g., node capture)

- Sensor networks closely interact with people and with their physical environments

- Communication patterns differ from traditional networks
Physical Security

- Main concern: node-capture
- How vital is this node? What functionality do adversaries have access to now? Keys? Sensor data? Etc.
- “I am behind a firewall” mentality
- Drastically different threat model

So am I! (behind your firewall)
Crypto-related Challenges
Key Management

- Trust model
- Key creation
- Key distribution
- Key storage
Key Establishment: Take One

- Simplest thing ever: one shared key
Key Establishment: Take Two

- Use a single shared key to establish a set of link keys
Securing WSNs

- Symmetric key crypto was the only way to address encryption, until recently.
  - Does not scale for WSNs.

- Use Identity-Based Encryption
  - Nodes can exchange information that uniquely identifies each node, and can be used to exchange keys and to encrypt data

(Oliveira, et al., 2007)
# Comparing Crypto Schemes for WSNs

<table>
<thead>
<tr>
<th></th>
<th>Symmetric key Cryptography</th>
<th>Public Key Cryptography</th>
<th>Identity-Based Cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computational Complexity</strong></td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td><strong>Communication Overhead</strong></td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Key Distribution</strong></td>
<td>Problematic</td>
<td>Complex</td>
<td>Simple</td>
</tr>
<tr>
<td><strong>Number of Keys</strong></td>
<td>$O(n^2)$</td>
<td>$O(n)$</td>
<td>$n$</td>
</tr>
<tr>
<td><strong>Key Directory</strong></td>
<td>At Each Node</td>
<td>At Each node or Key Center</td>
<td>No</td>
</tr>
<tr>
<td><strong>Non-Repudiation</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Forward Encryption</strong></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Routing and Intrusion Detection-related Challenges
Aggregation Trees in WSNs

Legend

- Wireless sensor node
- Data transmission
- $V_i$: Sensor measurement

Diagram:

Base station

$V_1$, $V_2$, $V_3$:

$f(V_1, V_2, V_3)$
Types of Routing Protocols

- Proactive
  - Typically table-driven and distance-vector protocols

- Reactive (source-initiated on-demand)

- Hybrid
Attacks
Spoofing (Man-in-the-Middle)

I am ‘B’!
Fabrication

- Malicious node sends false (but “valid”) routing messages, to change the topology
  - e.g.: neighbors B and C are no longer available
Wormhole Attack
Modification

Tamper with the packet’s data payload (attack on integrity)
In general ad-hoc networks are supposed to withstand DoS better than fixed networks
Sinkholes

- Malicious node tries to attract all traffic to itself
  - e.g. by faking to be the best route for other nodes
Sleep Depravation

- A.k.a. Resource Consumption Attack

- Consume battery on the target by constantly communicating with it (routing updates, relay requests, etc.)
Sybil Attack

- Malicious node takes on identity of many other nodes, again, making other nodes communicate with it.
Attacking the Sensors

- Tampering with the surrounding environment to fool the sensors

- In general, WSNs are well positioned to detect such attacks
Other Attacks

- Eavesdropping
- Black hole attack
  - Malicious node falsely advertises routes without having actual routes established
- Byzantine attack
  - confuse target nodes with non-optimal routing updates
- Flooding (the entire network vs. DoS of a single node)
- Replay attack
- Location disclosure attack
Detecting Malicious Events

- Fire
- Compromised node
- False report
- Alert transmission
- False report
- Compromised node
- Co-detectors
- Normal nodes

Base station
References


Conclusion

- Don’t treat MANETs & WSNs as your average network

- Large problem space wrt security

- Always backup your PowerPoint presentations!
Q&A
Thank You!

Edward Bonver
edward@owasp.org

OWASP

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.