Robustness in Wireless Network Access Protocols

PhD Defense

Martin Eian
Department of Telematics
Supervisor: Professor Stig F. Mjølsnes
Co-supervisor: Professor Steinar H. Andresen
21 September 2012
Outline

— Motivation and Introduction
— Background
— Manual protocol analysis
— Formal model construction and verification
— Conclusions and open research problems
Motivation - Two Trends in Wireless Networking

— Commercial off-the-shelf (COTS) hardware and software
  • 802.11/WiFi local area networks
  • Mobile/Cellular networks
    — GSM (2G)
    — UMTS (3G)
    — LTE (4G)
  • 802.16/WiMAX wide area networks
— Safety critical applications
  • Medical
  • Road safety
  • Supervisory control and data aquisition (SCADA)
    — Power generation and distribution
    — Oil & gas
    — Industrial
    — Transportation
  • Emergency communications
Safety Critical Applications

— Key security requirement: Availability
— Availability can be disrupted by denial of service (DoS) attacks
— Case studies
  • U.S. public safety communications network - LTE
  • Hospitals - 802.11 medical devices
— Research questions
  • Are current protocols vulnerable?
  • How do we assess the severity of a protocol vulnerability?
  • How can we prevent protocol vulnerabilities?

Wireless Network Access Protocols
Definitions³

Protocol

Set of rules and formats, semantic and syntactic, permitting information systems to exchange information.

Availability

The property of [resources] being accessible and useable upon demand by an authorized entity.

Denial of Service (DoS)

The prevention of authorized access to resources or the delaying of time-critical operations.

³Committee on National Security Systems Instruction No. 4009, National Information Assurance Glossary
Communication Protocols

— Formatting of data
  • Control/management messages
  • Data messages

— Behaviour
  • When to send a message
  • What to do when a message is received
  • Model: finite state machine
    — States
    — Transitions

\[^4\]Packets, frames, protocol data units
## Project Phases and Published Papers

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
<th>Papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>Literature review, problem definition</td>
<td>Fragility of the Robust Security Network: 802.11 Denial of Service 7th International Conference on Applied Cryptography and Network Security (ACNS’09)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A Practical Cryptographic Denial of Service Attack Against 802.11i TKIP and CCMP Ninth International Conference on Cryptology And Network Security (CANS 2010)</td>
</tr>
<tr>
<td>2:</td>
<td>Manual protocol analysis</td>
<td>The Modeling and Comparison of Wireless Network Denial of Service Attacks 3rd ACM SOSP Workshop on Networking, Systems, and Applications on Mobile Handhelds (MobiHeld ’11)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A Formal Analysis of IEEE 802.11w Deadlock Vulnerabilities 31st Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2012)</td>
</tr>
<tr>
<td>3:</td>
<td>Formal model construction and verification</td>
<td></td>
</tr>
</tbody>
</table>

Martin Eian, Robustness in Wireless Network Access Protocols
Denial of Service Attacks

— Attacks against Availability
— Disrupt the communication service
— Categories
  • Jamming → Transmit noise
  • Flooding → Exhaust resources
  • Implementation specific → Exploit bugs
  • Semantic → Exploit protocol vulnerabilities
Semantic Denial of Service Attacks

— Protocol vulnerabilities - desynchronize state
  • Unprotected control/management messages
— Attack amplification
  • Denial of Service time : Adversary transmission time
  • 10:1
  • 100:1
  • 1000:1
  • ...
— Special case: deadlocks
— Current wireless access protocols are vulnerable
The Denial of Service Problem

Network User

Access Point

Adversary
The Denial of Service Problem

Network User → Authentication Request → Access Point

Adversary
The Denial of Service Problem

Network User → Access Point

Authentication Response

Adversary
The Denial of Service Problem

Network User → Association Request → Access Point

Adversary
The Denial of Service Problem

Network User

Association Response

Access Point

Adversary
The Denial of Service Problem

Network User

Service Enabled

Access Point

Adversary
The Denial of Service Problem

Network User

Service Enabled

Access Point

Deauthentication

Adversary
The Denial of Service Problem

Network User

Access Point

Adversary
The Denial of Service Problem - MSC

![Diagram](image-url)
Summary of Phase 1

— Scope: semantic protocol vulnerabilities
— Case study: IEEE 802.11
— Start manual analysis
## Project Phases and Published Papers

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
<th>Published Papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>Literature review, problem definition</td>
<td>Fragility of the Robust Security Network: 802.11 Denial of Service&lt;br&gt;7th International Conference on Applied Cryptography and Network Security (ACNS’09)&lt;br&gt;A Practical Cryptographic Denial of Service Attack Against 802.11i TKIP and CCMP&lt;br&gt;Ninth International Conference on Cryptology And Network Security (CANS 2010)</td>
</tr>
<tr>
<td>3:</td>
<td>Formal model construction and verification</td>
<td></td>
</tr>
</tbody>
</table>
Case Study - IEEE 802.11 (1997)

— Standard for wireless local area networks
— PHY and MAC layers
— Three message types
  • Control frames
  • Management frames
  • Data frames
— Extensively analyzed for DoS vulnerabilities
— Facilitates experimental validation
— Scope
  • 802.11 MAC layer protocols
  • 802.11i and 802.11w amendments
802.11 States, Authentication and Association

— Provides
  • Integrity
  • Confidentiality
  • Replay protection
  • Sender authenticity (unicast)

— TKIP and AES-CCMP

— Security Associations (SAs)
  • Pairwise keys
  • Security parameters
  • Deleted on successful authentication, (re)association, deauthentication, disassociation

— Only protects data frames (not management/control)
— Uses deauthentication to recover from lost key synchronization
Deauthentication Attack - 802.11i
802.11i TKIP

— Weak message integrity code (MIC)

— Countermeasures
  ● 2 MIC failures in 60 seconds
  ● Shut down for 60 seconds
  ● Delete all security associations using TKIP
  ● Design goal: difficult to deliberately cause MIC failures

— TKIP sequence counter (TSC) - prevent replay

— 802.11e quality of service (QoS)
  ● One TSC per QoS class
TKIP Countermeasures Attack (Paper B)

- **Adversary**
- **Network User**
- **Access Point**

- Broadcast QoS Message Priority 1
- MIC Failure
- Countermeasures
- 60 seconds DoS
- MIC Failure Report
- MIC Failure

- Broadcast Message
- Broadcast Message
- MIC Failure Report
- MIC Failure
- Countermeasures
802.11w: Protected Management Frames (2009)

RSN protection for:
  — Deauthentication
  — Disassociation
  — Action

...but not for:
  — Authentication
    ● Chicken and egg problem?
  — Association
    ● Backward compatibility
Authentication Attack (Paper A)

Adversary

Network User

Access Point

State 3

Security Association

Authentication Request

Authentication Response

Protected Data

Protected Disassociation

State 2

Delete Security Association

Delete Security Association

Association Request

Association Response

State 3

EAPOL 1

EAPOL 2

EAPOL 3

EAPOL 4

Security Association
Summary of Phase 2

— Contributions
  • Discovered vulnerabilities
  • Experimental validation
  • Proposed robust solutions and temporary workarounds
— A decade of 802.11 analysis\(^5\)
— New vulnerabilities found
— Manual analysis insufficient
— Use formal methods
— Goal: automatically find semantic protocol vulnerabilities

## Project Phases and Published Papers

| 1: Literature review, problem definition | Fragility of the Robust Security Network: 802.11 Denial of Service  
7th International Conference on Applied Cryptography and Network Security (ACNS’09) |
| 2: Manual protocol analysis | A Practical Cryptographic Denial of Service Attack Against 802.11i TKIP and CCMP  
Ninth International Conference on Cryptology And Network Security (CANS 2010) |
| 3: Formal model construction and verification | The Modeling and Comparison of Wireless Network Denial of Service Attacks  
3rd ACM SOSP Workshop on Networking, Systems, and Applications on Mobile Handhelds (MobiHeld ’11)  
A Formal Analysis of IEEE 802.11w Deadlock Vulnerabilities  
31st Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2012) |
Formal Method Development

— Method: Model checking
— Bottom-up approach
  • Cost quantification
  • Model implementation in Promela
  • Model verification using SPIN
  • Experimental validation
  • Formal definition
Construction of Models

— Cost Model
— Protocol Model
— Adversary Model
Cost Model

— Cost: energy, computational, memory, monetary, probability of detection/location, **time**

— Protocol participant cost $\Gamma_P$
  - Time without communication service
  - Implementation: global variable

— Adversary cost $\Gamma_A$
  - Total adversary transmission time
  - Implementation: global variable

— Attack efficiency/amplification $E$
  - $E = \frac{\Gamma_P}{\Gamma_A}$

— Bounds
  - $\Gamma_P$ is finite
  - $\Gamma_A > 0$
  - $E$ not defined for deadlock attacks
Attack Efficiency $\mathcal{E}$

$\frac{\Gamma_P}{\Gamma_A}$

- 802.11
- 802.11i
- 802.11w

- Deauth(STA)
- Deauth(AP)
- Disassoc(STA)
- Disassoc(AP)
- Virtual CS
- Authentication
- Association
- Quiet
- TKIP
General Protocol Model

- Initiator
  - Promela `proctype`
- Responder
  - Promela `proctype`
- I/O: Protocol messages
  - Promela `chan`
Protocol Model Challenges

— Stop model execution if protocol is unable to recover
  • Easy deadlock detection (SPIN “invalid endstates”)
— Mental image: data frames ping pong
— Only send data when receiving data
  • Exception 1: after EAPOL4
  • Exception 2: after channel switch recovery
— Timeouts
  • Explicit notification by recipient
  • Promela `timeout` statement
  • Allow adversary to halt, then resume when `timeout` is executed
    — Detect attacks where adversary sends messages after timeout
Adversary Model

— Non-deterministic
— Can read and send unprotected messages
— Cannot delete messages
  ● Distinction from Standard/Dolev-Yao Cryptographic Model
— Limited message budget
Adversary Model - Promela

```
proctype Adversary() {
    short pkts = 0; Msg m; m.type = DUMMY; m.class = 1; m.ch = 1; m.mic = 0;
do
    :: (pkts >= att) -> break;
    :: pkts < att && (setup || established) -> 
      if
        :: m.type == DUMMY -> break;
        :: m.type == DUMMY && (pkts > 0) -> 
          if
            :: timeoutflag -> timeoutflag = 0;
          fi
        :: m.type == DUMMY -> 
          if
            :: m.type = deauth -> m.class = 1;
            :: m.type = disassoc -> m.class = 2;
            :: m.type = authreq -> m.class = 1;
            :: m.type = authresp -> m.class = 1;
            :: m.type = assocreq -> m.class = 2;
            :: m.type = assocresp -> m.class = 2;
            :: dot11h -> m.type = csw; m.class = 1;
          fi
        :: m.type != DUMMY -> 
          if
            :: atomic{pkts++; toAP ! m; m.type = DUMMY;} 
            :: atomic{pkts++; toSTA ! m; m.type = DUMMY;} 
          fi
      fi
  od
}
```
802.11 Challenges

— Model construction revealed ambiguities and gaps in protocol specifications
  • Example: authentication request received in State 3
— Checked protocol implementations
  • Cisco
  • hostapd
— Different interpretations
  • Implement both
  • Verify both
Model Verification

— Model checker: SPIN
— Using cost model
  • Select efficiency threshold $T$
  • Check LTL property: $\square((\Gamma_A = 0) \lor (\frac{\Gamma_P}{\Gamma_A} < T))$
— Deadlocks
  • Does not require cost model
  • Check SPIN property “invalid endstates”
Model Verification Complexity and Performance

<table>
<thead>
<tr>
<th>Adversary</th>
<th>States</th>
<th>Transitions</th>
<th>Time (s)</th>
<th>Htime</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8,382</td>
<td>14,374</td>
<td>0.1</td>
<td>0.1 sec</td>
</tr>
<tr>
<td>2</td>
<td>380,263</td>
<td>729,614</td>
<td>8.8</td>
<td>8.8 sec</td>
</tr>
<tr>
<td>3</td>
<td>10,744,856</td>
<td>22,009,511</td>
<td>1,260.0</td>
<td>21 min</td>
</tr>
<tr>
<td>4</td>
<td>238,582,500</td>
<td>508,034,440</td>
<td>95,300.0</td>
<td>26.5 hrs</td>
</tr>
</tbody>
</table>

₆Intel Xeon 2.66GHz CPU
802.11i Deadlock Attack (Paper C)
802.11w Deadlock Attack 1 (Paper D)
802.11w Deadlock Attack 2 (Paper D)
802.11w Deadlock Attack 3 (Paper D)
Cost Model Results

— Previously published attacks verified
— Highest efficiency: Quiet attack\(^7\)
— Difficult to find new lower efficiency attacks
  • Too many counterexamples from model checker
  • Partial solution by limiting adversary and protocol - e.g. 802.11h support
— Modify protocol to remove vulnerabilities
  • Challenge: experimental validation

Conclusions

— Proposed formal method is
  • Practical
  • Useful

— Found severe vulnerabilities in existing protocols
  • Common cause: protocol modifications
  • Eluded extensive manual analysis

— Experimental validation of all results
  • Differences in interpretation of the standard
Research Questions Retrospective

— Are current protocols vulnerable?
  • Yes. Why?
  • Complexity makes manual analysis insufficient
  • Protocol modifications can have unintended consequences

— How do we assess the severity of a protocol vulnerability?
  • Quantify the costs
  • Proposed cost model

— How can we prevent protocol vulnerabilities?
  • With the help of formal methods during protocol design
  • Proposed formal method
Protocol Design

1. Design Protocol
2. Construct Formal Model
3. Run Model Checker
4. Vulnerable?
   - Yes: Implement Protocol
   - No: Re-design Protocol

www.ntnu.no Martin Eian, Robustness in Wireless Network Access Protocols
Open Research Problems

— Integration with other models and tools
— Alternative cost and adversary models
— Complete 802.11 model
— Other wireless network access protocols
  • GSM
  • UMTS
  • LTE
  • 802.16 (WiMAX)
— Real time support
— Protocol design principles
Thank You!