Formal Modeling and Proving Cryptographic Properties of the Optin Sensor Protocol

CHALLENGES: secure communicating systems

PRODUCTIVE SECTOR: automobile

PROBLEM DESCRIPTION

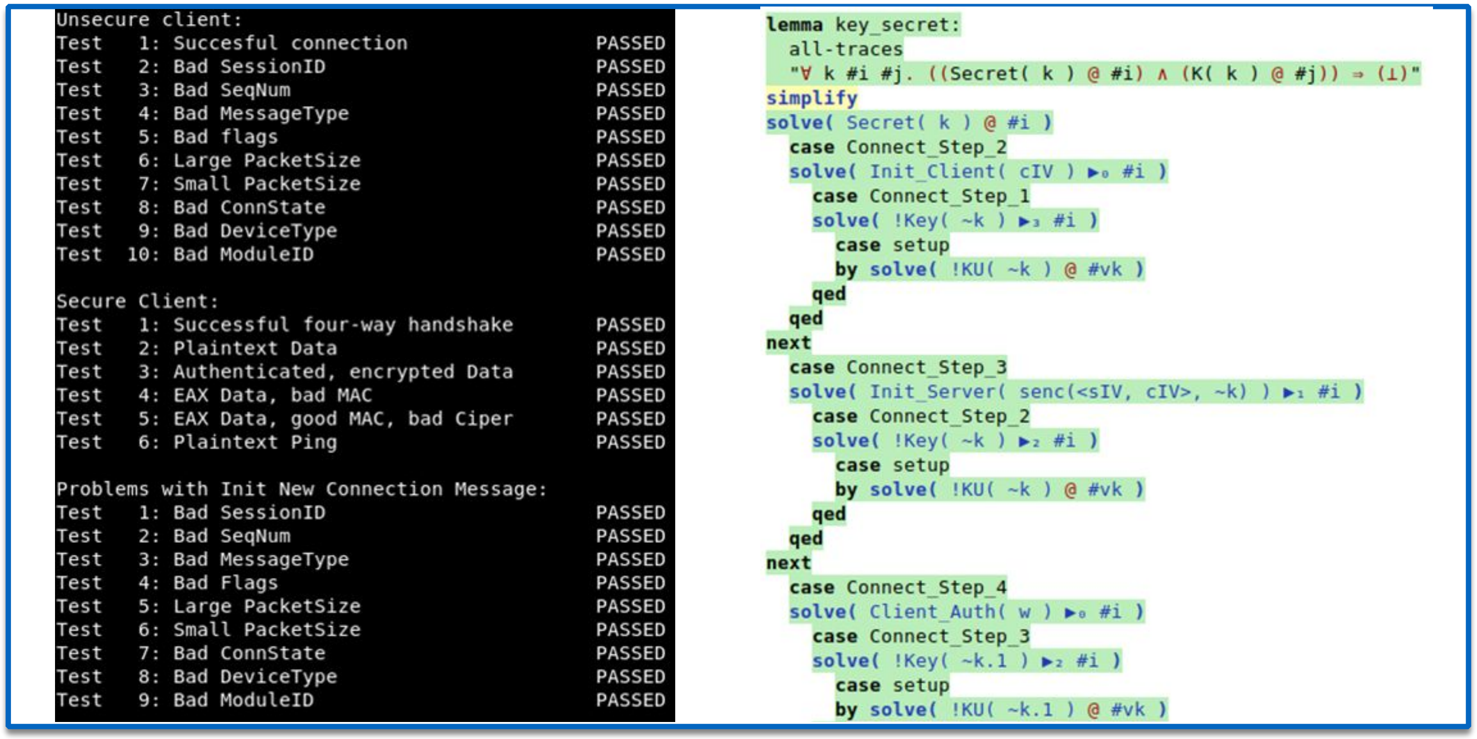
In this project aided with automatic theorem proving we developed a lightweight cryptographic extension of the Optin Sensor Protocol which is heavily used at our industrial partner in IoT devices.

CHALLENGES AND GOALS

We determinedd the security requirements for some typical industrial use of the OSP protocol, then extended the protocol with cryptography. We also analyzed the security properties of the new extension, and implemented and tested the new protocol features. Moreover, we validated the new design by mathematical modeling and published the new protocol version

MATHEMATICAL AND COMPUTATIONAL METHODS

For validation of the new protocol version mathematical modeling, namely automatic theorm prooving was used. We modeled both the new protocol design and the security requirements by logic formulas. We used the TAMARIN-Proover software for formal verification of the key security properties.



```
Unsecure client:
Test   1: Succesful connection                        PASSED
Test   2: Bad SessionID                               PASSED
Test   3: Bad SeqNum                                  PASSED
Test   4: Bad MessageType                             PASSED
Test   5: Bad flags                                   PASSED
Test   6: Large PacketSize                            PASSED
Test   7: Small PacketSize                            PASSED
Test   8: Bad ConnState                               PASSED
Test   9: Bad DeviceType                              PASSED
Test  10: Bad ModuleID                                PASSED

Secure Client:
Test   1: Successful four-way handshake               PASSED
Test   2: Plaintext Data                              PASSED
Test   3: Authenticated, encrypted Data               PASSED
Test   4: EAX Data, bad MAC                           PASSED
Test   5: EAX Data, good MAC, bad Ciper               PASSED
Test   6: Plaintext Ping                              PASSED

Problems with Init New Connection Message:
Test   1: Bad SessionID                               PASSED
Test   2: Bad SeqNum                                  PASSED
Test   3: Bad MessageType                             PASSED
Test   4: Bad Flags                                   PASSED
Test   5: Large PacketSize                            PASSED
Test   6: Small PacketSize                            PASSED
Test   7: Bad ConnState                               PASSED
Test   8: Bad DeviceType                              PASSED
Test   9: Bad ModuleID                                PASSED
```

```
lemma key_secret:
  all-traces
  "∀ k #i #j. ((Secret( k ) @ #i) ∧ (K( k ) @ #j)) ⇒ (⊥)"
simplify
solve( Secret( k ) @ #i )
  case Connect_Step_2
  solve( Init_Client( cIV ) ▶₀ #i )
    case Connect_Step_1
    solve( !Key( ~k ) ▶₃ #i )
      case setup
      by solve( !KU( ~k ) @ #vk )
    qed
  qed
next
  case Connect_Step_3
  solve( Init_Server( senc(<sIV, cIV>, ~k) ) ▶₁ #i )
    case Connect_Step_2
    solve( !Key( ~k ) ▶₂ #i )
      case setup
      by solve( !KU( ~k ) @ #vk )
    qed
  qed
next
  case Connect_Step_4
  solve( Client_Auth( w ) ▶₀ #i )
    case Connect_Step_3
    solve( !Key( ~k.1 ) ▶₂ #i )
      case setup
      by solve( !KU( ~k.1 ) @ #vk )
```

Testing and verification of the new design

Formal Modeling and Proving Cryptographic Properties of the Optin Sensor Protocol

Results and Benefits

The new and more secure design of the OSP 2.0 is in use in several ongoing projects and further applications of the protocol are planned.

The new public standard encourages wider both acemic--industrial and industrial—industrial cooperation.

Cryptographic and mathematical modeling insights are beneficial for the system engineers of the company

The new OSP 2.0 protocol standard is available for download from the website of the company: http://www.optin.hu/static/www/OSP_spec_v2_en.pdf

SZTE TTIK INFORMATIKAI INTÉZET

HU-MATHS-IN
Hungarian Service Network for Mathematics in Industry and Innovations

SZÉCHENYI 2020
Európai Unió Európai Strukturális és Beruházási Alapok
MAGYARORSZÁG KORMÁNYA
BEFEKTETÉS A JÖVŐBE

OPTIN

OPTIN Kft.