RECEIVER INDEPENDENT IMPLEMENTATION OF THE GALILEO OPEN SERVICE NAVIGATION MESSAGE AUTHENTICATION (OS-NMA)

ITSNT 2018: Navigation in Challenging Environment II

Xabier Zubizarreta, J. Rossouw van der Merwe, Ivana Lukčin, Alexander Rügamer, Wolfgang Felber

xabier.zubizarreta@iis.fraunhofer.de
Fraunhofer IIS, Nuremberg
The threat of spoofing

UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea

Getting lost near the Kremlin? Russia could be ‘GPS spoofing’
Need of protection

- Authentication at **signal level** (e.g. Galileo Public Regulated Service)

- Authentication at **message level**
AGENDA

- Introduction to OS-NMA
- Implementation
- Advantages, disadvantages, constraints, and dangers
Open Service Navigation Message Authentication (OS-NMA)

- OS NAV Messages
  - Signature
- “Certified” receiver
  - Public Key
- Authentication Message
- Simple receiver
- Nav Message + Signature
- Galileo Control Center
  - Private Key
- Navigation message
  - Key
  - Signature

- © Fraunhofer IIS
OS-NMA: A brief description

- Timed Efficient Stream Loss-tolerant Authentication (TESLA)
- 1) Root key verifies all keys
- 2) Each key verifies the previous Message Authentication Code (MAC)

Key generation

Root-key
Key 0

Key 1
Key 2
... Key N (seed key)

Transmission

MAC 1
Key 1
MAC 2
Key 2
...
**OS-NMA: A brief description**

- Asymmetrical cryptography (slow, done only once)
  - Elliptic Curve Digital Signature Algorithm (ECDSA) → 448-1043 bits
- Symmetrical cryptography (fast, done for key / MAC generation)
  - Hash-based message authentication code (HMAC) → 256 bits → Truncate
OS-NMA: A brief description

- **I/NAV**: 40 bits every 2 seconds
- **Subframe**: 600 bits (40 bits x 15 pages)
- **Header & Root-key (HKROOT)**: 120 bits (!)
  - Header
  - Digital Signature Message (DSM) Block
  - 6 - 16 subframes (3 to 8 minutes)
- **MAC section**: 480 bits
  - Contains the signatures

**Diagram:**
- **Sub-frame 1**
  - DSM & NMA Header
  - DSM Block 1
  - MACs
  - DSM Block ID
- **Sub-frame n**
  - DSM Block n
  - MACs
  - Parameters
  - Root-key Signature
  - Tags (MAC) Description

**Transmission (time)**

OS-NMA ICD v2.0.
Implementation set-up

Pre-processing

- Pre-computed keys
- Pre-compute OS-NMA bits
- Navigation message

Channel

Spirent GSS9000

Post-processing

- Sub-frames
- Satellite

Reference receiver

Parser

Python™
### Receiver Independent

- Raw navigation message bits available:

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Receiver</th>
<th>Raw bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Septentrio</td>
<td>PolaRx5</td>
<td>Accessible as GalRawINAV</td>
</tr>
<tr>
<td>u-blox</td>
<td>M8T</td>
<td>Accessible in UBX-RXM-SFRBX</td>
</tr>
<tr>
<td>Fraunhofer IIS</td>
<td>GOOSE</td>
<td>Custom direct write to file</td>
</tr>
<tr>
<td>Android</td>
<td>Selected smartphones</td>
<td>Accessible in GNSS Raw Data*</td>
</tr>
</tbody>
</table>

*From API 24 onwards*
Constraints: Time

- Time to First Authenticated Fix (TTFAF)
- From cold-start

\[ TTFAF \]

\[ t_{DSM} \]

\[ t_{acq} \]

DSM Contents
- Param.
- Signature
- Root-key-Tail
- Param.
- Signature

DSM Blocks
- DSM Block #1
- DSM Block #2
- DSM Block #3
- DSM Block #4
- DSM Block #5
- DSM Block #6
- DSM Block #7
- DSM Block #1
- DSM Block #2
- DSM Block #3

Lock status
- Not acquired
- Acquired

Decoded
Constraints: Time

- Slowest case ca. 420 seconds

Graph showing the percentage of received data over time. The graph includes lines for Signature and Root-key.

Additional information in a box:
- KS: 256 bits
- MS: 32 bits
- Sgl. size: 1042 bits
- NB: 14
- NMACK: 1
- MACs per MACK: 4 tags
Constraints: Time

- Fastest case 180 seconds (from cold start)
Constraints: Time to first alert

- Deny the signal and force re-decoding
- Avoided pre-trusting keys

Deny the signal and force re-decoding
Avoided pre-trusting keys
Constrasts: Security of algorithms

- Symmetric cryptography → Hashing is quantum safe
- Asymmetric cryptography → ECDSA is **not** quantum safe!
Use-cases

Secure connection up to the provider

OS-NMA

TOLL SERVICE PROVIDER

NO GNSS

GNSS
Use-cases: Project PRoPART

- The main objective of the PRoPART is to **develop and demonstrate a high availability positioning solution for connected automated driving applications.**
- enhance an existing RTK (Real Time Kinematic) software solution by exploiting the distinguished features of Galileo signals
Conclusions: Why / why not OS-NMA?

- Open Service
- Secure nav. msg.
- Low impact on TTF(A)F*
- Firmware update only

- Ground segment
- Long time to alarm
- Replay attacks
- Spreading authentication
THANK YOU!

Questions?

Contact: xabier.zubizarreta@iis.fraunhofer.de

The work for this paper has been conducted under the PRoPART project, which has received funding from the European GNSS Agency under the European Union’s Horizon 2020 research and innovation program under grant agreement No 776307.