Navigation Message Authentication

Cillian O'Driscoll

NNF Seminar on Safety and Security Issues in Positioning, Navigation and Timing

Oslo, 14 June 2023

Motivation

- Much interest in recent years in robust, secure, authentic and resilient navigation
- Learning from similar problems in communications systems, we are applying cryptographic schemes to add **authentication** capabilities
- **However** – there is a significant difference between comms and navigation

In navigation, the message (user PVT) is **unknown** to all parties

The Navigation Problem

- Navigation is fundamentally an **estimation** problem
  - The end user wishes to estimate the time-varying state for some entity
- Estimation requires **measurements** that are inherently noisy
- Measurements may be:
  - **Intrinsic**: not dependent on any external source (e.g. time, acceleration, etc)
  - **Extrinsic**: dependent on external information (e.g. declination of a fixed star)
- To fix one's position wrt an external frame of reference **requires** some extrinsic measurement
  - This is to some extent vulnerable to spoofing

GNSS Based PVT

- A GNSS is navigation system in which the extrinsic measurements are provided by a constellation of satellites orbiting the earth
- There are three fundamental premises to the correct operation of a GNSS:

1. Each satellite generates its signals at precise, pre-specified epochs (in the satellite's own clock domain)
2. Each satellite transmits accurate models of its own position, velocity and time
3. The signals have travelled in a more-or-less straight line at more-or-less the speed of light in vacuo from the satellite to the receiver

GNSS Based PVT Assurance

- How can we assure that these three premises are met?
  - We can **authenticate** the **origin** of the signals by introducing unpredictable elements
    - An attacker must observe the elements, but can replay them
    - Does **not guarantee** that signals are received **directly** from the satellites, but does guarantee that the signals originated with the satellites
  - We can **authenticate** the content of the navigation messages
    - This means the decoded ephemeris are as broadcast (does not prevent integrity failures!)
- But we still have a fundamental issue:

A GNSS receiver can be successfully spoofed even when the spoofed and authentic signals are identical, but shifted in time, frequency, amplitude or phase.

Recommended Reading

Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems

Logan Scott, *LS Consulting*

methods. To this end, we look at a four level signal authentication architecture:

0. **No Enhancement**. Receivers can ignore signal authentication features and still successfully operate. Higher levels maintain backwards compatibility with extant receivers.

1. **Data Message Authentication.** Can be implemented in software.

2. **Public Spreading Code Authentication** Requires precorrelation sample storage similar to block acquisition schemes.

3. **Private Spreading Code Authentication** Requires tamper resistant hardware and secure keying.

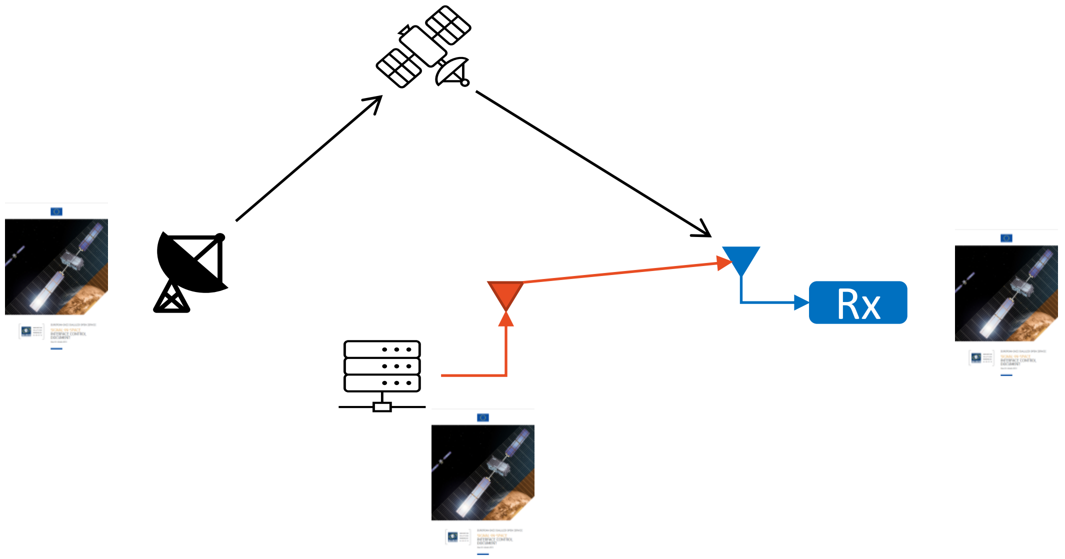
Scott, L. "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems", Proceedings of ION GPS/GNSS 2003.

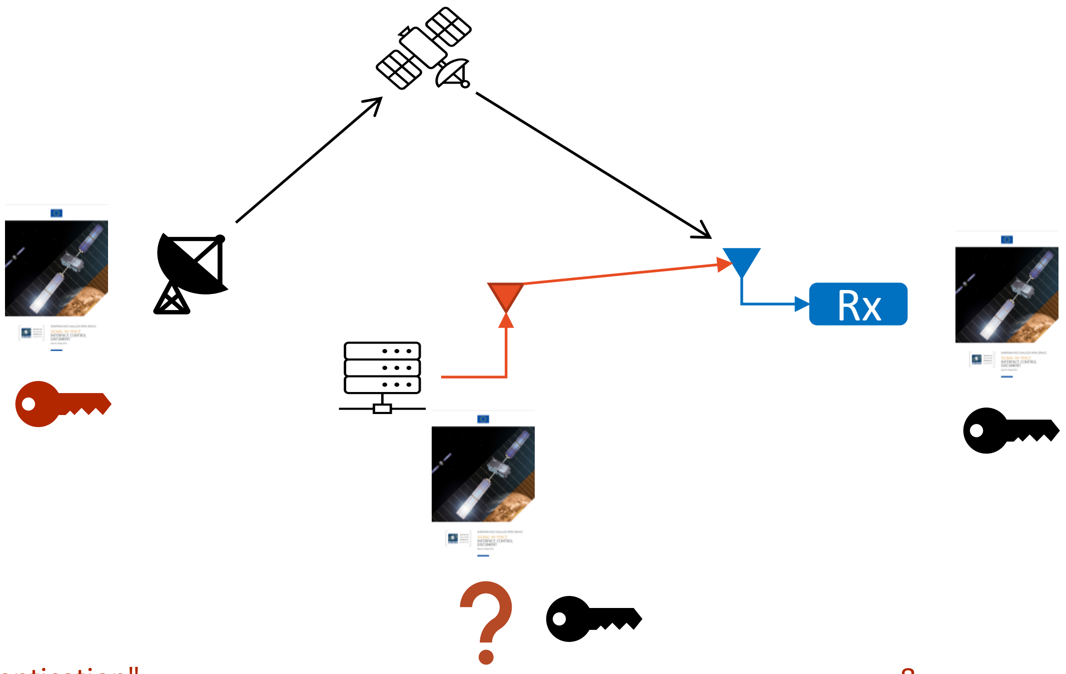
Some initial observations

- **Unpredictable elements** are **necessary** in GNSS signals to provide a proof of origin
  - But not **sufficient** to show that there has not been an interception and manipulation of the measurement
- **Message authentication** is **necessary** to ensure authenticity of orbit and clock models

Unpredictability and Verifiability

- With no unpredictability
  - An attacker can generate a **perfectly** legitimate signal
- Unpredictability ➔ elements the attacker **cannot** know in advance
- Verifiability ➔ Receiver can verify that the unpredictable elements are indeed from the system





Navigation Message Authentication

- NMA introduces **unpredictable** elements to the navigation data stream
- These elements are a function of the raw navigation data (ephemeris etc) and some **secret** known only to the system
- Users **verify** that the data and unpredictable elements correspond to one another, either:
  - By using asymmetric cryptography
  - Through a delayed release of the secret key

Recommended Reading

GPS Software Attacks

Tyler Nighswander
Carnegie Mellon University
Pittsburgh, PA, USA
tylerni7@cmu.edu

Brent Ledvina
Coherent Navigation
San Mateo, CA, USA
ledvina@coherentnavigation.com

Jonathan Diamond
Coherent Navigation
San Mateo, CA, USA
diamond@coherentnavigation.com

Robert Brumley
Coherent Navigation
San Mateo, CA, USA
brumley@coherentnavigation.com

David Brumley
Carnegie Mellon University
Pittsburgh, PA, USA
dbrumley@cmu.edu

ABSTRACT

Since its creation, the Global Positioning System (GPS) has grown from a limited purpose positioning system to a ubiquitous trusted source for positioning, navigation, and timing data. To date, researchers have essentially taken a signal processing approach to GPS security and shown that GPS is vulnerable to jamming and spoofing.

grown from a limited purpose positioning system to a ubiquitous trusted source for positioning, navigation, and timing (PNT) data. While GPS is commonly known for personal navigation, it is also widely used for precise timing and frequency calibration. For example, cell phone towers (e.g., Verizon) use GPS to calibrate the frequency and timing for transmissions, and the power grid uses GPS to coordinate time stamps fo

	uBlox	UAV	iFly	eXplorist	eTrex	NetRS	Arbiter
Vulnerable to Middle-of-the-Earth						√	
Vulnerable week #	√	√	√		√	√	√
Vulnerable to Date De-synchronize							√
Vulnerable OS			√	√		√	
Spoofable	√	√	√	√	√	√	√

Table 1: Successful attacks against receivers.

After the ephemeris is decoded, the receiver will enter a reboot cycle *even after the attack is stopped*. Thus, the attack achieves a similar goal to jamming: denying service, but unlike jamming, does not require continual broadcast. While DoS is not considered

Nighswander, Tyler, et al. "GPS software attacks." *Proceedings of the 2012 ACM conference on Computer and communications security*. 2012.

Benefits of NMA

- The primary role of NMA is, as the name suggests, to **authenticate** the navigation data
  - Prevents an attacker from maliciously modifying the message to mislead the victim
- Secondary benefit:
  - NMA introduces **unpredictable elements** to the signals
  - Attackers must observe the signal to effect a successful attack
  - Places a **lower bound on time**
    - If we successfully authenticate data with NMA, then current time must be later than the time the data was transmitted
  - Ties the data to the unpredictable elements and **vice versa**

What can we conclude from verified NMA?

- Let's assume the NMA check **passes** in our receiver ➔ What does this imply?
  1. Either:
     a) The navigation data received was indeed that broadcast by the system
     b) An attacker generated matching data/authentication data pair [very low probability]
  2. The time of reception is **later** than the time the unpredictable elements were broadcast by the satellite
     - We have a **lower bound on time**
  3. Either:
     a) The data was received directly from the GNSS satellite; or
     b) The data has been received by a 3rd party and re-broadcast
- It is, ultimately, up to the receiver to decide what to do with this information

What can we conclude from failed NMA?

- Let's assume the NMA check **fails** in our receiver ➔ What does this imply?
- Essentially one of the following **must** be true:
    1. The data we received was corrupted in such a way that the CRC still passed; or
    2. The data was generated by a 3rd party and not by the system; or
    3. The system suffered a failure and transmitted either the incorrect data or an incorrect signature
- Again, ultimately, up to the receiver to decide what to do with this information

Summary

- NMA is a **useful tool** in improving GNSS receiver security
- Forces an attacker to **observe** the true signal in order to make a successful attack
- Important to understand the implications of both **passing** and **failed** verifications
  - Receiver logic must account for all possibilities
  - Make decisions on corrective action based on *a priori* models of the likelihood of each scenario
- Galileo OSNMA is here today – let’s use it
  - Only from real-world use will we fully understand and realise its full potential

Thank you

cillian@codc.ie

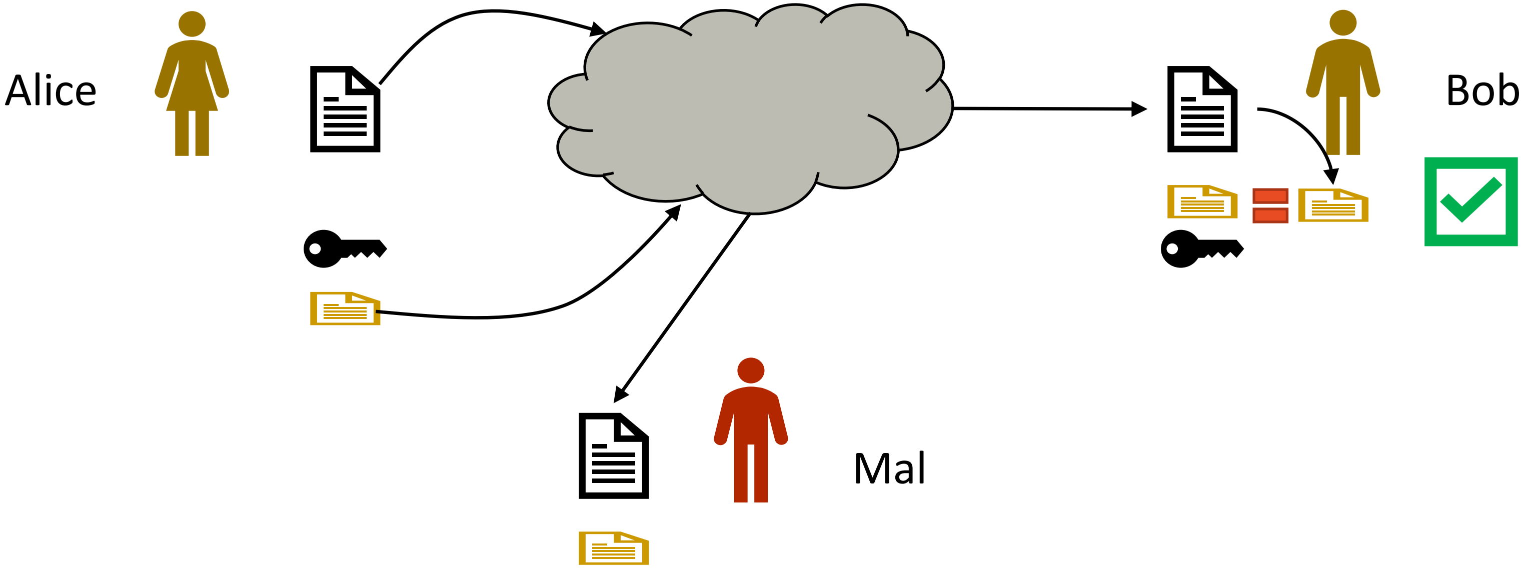
References

- Scott, L. “Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems”, Proceedings of ION GPS/GNSS 2003.
- Nighswander, Tyler, et al. "GPS software attacks." *Proceedings of the 2012 ACM conference on Computer and communications security*. 2012.

Extra Material

Symmetric Key Authentication

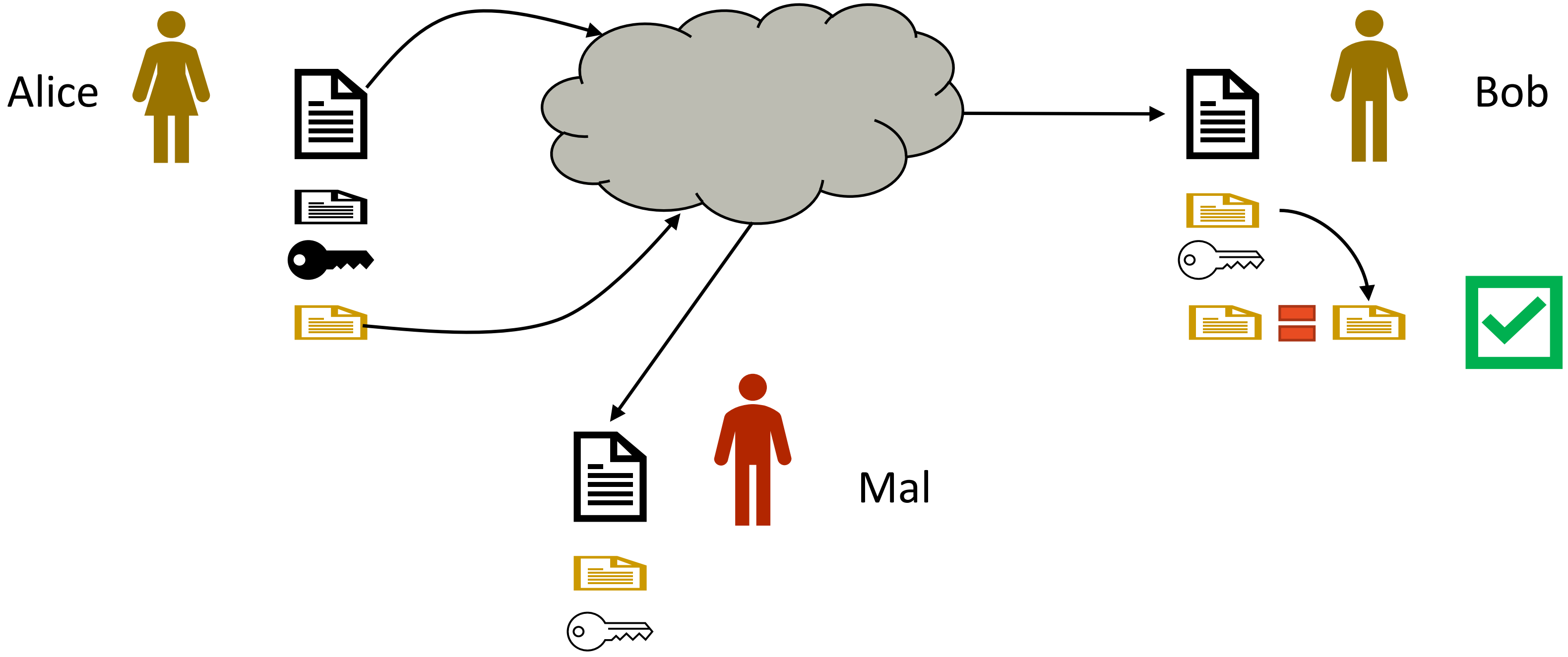
- Alice sends Bob a message, along with a MAC to enable verification of authenticity – Mal wishes to falsify the message



- Alice and Bob share a **secret key** which can be used to regenerate the MAC and verify that MAC and message agree

Asymmetric Key Authentication

- Here Alice has a **private key** which she uses to generate a **digital signature**
- She publishes here **public key** which anyone can use to **verify** the DS



NMA in the wild

Galileo: OSNMA

- Galileo has introduced Open Service Navigation Message Authentication (**OSNMA**)
- 40 bits in very I/NAV page pair in E1B are used to disseminate the authentication information
  - 32 bits contain Message Authentication Codes (**MACs**) and **keys**
  - 8 bits contain status and other data
- OSNMA is here **today** – use it!

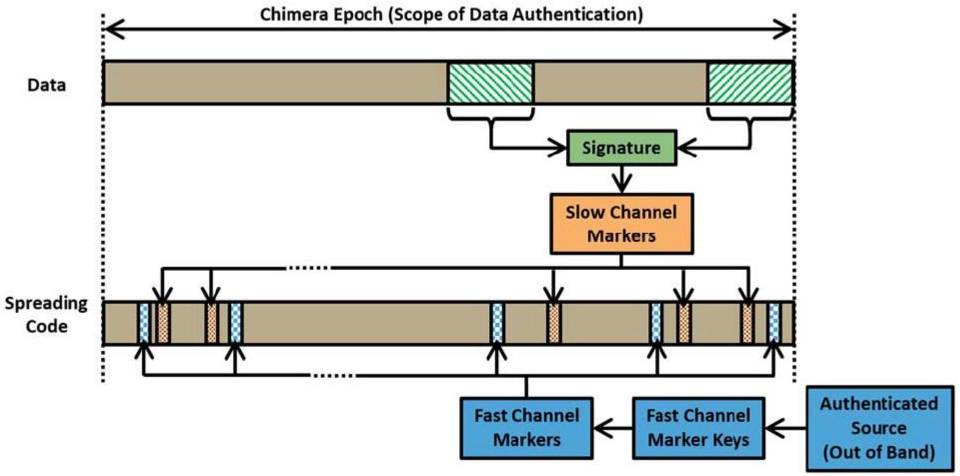
E1-B

Even/odd=1	Page Type	Data (2/2)	OSNMA	SAR	Spare	CRC_j	SSP	Tail	**Total (bits)**
1	1	16	40	22	2	24	8	6	120

Even/odd=0	Page Type	Data k (1/2)	Tail	**Total (bits)**
1	1	112	6	120

GPS: Chimera

- **CHI**ps and **ME**ssage **R**obust **A**uthentication (Chimera) combines message and signal authentication
- Message authentication:
  - Asymmetric scheme
  - Authenticates all data every 18 seconds
- Planned for launch on the NTS-3 satellite later this year
- Unknown whether it will be integrated into GPS



Air Force Research Laboratory, “Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User Segment Interface” IS-AGT-100