E-GROUP
SOFTWARE & BEYOND

GALILEO:

In GPS We Trust?

Áron Szabó
Levente Kovács
Péter Ligeti

Budapest
2021-10-08

GNSS - comparison

GNSS	GPS	GLONASS	BeiDou	GALILEO

GNSS - comparison

GNSS	GPS	GLONASS	BeiDou	GALILEO
origin country	US	RU	CN	EU

GNSS - comparison

GNSS	GPS	GLONASS	BeiDou	GALILEO
origin country	US	RU	CN	EU
protected data	location date/time	location date/time	location date/time	location date/time

GNSS - comparison

GNSS	GPS	GLONASS	BeiDou	GALILEO
origin country	US	RU	CN	EU
protected data	location date/time	location date/time	location date/time	location date/time
type of applied cryptography	symmetric	symmetric	symmetric	symmetric asymmetric

GNSS - comparison

GNSS	GPS	GLONASS	BeiDou	GALILEO
origin country	US	RU	CN	EU
protected data	location date/time	location date/time	location date/time	location date/time
type of applied cryptography	symmetric	symmetric	symmetric	symmetric asymmetric
protected data is available to	military service	military service	military service	military service civilian service

GNSS - comparison

GNSS	GPS	GLONASS	BeiDou	GALILEO
origin country	US	RU	CN	EU
protected data	location date/time	location date/time	location date/time	location date/time
type of applied cryptography	symmetric	symmetric	symmetric	symmetric asymmetric
protected data is available to	military service	military service	military service	military service civilian service
protects against	spoofing (limited)	spoofing (limited)	spoofing (limited)	spoofing (unlimited)

GNSS - comparison

GNSS	GPS	GLONASS	BeiDou	GALILEO
origin country	US	RU	CN	EU
protected data	location date/time	location date/time	location date/time	location date/time
type of applied cryptography	symmetric	symmetric	symmetric	symmetric asymmetric
protected data is available to	military service	military service	military service	military service civilian service
protects against	spoofing (limited)	spoofing (limited)	spoofing (limited)	spoofing (unlimited)
does not protect against	meaconing jamming	meaconing jamming	meaconing jamming	meaconing jamming

MIJI: meaconing (replay attack, valid data)
MIJI: intrusion (unauthorized access to communication channel)
MIJI: jamming (DDoS, valid/invalid data)
MIJI: interference (noise)
spoofing (invalid/modified data)

GNSS - comparison

E-GROUP
SOFTWARE & BEYOND

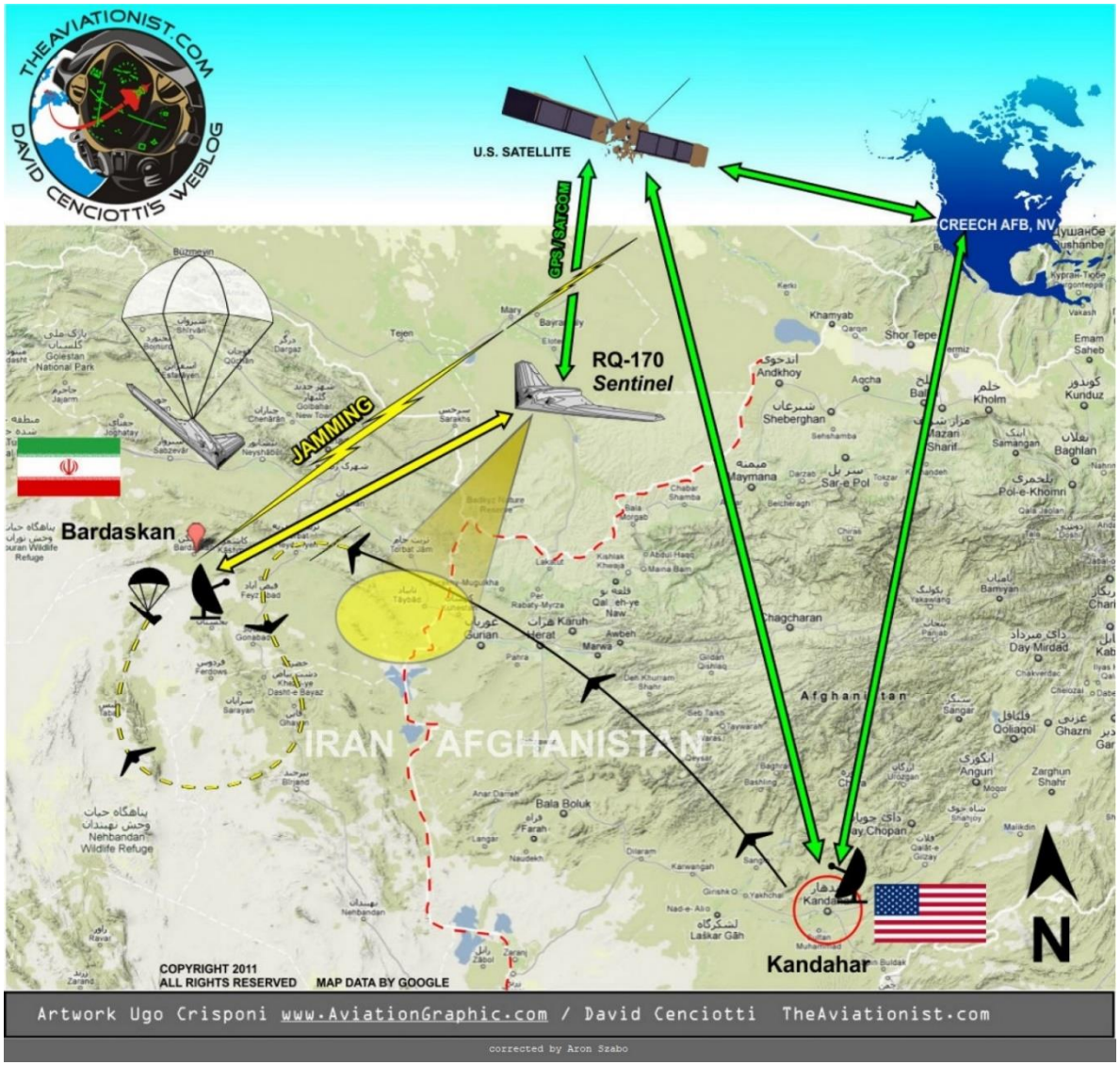
GNSS	GPS	GLONASS	BeiDou	GALILEO
origin country	US	RU	CN	EU
protected data	location date/time	location date/time	location date/time	location date/time
type of applied cryptography	symmetric	symmetric	symmetric	symmetric asymmetric
protected data is available to	military service	military service	military service	military service civilian service
protects against	spoofing (limited)	spoofing (limited)	spoofing (limited)	spoofing (unlimited)
does not protect against	meaconing jamming	meaconing jamming	meaconing jamming	meaconing jamming
not affects	intrusion interference	intrusion interference	intrusion interference	intrusion interference

MIJI: meaconing (replay attack, valid data)
MIJI: intrusion (unauthorized access to communication channel)
MIJI: jamming (DDoS, valid/invalid data)
MIJI: interference (noise)
spoofing (invalid/modified data)

GNSS - GPS (US) spoofing

E-GROUP
SOFTWARE & BEYOND

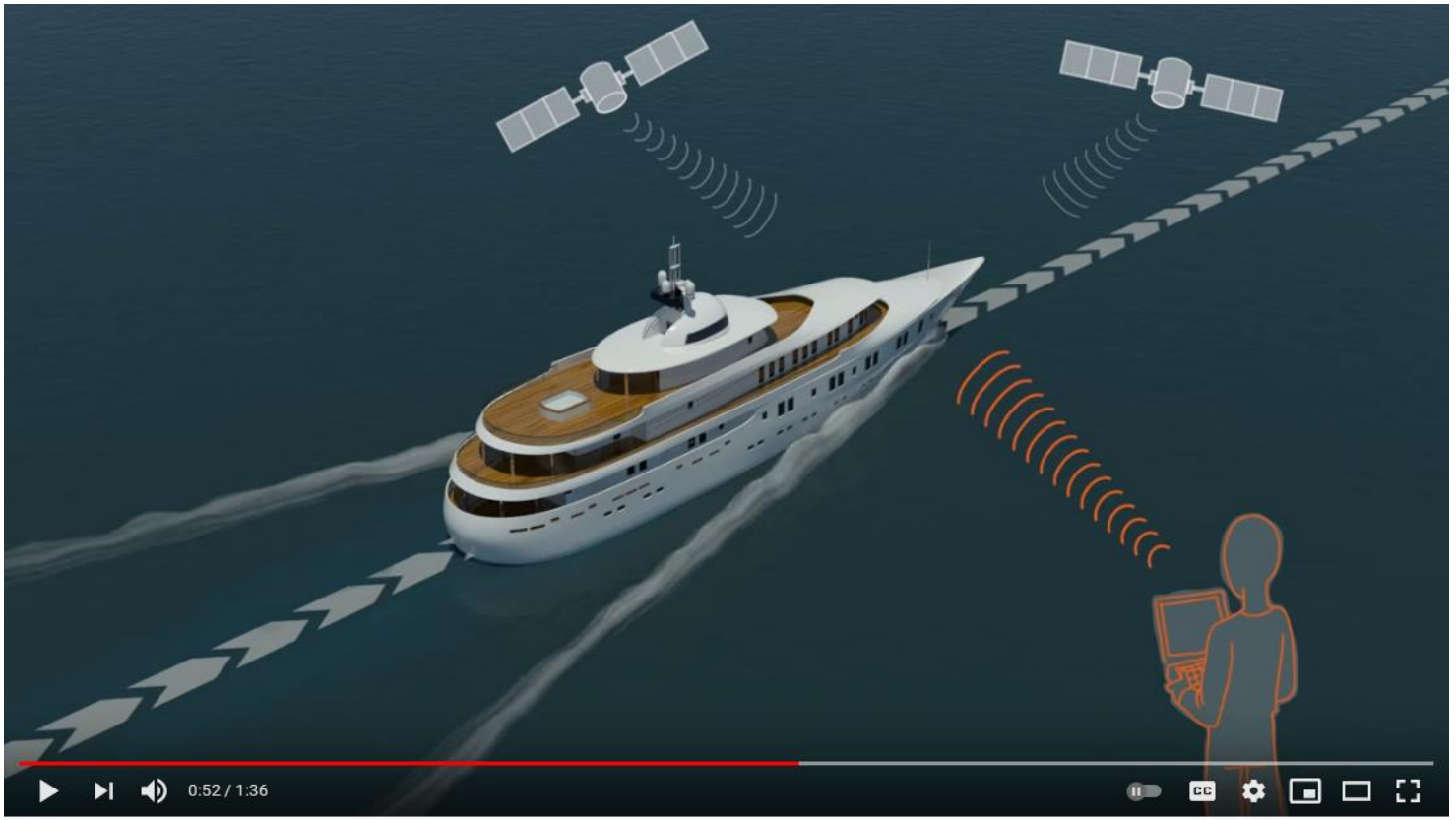
2011-12-04 Lockheed Martin RQ-170 Sentinel was captured by Iranian forces



GNSS – GPS (US) spoofing

E-GROUP
SOFTWARE & BEYOND

2013-07-29 yacht was hijacked from 50 km by University of Texas students



Spoofing on the High Seas

605,572 views • Jul 29, 2013

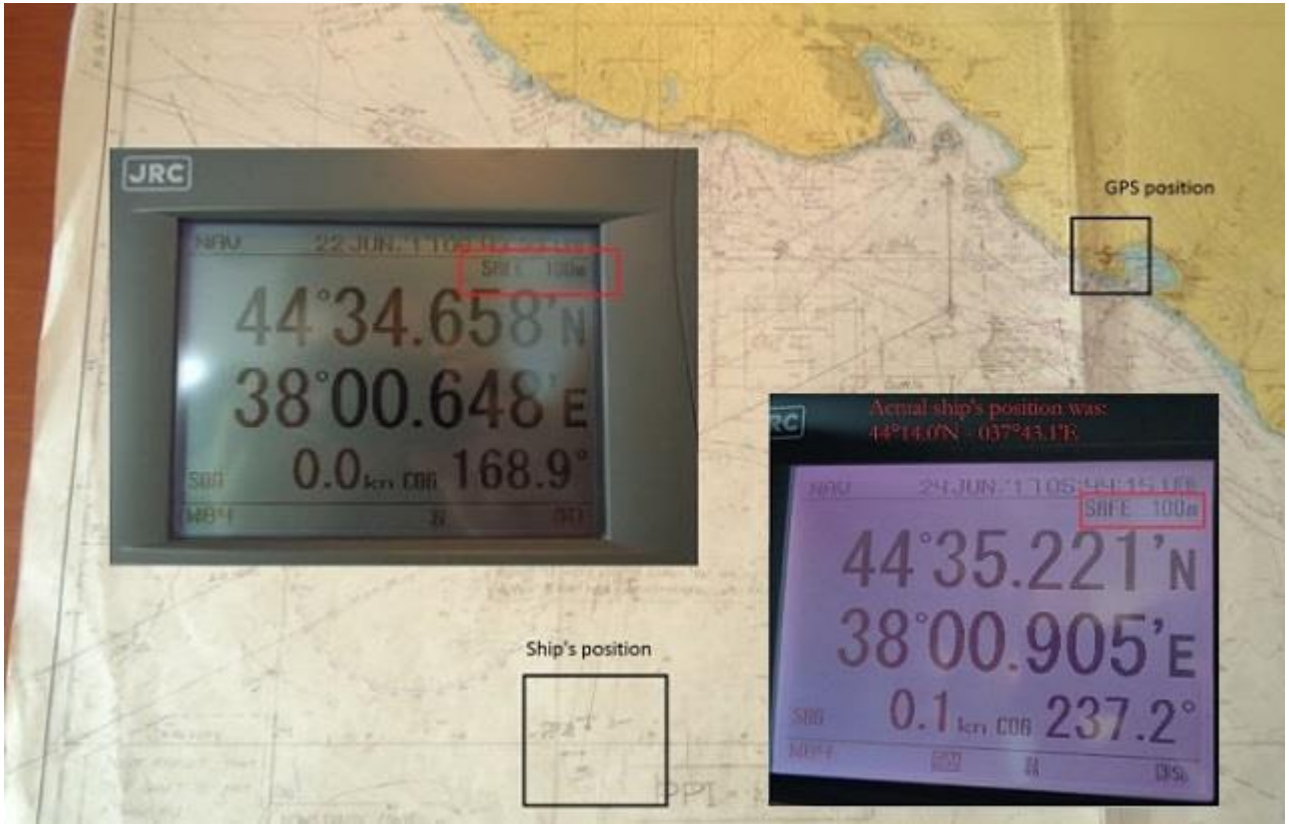
GNSS – GPS (US) spoofing

E-GROUP
SOFTWARE & BEYOND

2016-07-15 Pokemon GO was hijacked by HackRF SDR of Stefan Kiese
2018-08-17 $225 cost HackRF SDR was demonstrated by Chinese students

GNSS – GPS (US) spoofing

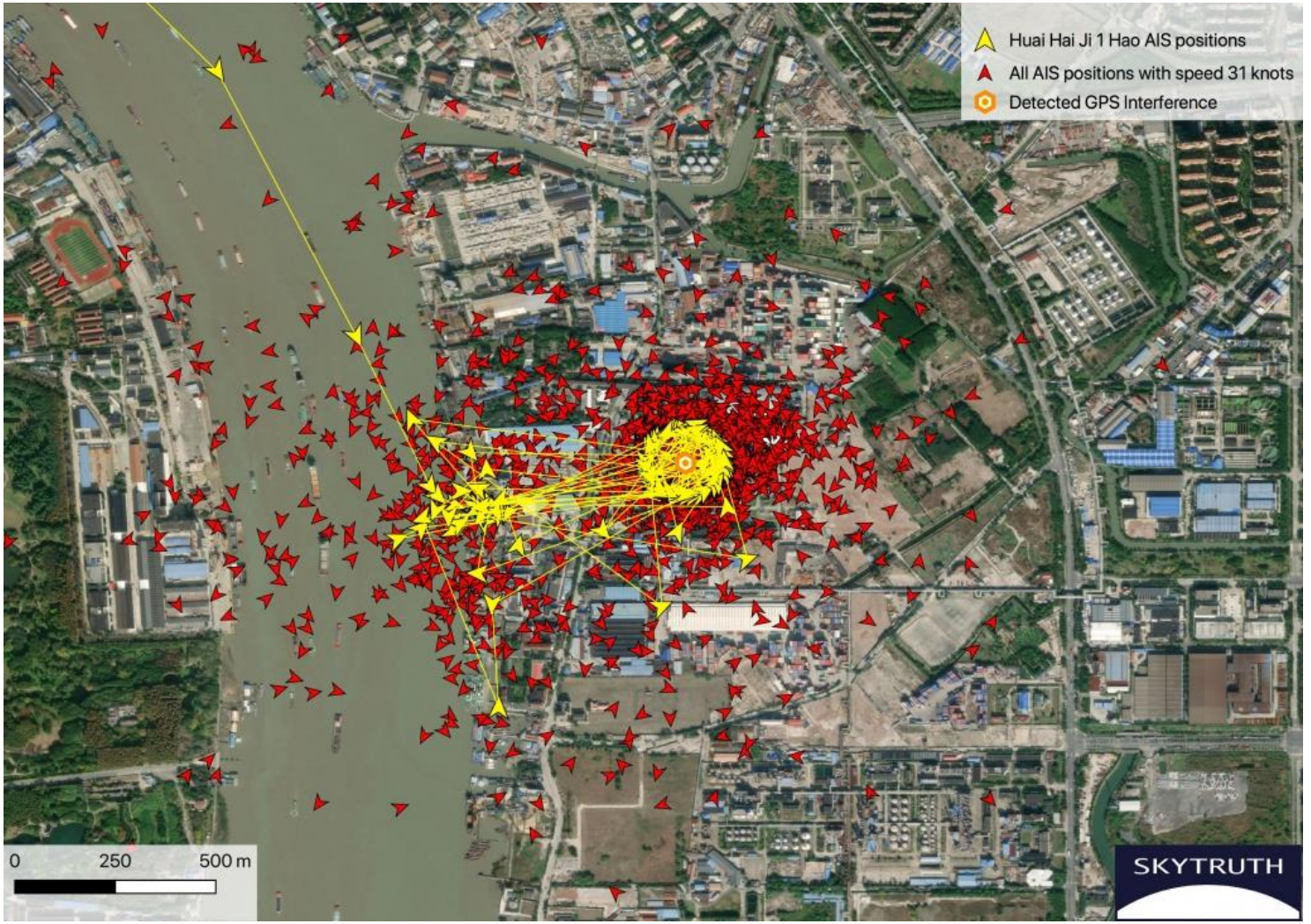
2017-06-22 ships were hijacked in the Black Sea by Russian forces



GNSS - GPS (US) spoofing

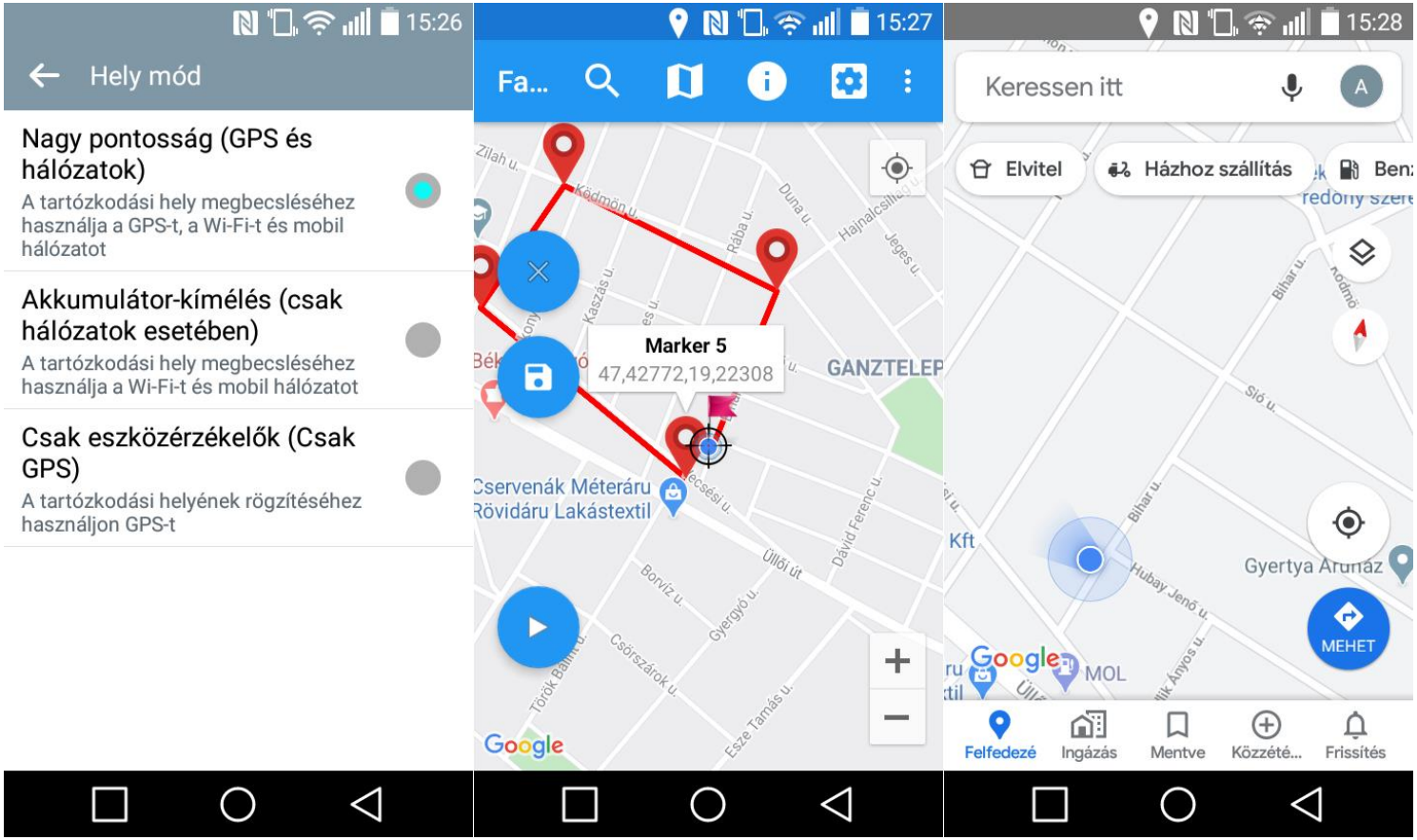
E-GROUP
SOFTWARE & BEYOND

2019-11-15 ships are cloned at port of Shanghai by Chinese smugglers



GNSS - GPS (US) spoofing

nowadays free apps can spoof mobile GPS (US) sensors by users



GNSS – GPS (US) spoofing

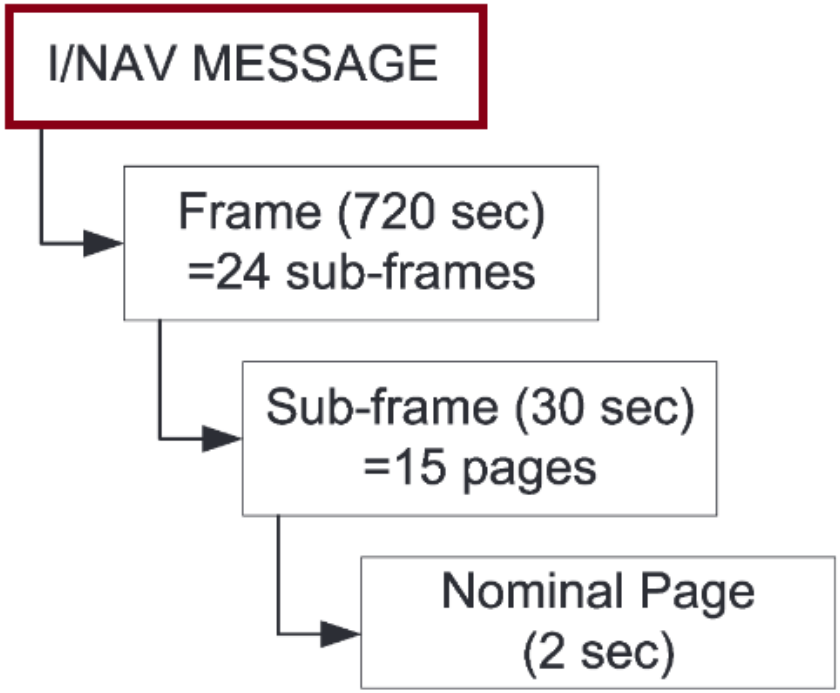
E-GROUP
SOFTWARE & BEYOND

nowadays free apps can spoof mobile GPS (US) sensors by users

- no root/jailbreak of device is needed
  (any device on market is suitable for this)
- no additional datasources can protect
  (Wi-Fi, GSM information beyond GPS are not sufficient)
- no high attack potential is required
  (any user can perform this as a one-click-hack)
- fake geolocation can be set
  (fixed positions)
- fake route can be set
  (series of positions with pre-set speed of movement)

GNSS - GALILEO (EU) protection

E1-B page contains OSNMA cryptographic layer



OSNMA
Open Service
Navigation Message Authentication

TESLA
IETF RFC 4082
Timed Efficient Stream
Loss-Tolerant Authentication

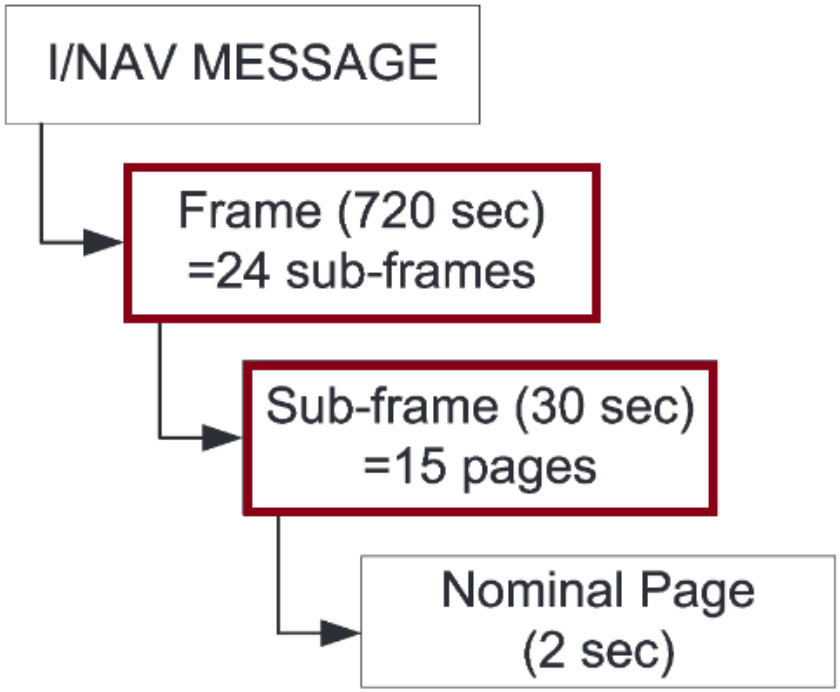
asymmetric key protects K0/KROOT TESLA key
symmetric key Kn is used to derive K0/KROOT
symmetric key protects navigation data

protected navigation data:
- ephemeris parameters
- time and clock correction parameters
- service parameters
- almanac parameters

GNSS - GALILEO (EU) protection

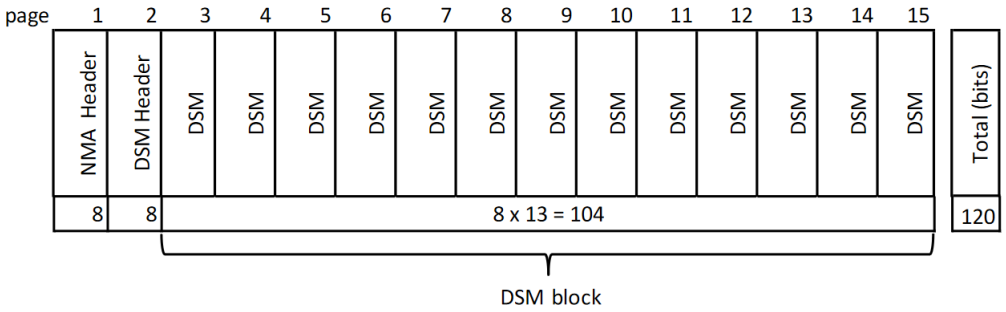
E-GROUP
SOFTWARE & BEYOND

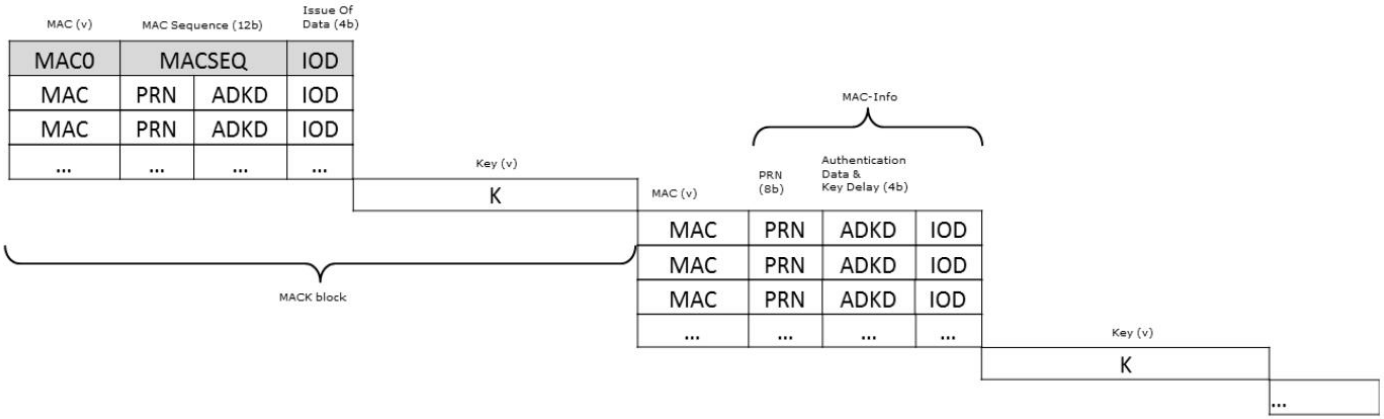
E1-B page contains OSNMA cryptographic layer



1 frame = 24 sub-frames
1 sub-frame = 15 pages

15 x 8 bits = 120 bits HKROOT
15 x 32 bits = 480 bits MACK

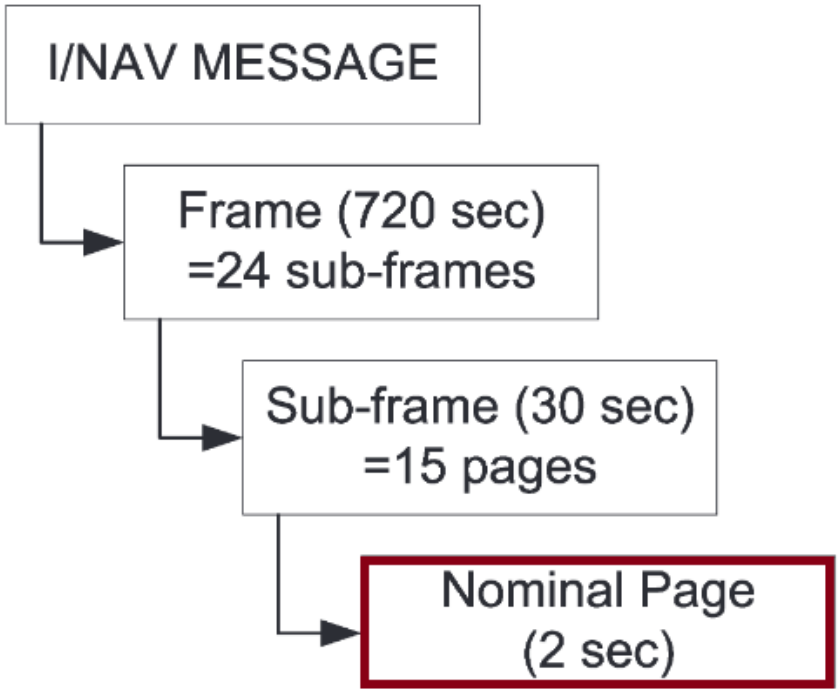




GNSS - GALILEO (EU) protection

E-GROUP
SOFTWARE & BEYOND

E1-B page contains OSNMA cryptographic layer



E1-B

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

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

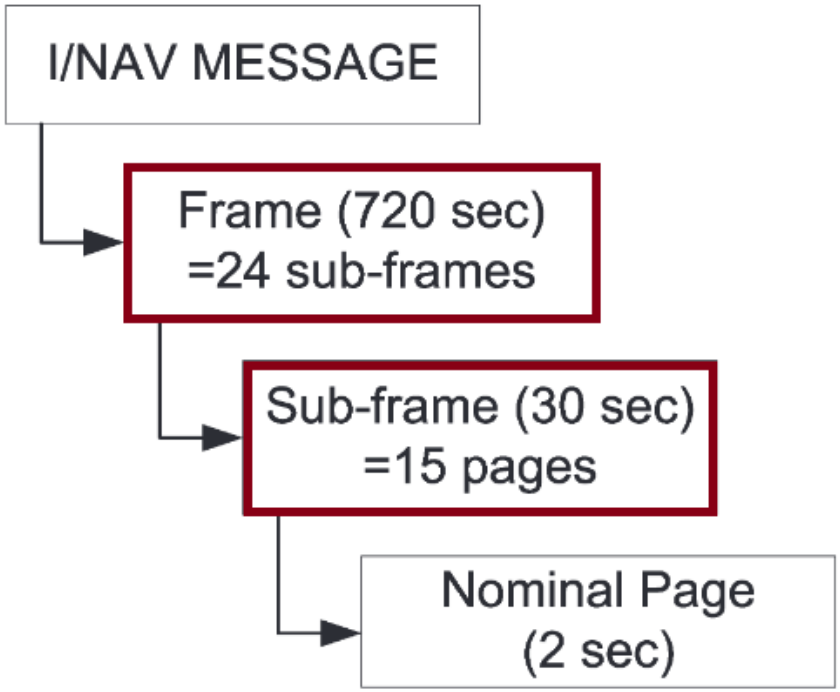
HKROOT	MACK
8	32

```
# GPSTest version: v3.8.4 (18076-google), Manufacturer: Xiaomi, Model: MI 8, GNSS HW Year: 2018, Platform: 8.1.0, API Level: 27
Nav,Svid,Type,Status,MessageId,Sub-messageId,Data(Bytes, 8-bit signed integer)
Nav,  15,1537,     1,       24,            2,2,0,113,-122,89,126,-118,30,-123,127,-79,93,16,108,-128,
                                            -125,1,88,-121,44,-91,-32,-86,-86,-86,83,49,83,63,64

Galileo I/NAV message (1537, 0x00000601), E1-B, 1=odd, "Reserved 1"="OSNMA" 40 bits (8 bits HKROOT + 32 bits MACK)
_____________________________________________________________________________________________________________
1       81      81      81      81      81      81      81      81      81      81      81      81      81      81      8
0000001000000000011100011000011001011001011111101000101000011110100001010111111110110001010111010001000001101100000
1       2       3       4       5       6       7       8       9       10      11      12      13      14      15

_____________________________________________________________________________________________________________
1       81      81      81      81      81      81      81      81      81      81      81      81      81      81      8
1000001100000001010110001000011100101100101001011110000010101010101010101010010100110011000101010011001111101000000
16      17      18      19      20      21      22      23      24      25      26      27      28      29      30
                <HKROOT><-------------MACK------------->
                01100010000111001011001010010111100000 10
```

GNSS - GALILEO (EU) protection

E-GROUP
SOFTWARE & BEYOND

E1-B page contains OSNMA cryptographic layer

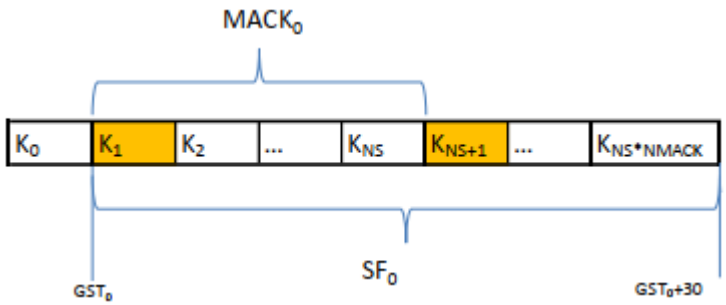


K1 TESLA key protects navigation data (HMAC)

Key index	WN	TOW	Key bits
414720	947	604770	0xA8F6692E5C1258E3CCF941ADBAF21615
414719	947	604770	0xF7CFDA81E1C4E83B227F18F0F226ADC6
414718	947	604770	0xD35422AB710779BE8ADF24013D9230A6
...	...	...	...
108	947	432030	0x5EA3A18FB127D4C7B31812C382D4C96D
...	...	...	...
73	947	432030	0x4E0E2DA7F80F547B874D4A2533316389
72	947	432000	0x47F767BFDC6674B6F108BE17A0198751
71	947	432000	0x3CA9190D0B21026D70E7FF8BAD6C6ED0
...	...	...	...
2	947	432000	0x22B30FBEE8C6C4A43480AF28A67D4A65
1	947	432000	0x81AEE575195E13C06961A705A191B9CD
0	947	431970	0xEE6772D9AB8396866DC57EADA1D29637

K1 is used to derive K0/KROOT (SHA-256)

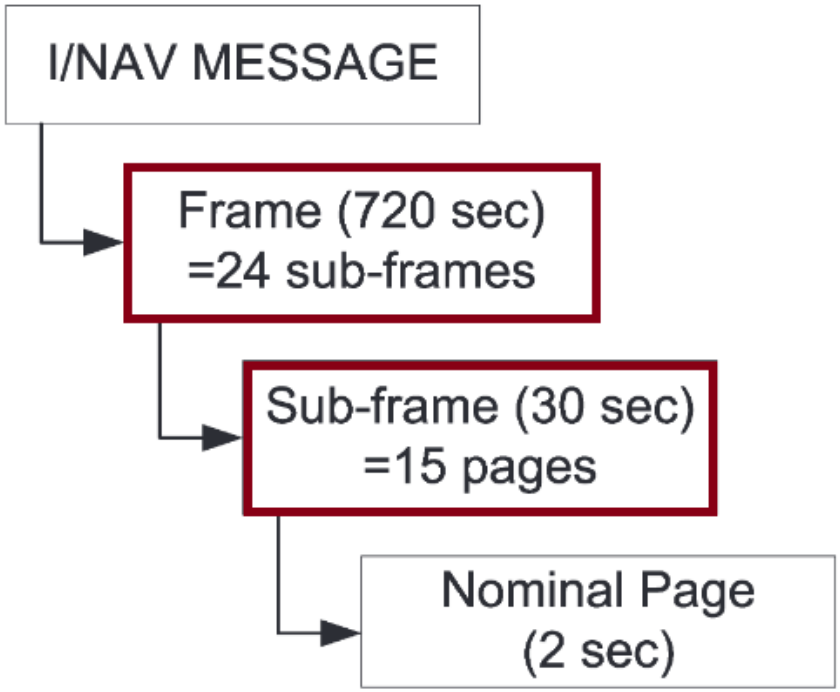
```
m0 = (K1 || GSTsf || Alpha || P3)
0x81AEE575195E13C06961A705A191B9CD3B369762F1CA3856A975
0xEE6772D9AB8396866DC57EADA1D29637
```



GNSS - GALILEO (EU) protection

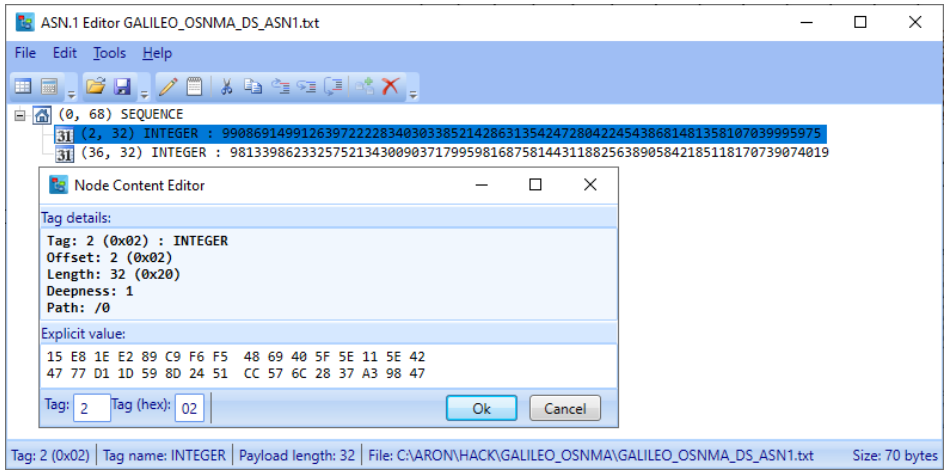
E-GROUP
SOFTWARE & BEYOND

E1-B page contains OSNMA cryptographic layer

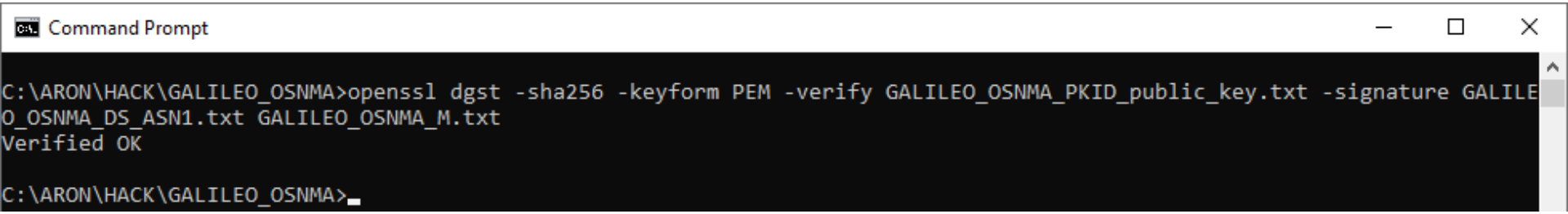


ECDSA protects K0/KROOT TESLA key (P-256)

```
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEc7RAsKw8qkRfvlVvn4p4la1XX0K0
rTSveYwqGMW8OovntszzLiy4dTGcSkvwo0gejSbRjkRnMpQBta/RDLnWOA==
-----END PUBLIC KEY-----
```




```
M = (NMA_Header || CIDKR || NMACK || HF || MF || KS || MS || MACLT || Rsvd || MO || KROOT WN || KROOT TOWH || Alpha || KROOT)
0x8220410B03B378F1CA3856A975EE6772D9AB8396866DC57EADA1D29637
```



GNSS - GALILEO (EU) pros/cons

E-GROUP
SOFTWARE & BEYOND

pros

- spoofing-resistant navigation systems for civilian services used by humans or vehicle (regular or self-driving/autonomous ground units, aircrafts, watercrafts)
- enhanced secure access control (enforce geofencing rules of IT systems beyond 2FA at government, banking, healthcare sector)
- person tracing (COVID-19 contact tracing, monitoring criminals, illegal migrants, security guards protecting a physical area)
- fighting against fake news (protected geolocation and time in JPEG/Exif tag)

PATROL
(Position Authenticated Tachograph foR OSNMA Launch)

GNSS – GALILEO (EU) pros/cons

E-GROUP
SOFTWARE & BEYOND

pros

- spoofing-resistant navigation systems for civilian services used by humans or vehicle (regular or self-driving/autonomous ground units, aircrafts, watercrafts)
- enhanced secure access control (enforce geofencing rules of IT systems beyond 2FA at government, banking, healthcare sector)
- person tracing (COVID-19 contact tracing, monitoring criminals, illegal migrants, security guards protecting a physical area)
- fighting against fake news (protected geolocation and time in JPEG/Exif tag)

cons

- lack of OSNMA-enabled signal
  GALILEO (EU) itself has been started on 2016-12-15 but OSNMA is still in testing phase and is not provided in production environment as part of the signal
- lack of OSNMA-enabled HW
  GALILEO (EU) itself is supported by mobile/tablet and wearable device vendors, but OSNMA cryptographic layer is not processed (except Broadcom BCM47755)
- lack of OSNMA-enabled SW
  GALILEO (EU) itself is supported by e.g. Android since API level 24, but automatic switching between data-component and pilot-component of E1-B shall be controlled

GNSS - GALILEO (EU) references

E-GROUP
SOFTWARE & BEYOND

useful links

https://www.euspa.europa.eu/
sites/default/files/expo/2.6_carlo_sarto_qascom.pdf

https://www.euspa.europa.eu/
simplecount_pdf/tracker?file=expo/2.4_moises_navarro-gallardo_-_airbus_-_guidelines_os_nma_implementation_in_smartphones.pdf

https://datatracker.ietf.org/
doc/html/rfc4082

https://insidegnss.com/
category/a-system-categories/galileo/

https://www.esa.int/
Applications/Navigation/Galileo

http://www.kormanyablak.org/
it_security/2021-07-04.php

E-GROUP SOFTWARE & BEYOND
NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE HUNGARY
No. 2019-1.3.1-KK-2019-00011
PROJECT
FINANCED FROM
THE NRDI FUND