GPS SPOOFING OF UAV

YUAN Jian
Unicorn Team – Radio and Hardware Security Research
Qihoo 360 Technology Co. Ltd.

Who we are? Unicorn Team

- Qihoo360's UnicornTeam consists of a group of brilliant security researchers. We focus on the security of anything that uses radio technologies, from small things like RFID, NFC and WSN to big things like GPS, UAV, Smart Cars, Telecom and SATCOM.
- Our primary mission is to guarantee that Qihoo360 is not vulnerable to any wireless attack.
- During our research, we create and produce various devices and systems, for both attack and defense purposes.

Beginning of the story …

Civilian-use GPS C/A Signal

GPS C/A signal is for civilian usage, and unencrypted.

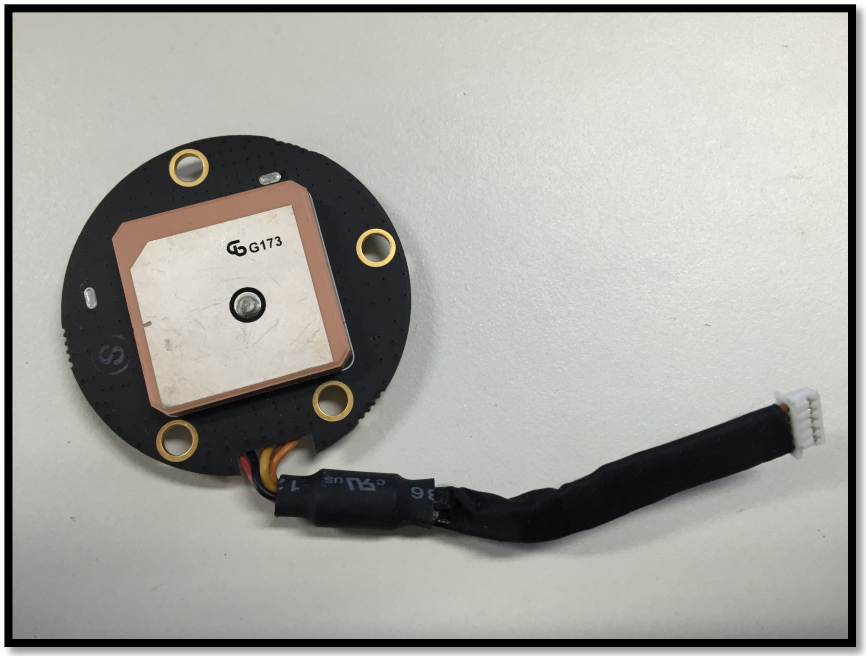
Replay attack is a typical GPS spoofing method.

Record

Replay

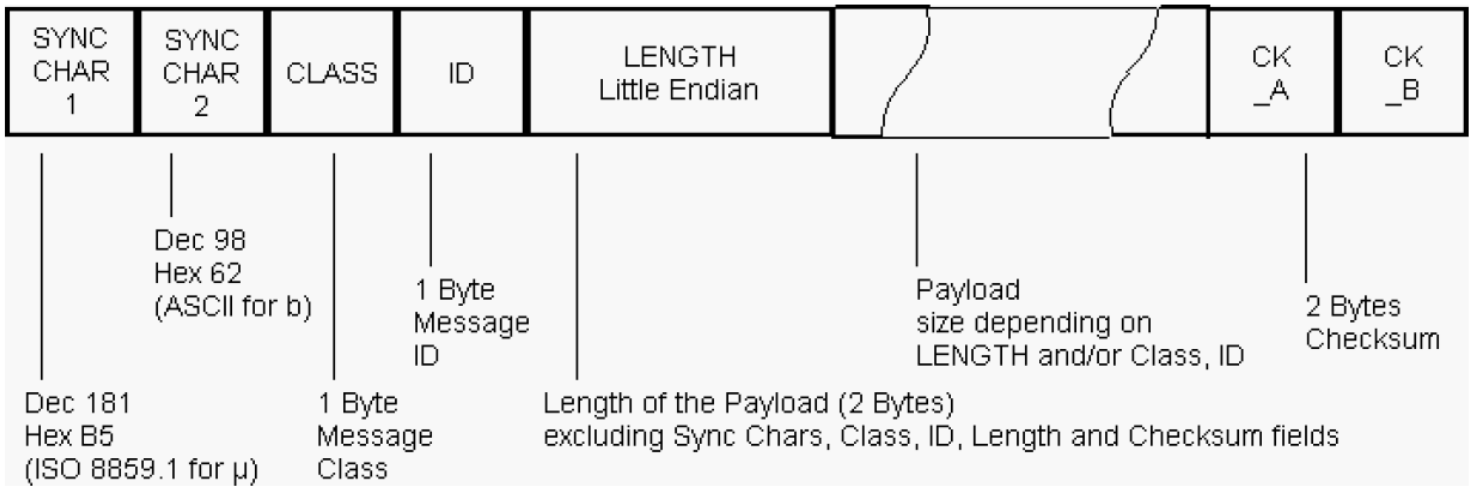
Spoof UAV In It

- GPS Module

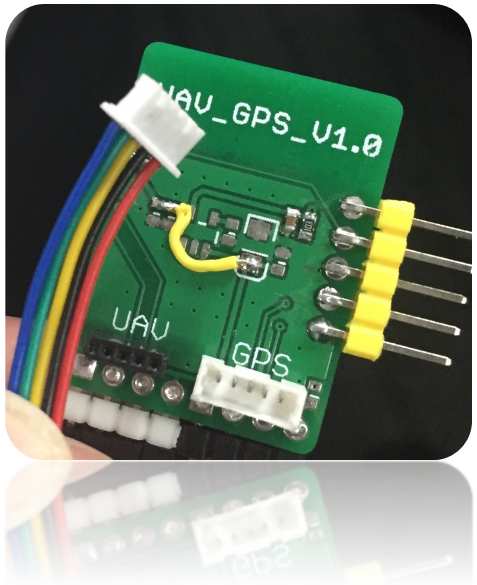


How to spoof GPS of UAV?

Data Format


SYNC CHAR 1
SYNC CHAR 2
CLASS
ID
LENGTH Little Endian
CK _A
CK _B
Dec 98
Hex 62
(ASCII for b)
1 Byte Message ID
Payload size depending on LENGTH and/or Class, ID
2 Bytes Checksum
Dec 181
Hex B5
(ISO 8859.1 for µ)
1 Byte Message Class
Length of the Payload (2 Bytes)
excluding Sync Chars, Class, ID, Length and Checksum fields

So, we made tools



Key Features

- Direct Mode : never change anything.
- Suspend Mode : UAV would receive nothing.
- Replace Mode: change to any place you want.
- Offset Mode: add some offset to current position.

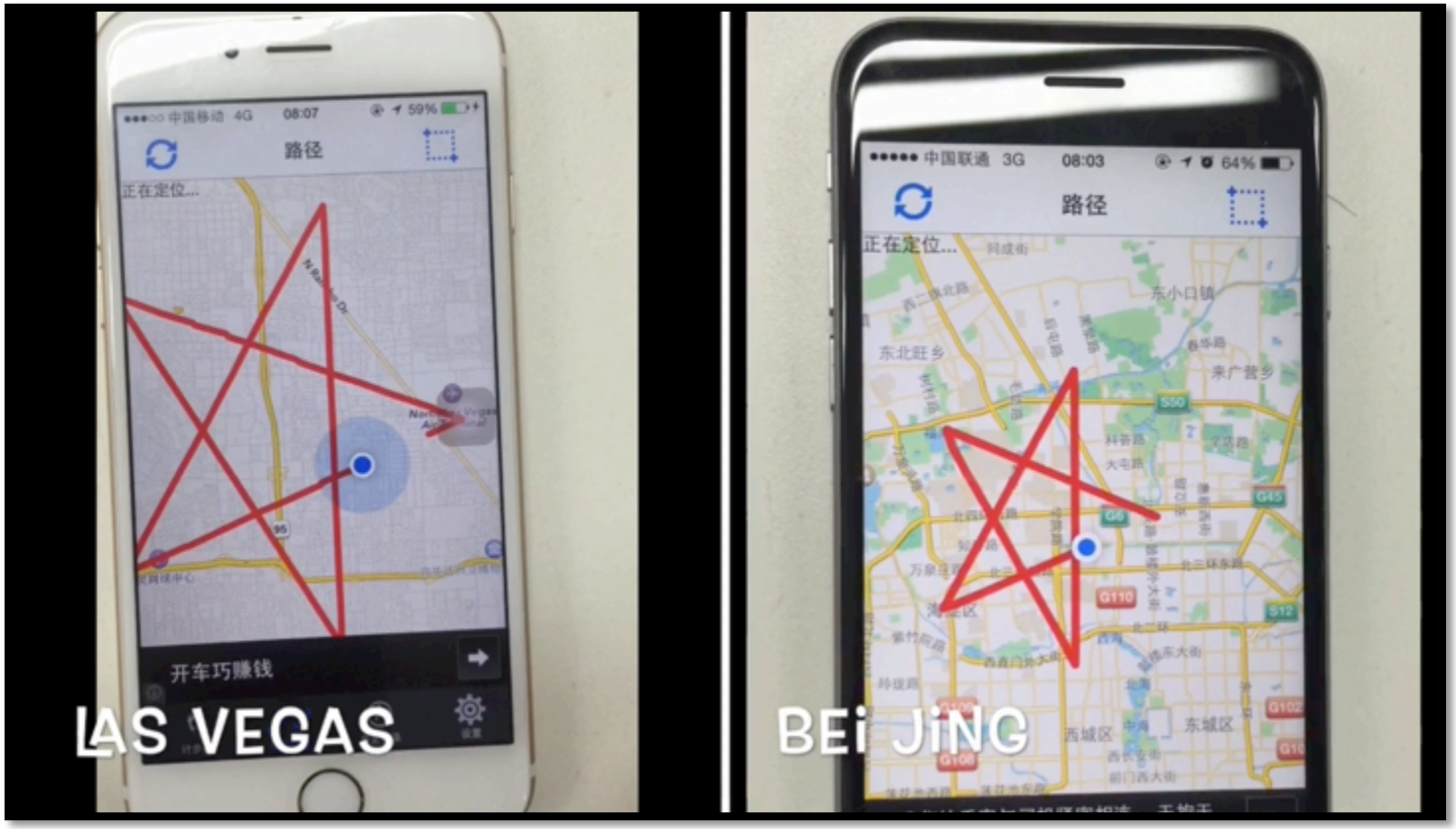
360UNICORNTEAM

Another Way

If Create any GPS signal
rather than Record & Replay…

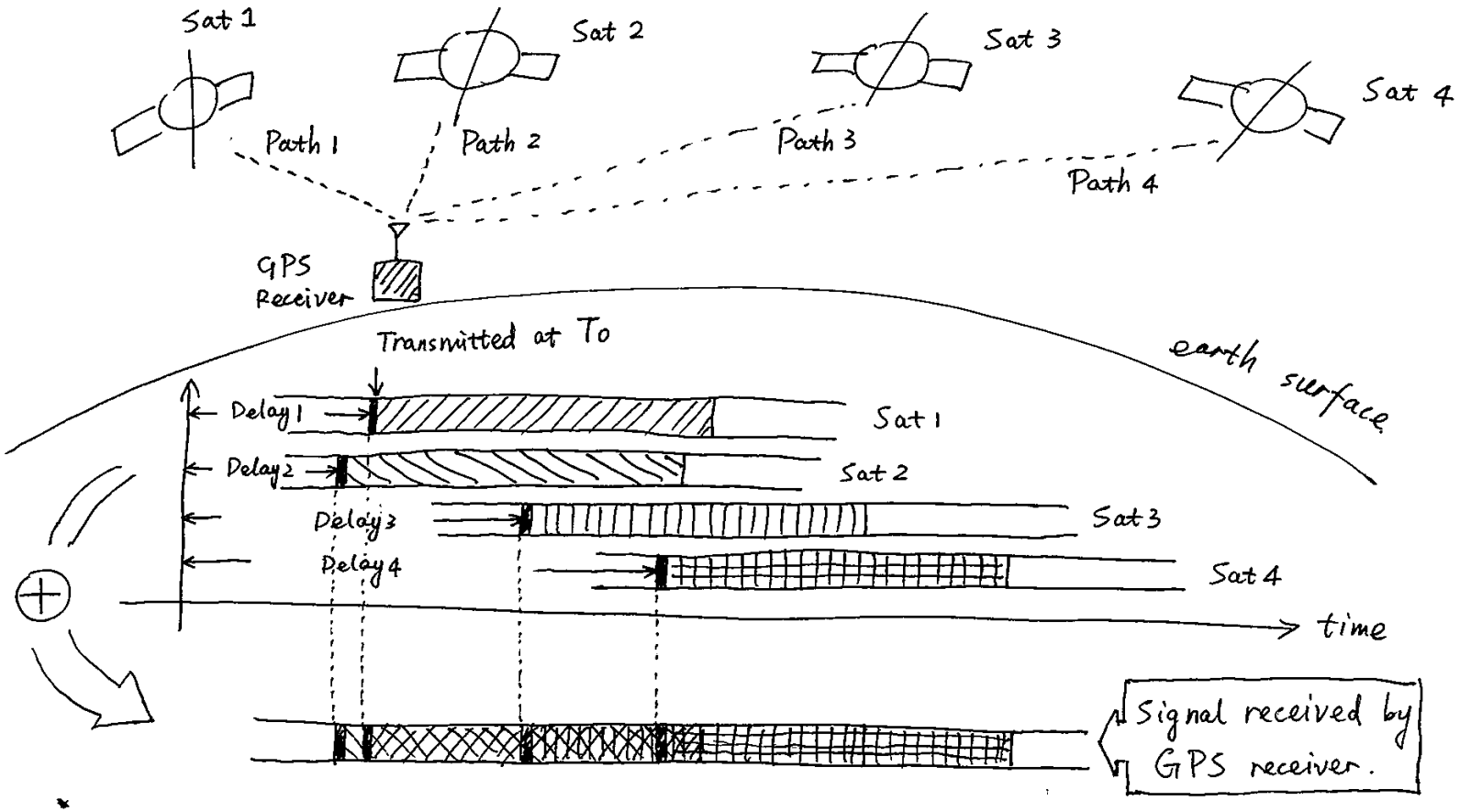
This is not a replay

- Motion curve



Basic principle of GPS system

GPS principle



Key information in Pseudo-range equations

$$\begin{cases} (T + D_1 - T_0) \cdot C = Pos(x_1, y_1, z_1) - Pos(x, y, z) \\ (T + D_2 - T_0) \cdot C = Pos(x_2, y_2, z_2) - Pos(x, y, z) \\ (T + D_3 - T_0) \cdot C = Pos(x_3, y_3, z_3) - Pos(x, y, z) \\ (T + D_4 - T_0) \cdot C = Pos(x_4, y_4, z_4) - Pos(x, y, z) \end{cases}$$

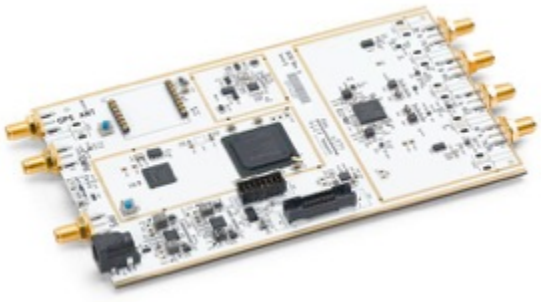
Calculate the delays at receiver

WHEN

WHERE

we have

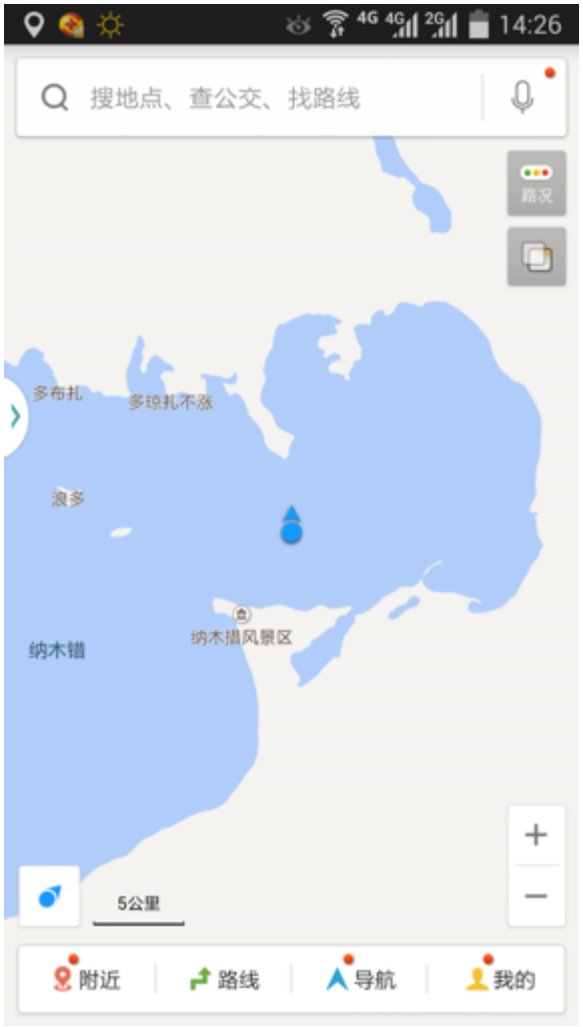
USRP



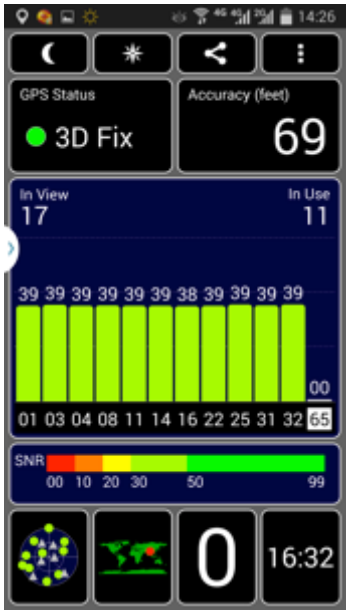
bladeRF

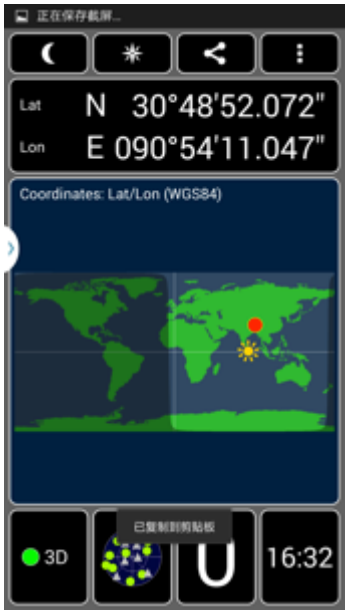
HackRF

Bingo! Samsung Note 3

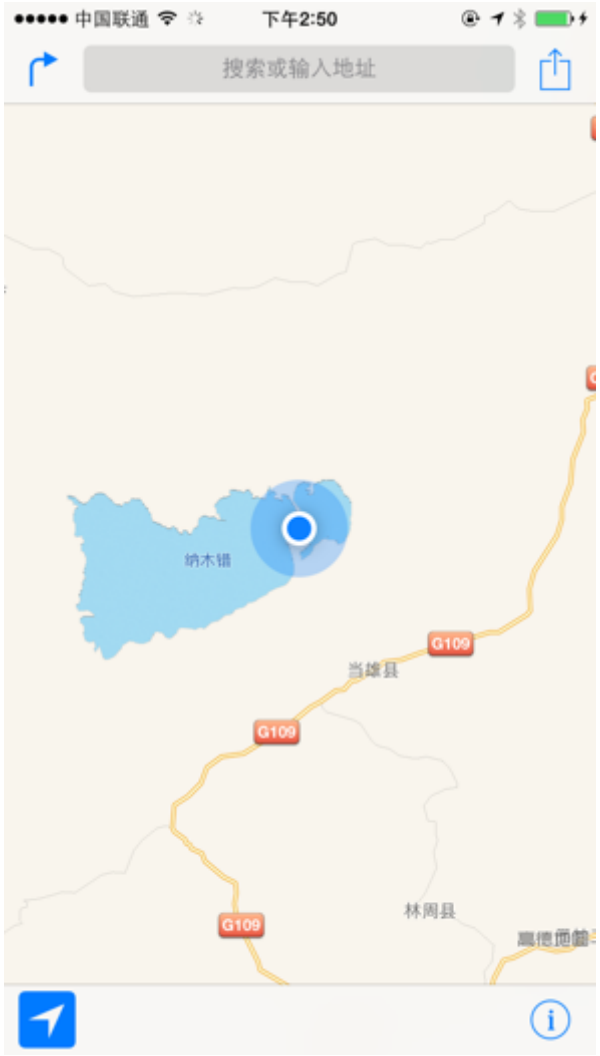


- Located at Namco Lake in Tibet but the cellphone is actually in Beijing.

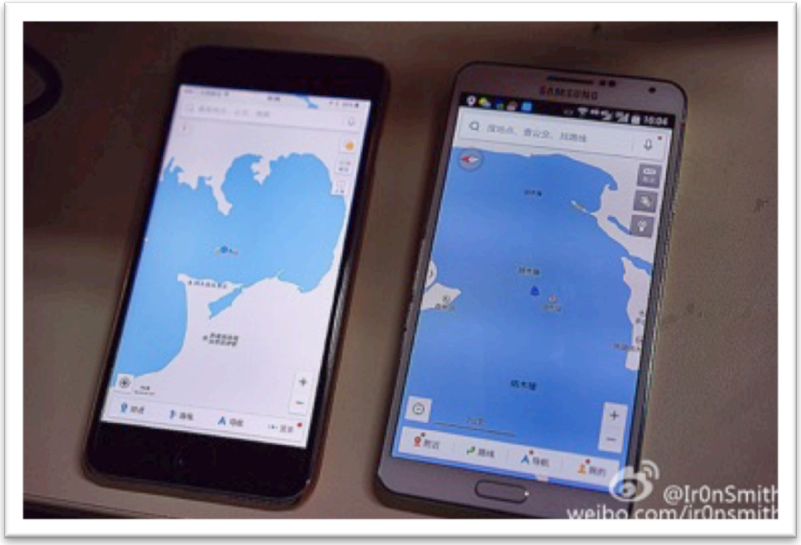




Bingo! iPhone 6



- Namco Lake in Tibet
- iPhone positioning is much slower.
- The cellphone clock was also reset to wrong time if auto-calibration is enabled.



DJI drone - forbidden area policy

- To avoid the risk from drone,to people and to critical facilities, drone flying are forbidden in many cities.

- For example, DJI drone's engine will keep off when it finds the position is in forbidden area.

A drone that crashed on the grounds of the White House had evaded radar detection.

Try to spoof cars

- The car, BYD Qin,was located in a lake center.

Lessons – how to anti-spoof

- Application layer
  - Now usually GPS has highest priority. Cellphone is spoofed even if it has cellular network connection.
  - Use multi-mode positioning, GLONASS, Beidou
  - Jointly consider cellular network and wifi positioning
- Civil GPS receiver chipset
  - Use some algorithms to detect spoofing
- Civil GPS transmitter
  - Add digital signatures into the extensible GPS civil navigation message

GPS is still a great system

- First global positioning system
- Usable for all of the world
- Very low cost, small size…

- It keeps updating,so we believe the security issue will be improved in future.

Thank you!