Security in Radio Communications

Radio - common use-cases

- Why & when do we use radios?
- How far does the signal reach?
- How do we know its source?

Rules in radio communications

- Assume everyone is listening to everything you send.
- Assume anyone wants to jam you.
- Assume anyone wants to impersonate you.

Rules in radio communications

- Assume everyone is listening to everything you send.
- Assume anyone wants to jam you.
- Assume anyone wants to impersonate you.

Now try to send messages securely.

Number stations

Old school radio security (cold-war era):

https://www.youtube.com/watch?v=qyRpT-u44pU

- Messages are sent by a high-powered fixed installation (shortwave band).
- The transmitter can cover half a continent.
- Only the intended receivers can decode the message.

Number stations

Old school radio security (cold-war era):

https://www.youtube.com/watch?v=qyRpT-u44pU

- Receivers have plausible deniability (for reception, common SW receivers were used).

- Because they don’t have to transmit, they do not reveal their locations.

Number stations

Old school radio security (cold-war era):

https://www.youtube.com/watch?v=qyRpT-u44pU (numbers start at 2:50)

As good as it gets:

- The message has to go through, even with glitches
  - low throughput must be used.
- Modern communications uses ARQ (Automatic Repeat reQuest)
  - but this means the receiver must reveal his position.

Number stations

Still used (according to the FBI):

http://www.bbc.com/future/story/20170801-the-ghostly-radio-station-that-no-one-claims-to-run

It also fits with a series of **arrests across the United States** back in 2010. The FBI announced that it had broken up a “long term, deep cover” network of Russian agents, who were said to have received their instructions via coded messages on shortwave radio – specifically 7887 kHz.

Number stations

Some are still operational.
Search for **UVB-76**.

Try it at home!

Broadcast area	Russia
Frequency	4625 kHz Shortwave
Format	Repeated buzzing sound
Language(s)	Russian
Former callsigns	УВБ-76, МДЖБ, ЖУО3
Former frequencies	4625 kHz
Owner	Russian Armed Forces
Sister stations	The Pip, The Squeaky Wheel

https://en.wikipedia.org/wiki/UVB-76

Why some locations should be kept secret

While in a secret locations, don’t post check-ins on Facebook.

Should be obvious, right?

Why some locations should be kept secret

While in a secret locations, don't post check-ins on Facebook.

Should be obvious, right?

Right !?

https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Fitness tracking app Strava gives away location of secret US army bases

Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities

Latest: Strava suggests military users 'opt out' of heatmap as row deepens

▲ A military base in Helmand Province, Afghanistan with route taken by joggers highlighted by Strava. Photograph: Strava Heatmap

Why some locations should be kept secret

While in a secret locations, don't post check-ins on Facebook.

Should be obvious, right?

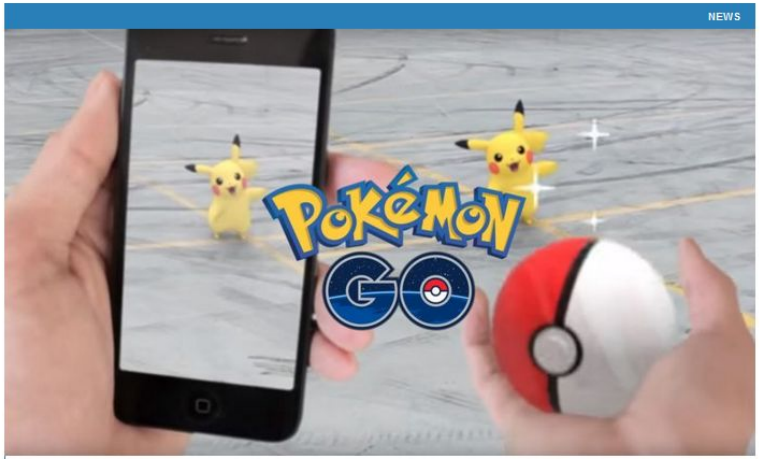
Right !?

Oh, come on…

https://www.cultofmac.com/438174/china-is-worried-pokemon-go-will-uncover-secret-military-bases/

China is worried *Pokémon Go* will uncover secret military bases

BY LUKE DORMEHL • 5:54 AM, JULY 15, 2016



All your base are belong to Pikachu.
Photo: Niantic Labs

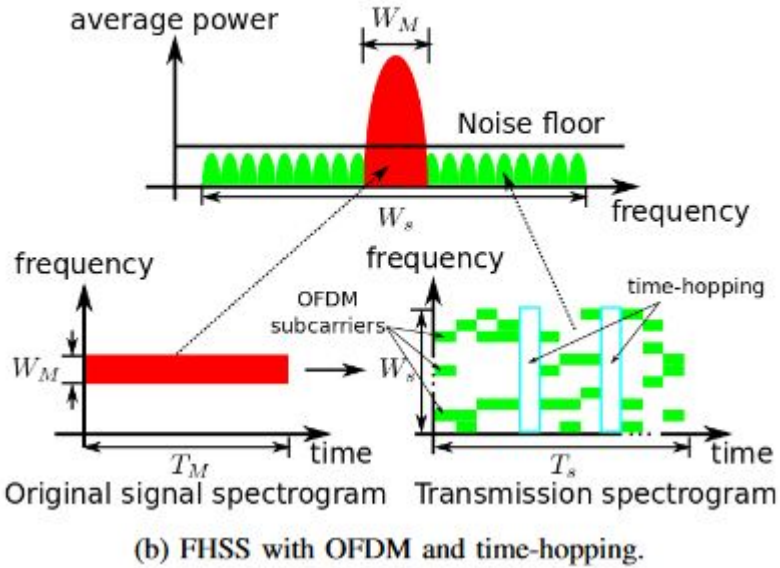
With *Pokémon Go* mania running wild, did you really think the worst that might happen was some would-be Ash Ketchum stumbling across a dead body?

Modern solutions to hide the transmission

A transmitter can either transmit the payload straight ahead, or use a frequency-hopping spread-spectrum solution.

This makes easier to hide the signal under the noise floor.

Demo: http://websdr.yo3ggx.ro:8765/



(b) FHSS with OFDM and time-hopping.

https://arxiv.org/pdf/1506.00066.pdf

Walkie talkies… and the illusion of privacy

Regular walkie talkies (PMR446 devices) have a short range (few blocks, less than 1 Watt) and can be used by anyone.

These also allow “coded channels”... but these are not secure.

Professional radios

These are not secure either (mostly).

The communication is protected by law (enforced by ANRCTI):

- Protected against interference
- Protected against unauthorized transmissions

Demo 173.030MHz .

Professional radios

Shouldn’t this communication be secure?

Professional radios

Shouldn’t this communication be secure?

Not necessarily - the communications are not sensitive, and making them encrypted would also make them more unreliable.

Professional radios

Shouldn’t this communication be secure?

Not necessarily - the communications are not sensitive, and making them encrypted would also make them more unreliable.

But some services still need secure communications.
This is why the police, army, etc. use encrypted channels.

Radios in aviation

Airplanes report their position and bearing over ADS-B.
(plaintext, unencrypted, unauthenticated protocol).

Airplane pilots are trained to rely more on the automated TCAS warnings than on Traffic Control's instructions.
(TCAS = traffic collision avoidance system)

The data must be confirmed by the airplane's radar before taken into account.
Why?

Amateur radios

By law, amateur radio operators must not use encryption.

People use the allocated frequencies just for fun.

Demo: http://aprs.fi/
Demo: RoLink/YO3KXL (439.075MHz) FT8 on 20m and http://pskreporter.info/

Satellite communications - ISEE-3

- **International Sun-Earth Explorer-3.**
- Launched in 1978.

- Became the first spacecraft to visit a comet, passing through the plasma tail of Giacobini-Zinner comet within about 7,800 km (4,800 mi) of the nucleus on September 11, 1985.

- NASA suspended routine contact with ISEE-3 in 1997.

Satellite communications - ISEE-3

- “Reboot” effort appeared in 2014.
- No encryption, no authorization needed.
- Obsolete hardware had to be rebuilt.
- Required a 70-meter antenna to transmit the signal.

https://en.wikipedia.org/wiki/Goldstone_Deep_Space_Communications_Complex

Satellite communications - ISEE-3

- Control was regained (by a team of volunteers) for a few days.
- The satellite went unresponsive shortly after.

Satellite communications - Voyager 2

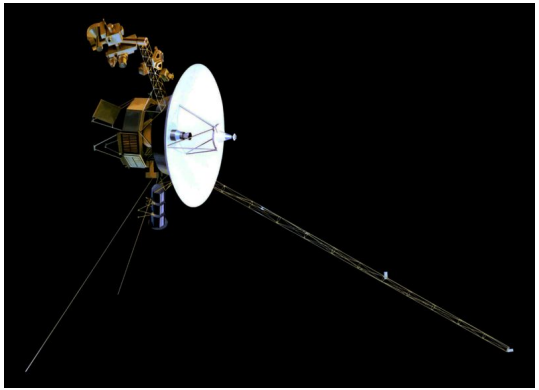
- Voyager 2 was launched in 1977.

- In 2010, the memory chips on the Voyager 2 probe got corrupted.
- A team of engineers had to send the “reboot” command to the probe.

- The probe is so far, it has a Round-Trip Time of 26 hours!
- The probe reached interstellar space in December 2018 and it’s still transmitting data.

Earlier this month, engineers suspended Voyager 2's science measurements because of an unexpected problem in its communications stream. A glitch in the flight data system, which formats information for radioing to Earth, was believed to be the problem. Engineers were able to replicate the glitch in a computer lab, showing that a single bit flip was responsible. NASA plans to reset Voyager's memory tomorrow.

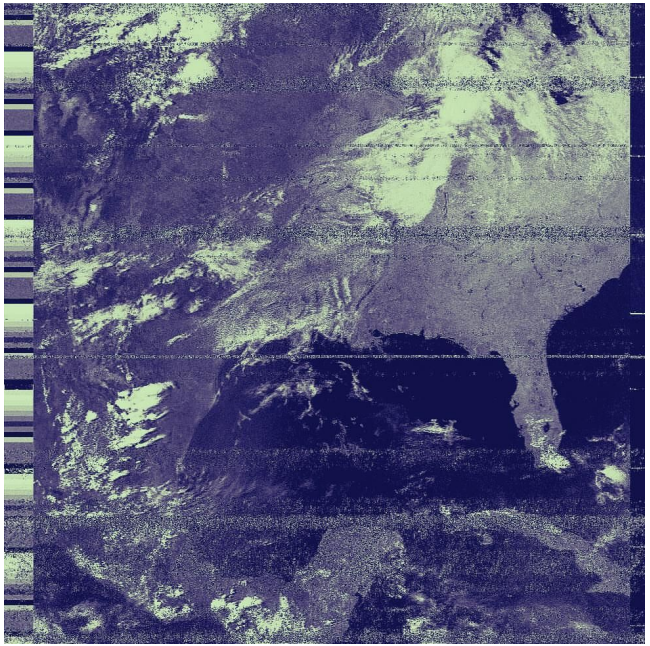
The spacecraft is so far away it takes nearly 13 hours for a radio signal from Earth, traveling at the speed of light, to reach it, and another 13 hours to receive a response.



https://www.zdnet.com/article/nasa-to-reset-voyager-2-memory/

Satellite communications - weather

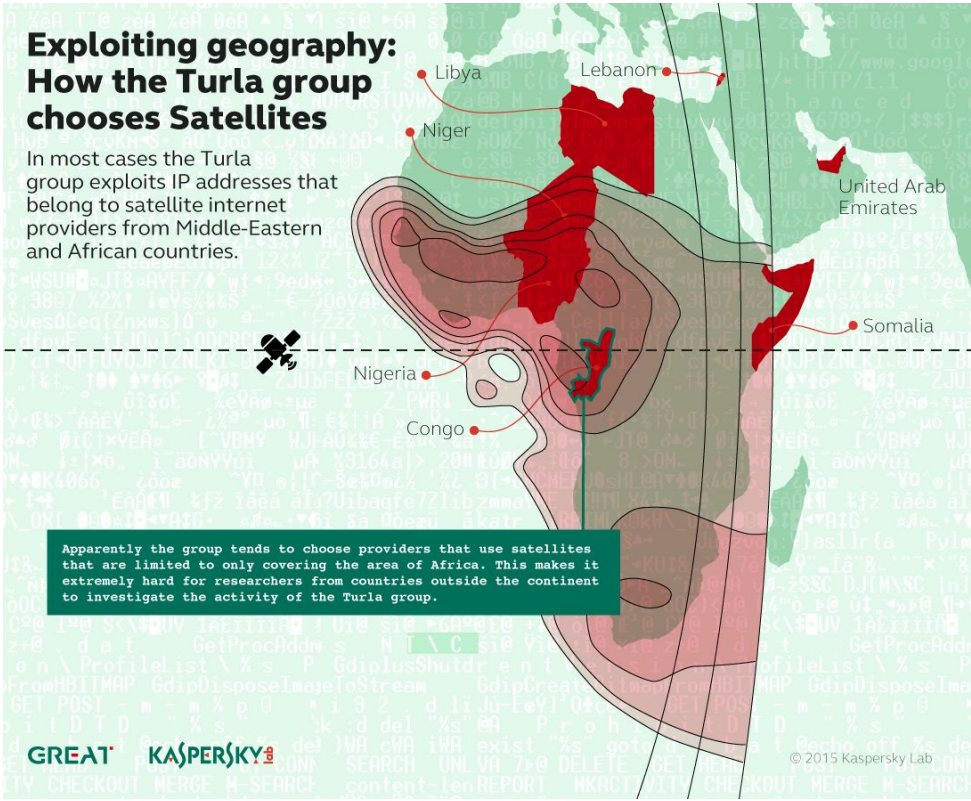
- Weather satellites broadcast the data continuously.
- Because of the interference (and because it’s not critical information) it doesn’t require encrypted transmission.
- It’s orders of magnitude simpler to recover the data this way.



- Because it’s unencrypted, it can be sniffed using a $10 dongle and a Raspberry Pi.

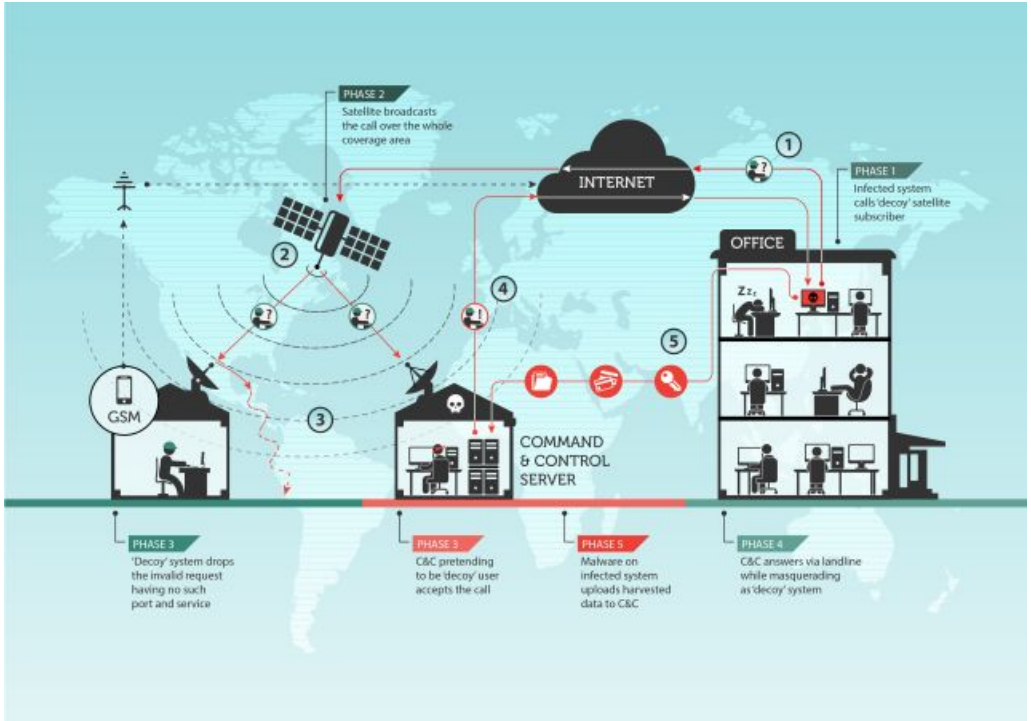
Satellite communications - Turla

https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/



Satellite communications - Turla

https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/



Q & A