

Secure Positioning and VC Systems

Panos Papadimitratos

panos.papadimitratos@epfl.ch



Localization

- Mobile computing is becoming increasingly location-based
 - Location-aware devices
 - Location-based services
- Two main problems
 - Determine the location of a (another) device
 - Could be as simple as asking a location-aware device to report its location
 - Often, some infrastructure performs the task
 - Determine own location
 - With the help of own equipment and some infrastructure

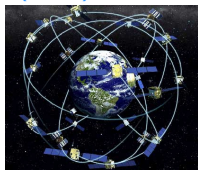
2

Localization (cont'd)



Sensing

Part of graphics by Nokia



Global Navigation Satellite Systems



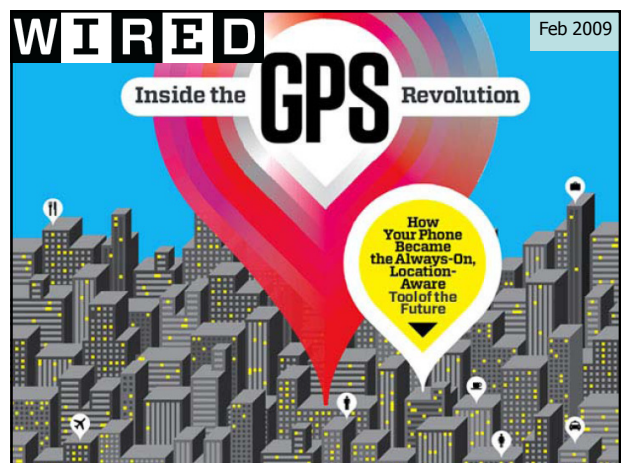
Navigation



Context awareness

3

Fleet and cargo management

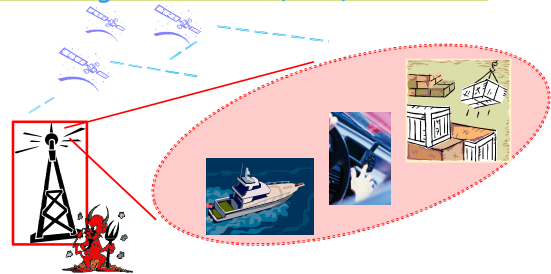


Attacking Localization

- Mislead devices (and their users) about their location
 - Compromise the device: hard
 - Compromise the infrastructure: much harder
 - Interfere with the infrastructure-to-device wireless communication: Easy
 - Jam → Outage
 - Overwrite legitimate transmissions with synthesized ones → Control loc_v and t_v

5

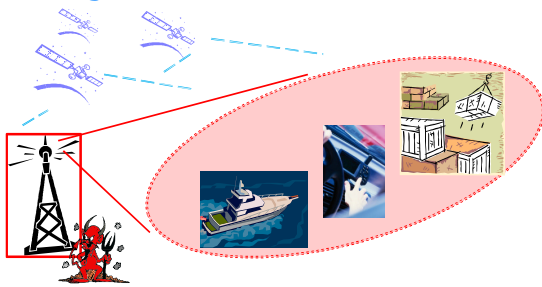
Attacking Localization (cont'd)



- *Attacker*: Easy to overwrite legitimate GPS signals
- *System*: GPS receiver locks on spoofed signals

6

Attacking Localization (cont'd)



- *Consequence*: User/system with false, attacker-controlled location & time

7

Attacking Localization (cont'd)

Armored Vehicle Demonstration flop [2001]

Russian Truck Hijacking [2007]

California Cell Infrastructure Outage [2008]

...More to come

8

Page last updated at 20:45 GMT, Tuesday, 23 February 2010

E-mail this to a friend Printable version

Sat-nav systems under growing threat from 'jammers'

By Jason Palmer
Science and technology reporter, BBC News

Technology that depends on satellite navigation signals is increasingly threatened by attack from widely available equipment, experts say.

While "jamming" sat-nav equipment with noise signals is on the rise, more sophisticated methods allow hackers even to program what receivers display.


At risk are not only sat-nav users, but also critical national infrastructure.

A UK meeting outlining the risks was held at the National Physical Laboratory in Teddington on Tuesday.

The meeting was organised by the government-funded Digital Systems Knowledge Transfer Network.

"GPS gives us transportation, distribution industry, just-in-time manufacturing, emergency services operations – even mining, road building and farming, all these and a zillion more," David Last, a consultant engineer and former president of the Royal Institute of Navigation, told the conference.

"But what few people outside this community recognise is the high-precision timing that GPS provides to keep our telephone networks, the internet, banking transactions and even our power grid online."



Society will only get ever more dependent on sat-nav systems

SEE ALSO

GPS to suffer from awakening sun
10 Feb 10 | Science & Environment

Nokia launches sat-nav challenge
21 Jan 10 | Technology

Contracts for Galileo sat-nav
07 Jan 10 | Science & Environment

Will smartphones see off sat-nav?
01 Jan 10 | Technology

RELATED INTERNET LINKS

National Physical Laboratory
Digital Systems Knowledge Transfer Network
Royal Institute of Navigation
General Lighthouse Authorities

The BBC is not responsible for the content of external internet sites

TOP SCIENCE & ENVIRONMENT STORIES

LHC fault forces 2011 shutdown
Ancient eggshell yields its DNA
Nanotech "fuse" for novel battery

News feeds

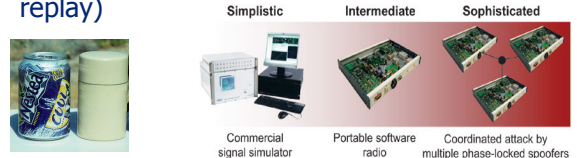
MOST POPULAR STORIES NOW

SHARED READ WATCHED/LISTENED

US apology for Gaddafi comments
US attacks East Jerusalem plans

Attacking Localization (cont'd)

- GPS Jammers and Simulators
- Meaconing (record and re-broadcast, a.k.a. replay)



Low-power jammer (1 W); it can affect a 35km radius

B. O'Hanlon, B. Ledvina, M.L. Psiaki, P.M. Kintner Jr, T. E. Humphreys, "Assessing the GPS Spoofing Threat," GPS World, January 2009

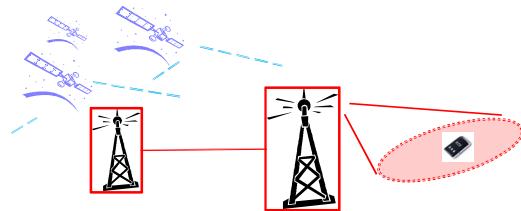
10

Securing Localization

- Authenticate navigation messages (NAV)
 - Public key crypto: one private-public key pair per satellite
 - Symmetric key authentication; single system key
 - Need tamper-resistant storage at receivers
- Public key authentication delays can be significant
 - Low NAV transmission rate: ~ 40 sec for a signature
 - Caution: Need to maintain the relative NAV arrival timings
- Civilian GNSS do not currently offer authentication

11

Attacking Localization (cont'd)

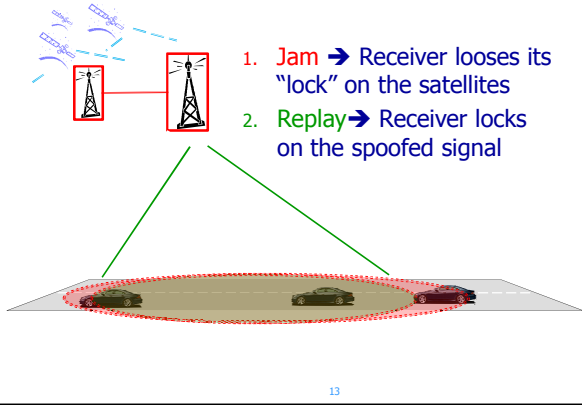


- Replay attacks can be effective even against future systems with authentication (e.g., Galileo)

P. P. and A. Jovanovic, "Protection and Fundamental Vulnerability of Global Navigation Satellite Systems (GNSS)," IEEE IWSSC 2008

12

Attacking Localization (cont'd)



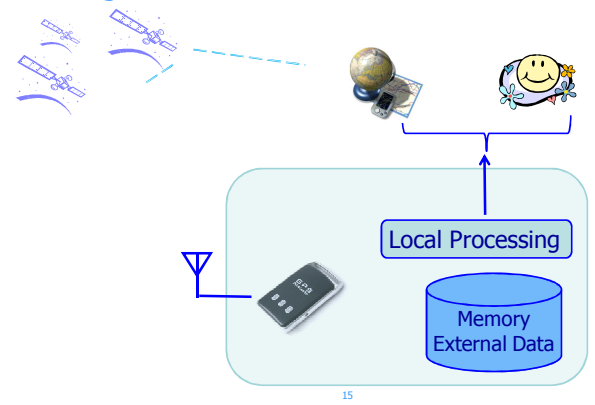
Securing Localization (cont'd)

- *Assumption:* the adversary covers part of the system
- *Objective:* Receivers detect the attack onset
 - No additional complex equipment
 - No system reconfiguration
 - Resilience to sophisticated adversaries
- *Approach:* Rely on own (receiver) measurements
 - Predict future values from available ones that are deemed correct
 - Discrepancy between measurements and predicted values → **Attack**

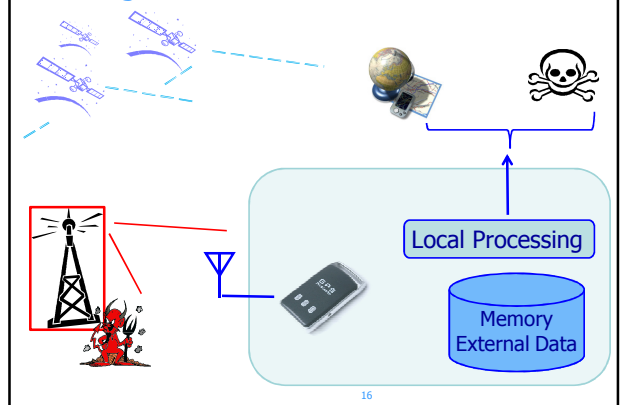
P. P. and A. Jovanovic, "GNSS positioning: Attacks and Countermeasures," IEEE MILCOM 2008

14

Securing Localization (cont'd)



Securing Localization (cont'd)



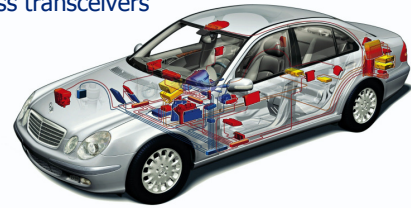
Securing own position

- Vulnerability of GNSS: Long known issue, could become a major problem
- Upcoming systems are to enhance availability (against unintentional interference) and offer security features
- Attacks at the physical layer (e.g., replay attacks) are possible even when cryptographic protection is available
- Simple non-cryptographic solutions can raise the bar even for sophisticated adversaries

17

Vehicular Communications

- Vehicles equipped with
 - Computers
 - Sensors
 - Including positioning systems (GPS, Galileo)
 - Wireless transceivers



Vehicle illustration courtesy of Daimler

18

Vehicular Communications (cont'd)

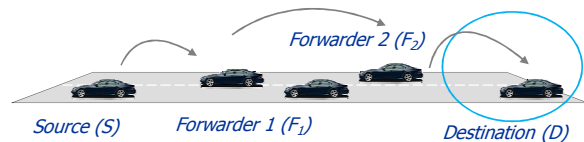


Illustration by the Car-to-Car Communication Consortium

19

Geo-Cast

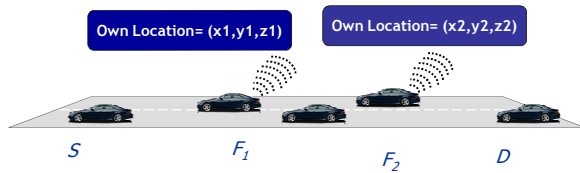
- Position-based routing
 - Relaying nodes (forwarders) also send packets to the geographically closest node to the destination (location)



20

Geo-Cast (cont'd)

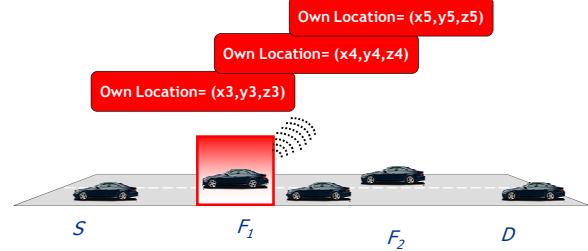
- Nodes autonomously inform the system about their location



21

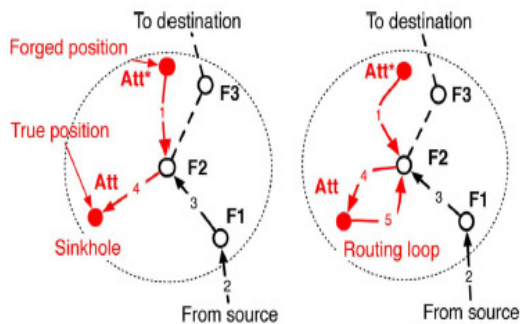
Attacking Geo-Cast

- Adversarial nodes could announce false positions (not the actual ones), beyond benign system errors



22

Attacking Geo-Cast (cont'd)



23

Securing Geo-Cast

- Set of cryptographic and non-cryptographic mechanisms, including
 - Secure Neighbor Discovery
 - Plausibility checking of neighbor locations

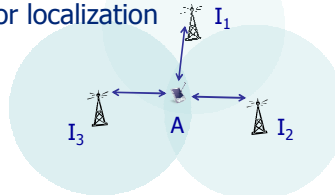
A. Festag, P. P., and T. Tielert, "Design and Performance of Secure Geocast for Vehicular Communication," IEEE Transactions on Vehicular Technology, vol. 59, no. 5, June 2010

- **More general problem:** adversarial devices (e.g., compromised) could 'lie' about their location within any other distributed protocol

24

Secure Localization (cont'd)

- Secure localization of **other devices**
- Infrastructure could be augmented with security features for localization



- **Challenge:**
 - Autonomous secure localization of other nodes

M. Fiore, C. Casetti, C.-F. Chiasserini, and **P. P.**, "Verification of Neighbor Positions in Mobile Networks," Work in progress, arXiv:1006.0806 e-print, June 2010

25

Secure Positioning and VC Systems

Panos Papadimitratos

panos.papadimitratos@epfl.ch

