# Galileo’s secrets

## KU Leuven researchers ensure safe ride for Europe’s navigation system

Senne Starckx
More articles by Senne \ flanderstoday.eu

In times when computers without internet access seem an artefact of the past and even the most basic kitchen appliances have wi-fi connectivity, few things in our lives seem safe from hackers’ prying eyes.

From the GPS receiver in your car, to the map application in your smartphone, a skilled hacker can easily take control of them and begin sending you false information remotely. In 2020, when Europe finally gets its own navigation system – the Galileo – these issues will become more pressing than ever.

The European Space Agency (ESA) is currently working to make sure that the system is airtight by the time it rolls out. After years of planning, the first of the 30 satellites were launched in 2011.

Galileo – run by the European Commission in partnership with the ESA – is seen as Europe’s answer to the American GPS and the Russian Glonass, at a time when the relations between the EU, the US and Russia have become chilly.

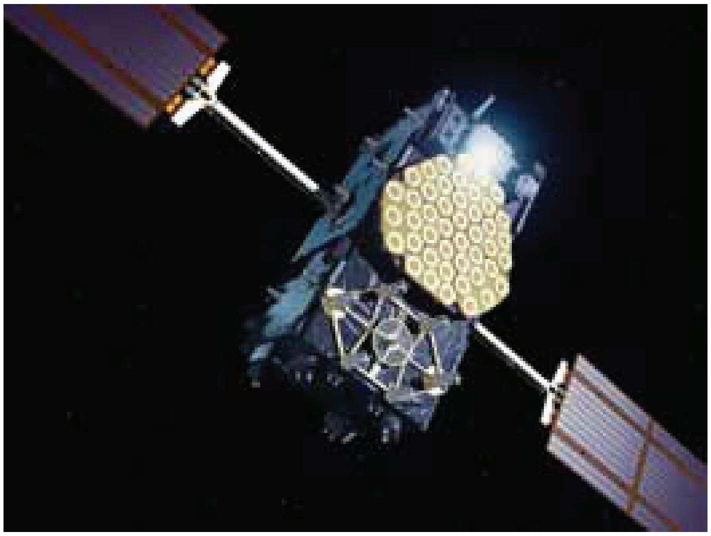
The team of scientists and researchers at ESA are working on authentication features that would prevent Galileo from picking up false signals or rejecting real ones. Vincent Rijmen and Tomer Ashur of the University of Leuven are the researchers helping the ESA make the signals more difficult to forge.

But it’s no easy task. Because half of the system’s satellites are already in orbit – and to avoid delaying the whole operation – they can implement only a handful of safety features at a time. This limit also works to not tax the signals’ limited bandwidth.

Some of the features appear very conventional, borrowing from electronic signatures used in credit card transactions, online banking and internet activities that involve transferring sensitive information.

“This is why we opted for the method used in electronic signatures,” says Rijmen, who works at the University of Leuven’s Department of Electrical Engineering. “These signatures take up less than 100 bits, which is also the reason why they expire so quickly. But this is not a problem in the case of satellite navigation because the location is authenticated every 30 seconds or less.”

Ashur, a PhD researcher under Rijmen’s mentorship, wrote the assessment report on the security features for the entire authentication system, weighing in on the benefits of certain cryptographic tools and parameters. “You could call me a cryptanalyst, which means that I usually try to ‘hack’ things,” he laughs. “But since it’s done by the good guys, I’d prefer to call it ‘a security assessment’.”



© P Carril/ESA

Artist’s impression of one of Galileo satellites

Why is it so important that the Galileo system is equipped with an airtight authentication protocol? “In 2007, I was working for a data security company that protects businesses from data leaks,” says Ashur. “We had a project with this huge bank in South Africa, and we were supposed to install our software on the bank’s computers.”

As is often the case, he continues, “some of the installations didn’t go so well, and one of them was so faulty that the host computer could no longer be started. Unfortunately, this computer was located in the security operations room and was responsible for showing the location of all the bank’s armoured trucks.”

A more trivial example, he adds, is the recent hype surrounding the *Pokémon Go* game. “Last September, a large number of users were banned from playing because some of them were cheating inside the game by providing fake location data and catching pokemons that were not in their vicinity.”

The existing satellite-based navigation systems, he explains, were originally developed for military purposes – the US Army still operates a high-precision version of its GPS system. “This is clearly a problem that needs solving.”

How does this compare to encryption used in emails or instant messengers? “Encryption has got nothing to do with this,” says Ashur. “The purpose of encryption is to hide information so that it cannot be read by an unauthorised party. Since satellite navigation data is openly transmitted, this is not what we were looking for.”

What the researchers did instead was add a sort of signature that “allows the receiver to verify that the data was really sent from the satellite and is not a forgery made by the hacker,” Ashur explains. “Data authentication is a common problem in cryptography, and there are standard methods on how to deal with it.”

Adding secret codes to Galileo’s system and signals is a real challenge. The cost of exchanging information between the satellites and the units on the ground “is extremely high,” says Ashur. “The environment in which we have to work is also very constrained. You could compare it to having to convey all the information in this article in only two sentences.”

## Q&A

**Gabriël Van de Velde is a mechatronics engineer at the Free University of Brussels (VUB), who recently won the Agoria Prize for his master’s work on making robotic mouths simpler to programme and look more human-like**

**Are human-like features that important in robots?**
Indeed they are. Even if many of us don’t realise it, artificial intelligence is present everywhere. We may not be afraid of Google or Facebook’s AI algorithms, but robots still frighten us – even though they are helping us in so many different ways, from robot-assisted surgery to elderly care. They play an increasingly important role in our everyday lives.

**How did you improve the movement of their mouths?**
I started with photographs of the human mouth. I transformed them and was able to compare the pictures with the robotic mouth that I was building. I used the differences in features to slightly adjust the robotic mouth. I used this principle over and over, until there were no noticeable differences anymore. The crucial aspect of my improvement is that technicians who build robots will no longer have to write a manual or implement a computer-guided calibration model. These techniques are expensive and time-consuming. Imagine that you have to calibrate a robotic head – fitted with more than 30 motors – for every mouth position. That’s a lot of work! My method was tested with only five motors, which is good for 52 reference positions. It only took an hour.

**You’re now working on a PhD in rotor technology – which has nothing to do with robots.**
For mechatronic engineers, life isn’t only about robots. I see a variety of potential study areas. Rotary dynamics has always fascinated me. I’m studying a new method to improve the speed of rapidly turning machines – beyond 60,000 revolutions per minute. That’s a big challenge! \ Interview by SS

## WEEK IN INNOVATION

### Volunteering improves health

Volunteers are generally in better health than those who never volunteer, showing similar health norms as people five years younger, according to a study led by PhD researcher Jens Detollenaere of Ghent University. Detollenaere, whose findings have just been published in the journal *Plos One*, analysed data from the European Social Survey (ESS), conducted in 2012 and 2013. The ESS measured the beliefs, preferences and behaviour of about 40,000 citizens from 29 European countries. People who volunteer turned out to be in substantially better health than non-volunteers, with health benefits comparable to those of being five years younger or being a native resident rather than a migrant.

### Pilot projects to test home hospital care

Federal health minister Maggie De Block has launched 12 pilot projects on home hospitalisation, to ascertain whether patients can get certain care at home, with the same quality and safety guarantees as in a hospital. The projects, which were selected following a call last year, will test a number of situations, including intravenous administration of antibiotics and cancer treatments. About 1,300 patients and 35 hospitals are involved, along with home care services and general practitioners. Minister De Block pointed to the advantages of home hospitalisation. Patients, she said, would receive care in a familiar and comfortable environment, can more easily receive friends and family and run little risk of some common hospital infections.

### New DNA databases to help police

The National Institute of Forensic Science and Criminology (NICC) will soon have two more DNA databases. DNA research is crucial in identifying suspects and finding missing persons. But during investigations, many people come into contact with crime scenes, including police, prosecutors and lab technicians, who can unintentionally leave their own DNA behind. A new database with DNA profiles of key figures involved in investigations will make it possible to quickly exclude their genetic material, thus speeding up investigations and reducing costs. The database containing genetic material of missing persons, meanwhile, should make it possible to solve older cases. \ Andy Furniere