Cyber security in satellite communication

Both private individuals and companies benefit from fast satellite communication these days. In doing so, they accept that their data is sent unencrypted and so can be intercepted. Researchers at the armasuisse Cyber-Defence Campus have found a solution to how data can be transferred quickly by satellite but still be protected.

Text: Dr Vincent Lenders
Hardly anyone uses WLAN without encryption today, because without protection, neighbours or an unknown stranger could intercept the data traffic. However, what has long been normal for WLAN appears to still be given little attention in satellite communication, as Dr Vincent Lenders, Head of the Cyber-Defence Campus at armasuisse discovered. Large international corporations and even operators of critical infrastructures still send data that should be protected completely unencrypted by satellite. In an extreme case, not only neighbours, but millions of curious people, can listen in, as satellite signals can be received without any problems over large areas and intercepted using simple equipment. How can this be?

Fast data transfer but no data protection
Satellite communication is very practical and extremely convenient for users. This is due to the fact that it works from anywhere on earth, as long as there are no obstacles between an antenna on the ground and the corresponding satellite in space. Large Swiss corporations and operators of critical infrastructure use the technology to communicate with their branch offices or connect to ships and aircraft. However, apart from these advantages, communication by satellite also has a significant disadvantage: the very great distances to the satellites, around 36,000 km, lead to perceptible time delays in data transmission. This is not a problem for applications such as television or geolocation. But when surfing the web, these lags lead to very long download times for websites. This is why satellite operators today prefer to use what are known...
as performance enhancing proxies to increase surfing speed. These act as an intermediary between transmitter and receiver and can compensate for the long delays by specifically adapting the communication protocol.

But therein lies the crux. If companies encrypt their data with a virtual private virtual network (VPN), for example, these proxies cannot accelerate the data traffic because they do not have the key. That is why there is the risk that many users, and even large companies, dispense with common encryption methods in the hope that no unauthorised strangers intercept the traffic.

Lack of awareness of the consequences of no data encryption
This is exactly what the researchers at the Cyber Defence Campus of armasuisse have realised. They point out that the data traffic of many companies is not encrypted, including their sensitive data. Even worse, it can be easily intercepted by a software-defined radio. It must therefore be assumed, says Dr Martin Strohmeier, an expert from the Cyber Defence Campus, that companies today are systematically spied on via satellite communication. And he adds: “Many companies are not aware of the problem, because they think that the satellite operator uses encryption.” But in most cases, this is not so.

Developing new secure encryption methods thanks to collaboration
Today, companies still have to decide between speed and security. But this could change in future. Since 2019, employees at the Cyber Defence Campus have been working with national and international universities on new solutions. In spring this year, the researchers were already able to present an initial prototype of a new proxy in Thun capable of encrypting data traffic without loss of speed. So users of satellite communication should be able to enjoy fast and secure communication in future, just as with WLAN today. This is particularly beneficial to private individuals and bodies, including the Armed Forces, who work with sensitive data that needs to be protected. However, various adjustments and clarifications are still required before it is fit for global use. The first deployment of this new proxy is planned for 2021 at armasuisse in Thun.

THE CYBERSPACE AND INFORMATION RESEARCH PROGRAMME
The Cyberspace and Information research programme ensures expertise in future technologies for the Swiss Armed Forces. The fields of research range from cyber security and information management to machine learning and data science.
Research demonstrator in Thun: a satellite dish installed on the roof sends and receives encrypted data with no loss of speed.