Autotalks

Truly Secure V2X

V2X Communication Security Technical Brief

Isolation from cellular network for minimizing the attack surface

Integrated Hardware Security Module (HSM) for securely storing credentials

Integrated hardware acceleration for global verification

Multiple defense layers for maximal protection

Automotive Security

In several recent, highly publicized incidents, it was shown how simple it can be to hack and manipulate a vehicle via an insecure wireless interface. This has caught the attention of regulators worldwide. The first to officially address this is UNECE WP.29, applicable in all European countries, Japan and South Korea, which have added wireless interfaces security to type approval. Any newly developed vehicle must prove its security before reaching the streets.

V2X (Vehicle to Everything) technology is the first utilization of communication for vehicle safety. Alerts are displayed to the driver based on the content of V2X messages. In the future, vehicles will brake based on V2X messages in order to avoid risks that are undetectable by any other vehicle sensor. This highlights the importance of security to assure reliable and trustable V2X operation. This paper will discuss the main considerations in V2X security, provide design best practices, and describe Autotalks' strategy for a truly secure V2X.

V2X Security

V2X specifications and deployment guidelines were developed to address V2X-specific security challenges. The V2X unit needs to sign and authenticate messages while detecting and neutralizing threats in real-time. Cooperative Awareness Messages (CAM) / Basic Safety Messages (BSM) are exchanged between hundreds of vehicles cruising at high speed. These are ad-hoc, low-latency, anonymous broadcast messages that demand immediate handling. To facilitate that, V2X includes comprehensive processes for certificate distribution and management over the lifetime of the vehicular or roadside unit.

V2X Security Guidelines

A complete and trusted security solution should be multi-layered to deal with multiple threats. First and foremost, the security assets, namely the private keys, should be securely stored in Hardware Security Module (HSM), protected against unauthorized access. Next, all incoming V2X messages should be verified – since any of the messages could put the vehicle at risk. The security verification must be performed in real-time. Limited verification engine should be avoided since it queues V2X messages, introducing delay which may outdate and invalidate the message.

And multiple layers of protection are needed, in case some SW vulnerability will be found. The firmware authenticity should be verified using a secure boot process. A pr otected firmware field update is needed for enhancing security schemes over time. Security assets, HSM and verification engine, and interfaces outside the V2X domain should be protected against malicious access. Finally, security systems must be certified. The scope of the minimal certification is the HSM, and in the future, will grow to cover the entire V2X operation.

Multiple defense layers

The need for multiple defense layers has been recognized by regulators. Citing NHTSA V2X NPRM draft: "A layered approach to vehicle cybersecurity within a risk-based framework reduces the probability of an attack's success and mitigates the ramifications of a potential unauthorized access." Autotalks' truly secure solution follows this guideline.

Autotalks multiple defense layers protect against attacks, vulnerabilities, malware, and worms. Bogus messages are filtered as early as possible by the first protection layer. The integration of security engines inside Autotalks' device assures that access is tightly monitored to prevent misuse. V2X application receives only trusted messages.

For example, the HSM may strongly protect the security credential, but if malicious software can command it to sign a bogus message, then the overall system is not protected. Any system is as secure as its weakest element.

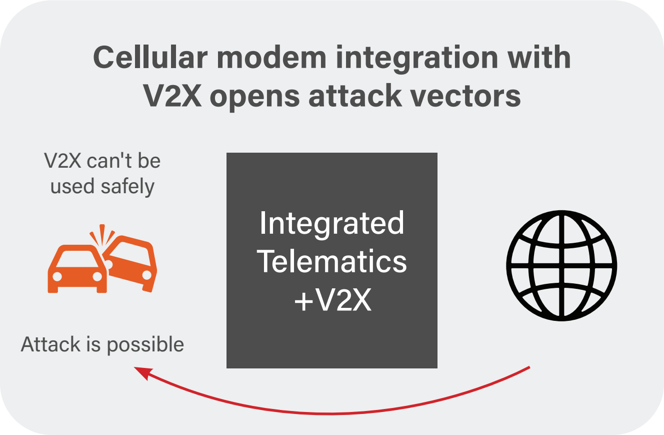
Misbehavior detection identifies what may seem as legitimate data, either resulting from compromised or faulty devices. Bad actors are detected and reported. Autotalks applies patented technology for the highest detection reliability of bad actors while minimizing false detections.

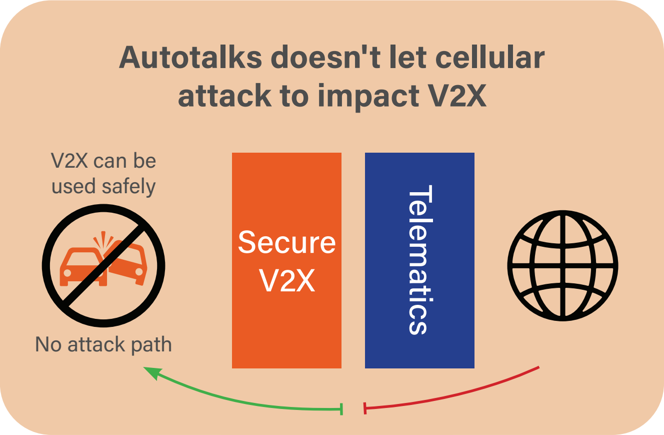
V2X isolation from the cellular network bounds surface of attack

The surface of attack is the sum of the points in an environment (the "attack vectors") at which an unauthorized user (the "attacker") can try to inject or extract data. A common approach to improving security is to reduce the attack surface.

V2X functionality is added to vehicles either in dedicated V2X ECU (Electronic Control Unit) or Telematics unit (TCU). Dedicated V2X ECU is the most secure because of the limited functionality and number of interfaces, which can be thoroughly tested and analyzed. V2X TCU integration may reduce cost, but, if performed without strict domain isolation, the V2X security is severely compromised.

The diagrams below show TCUs with isolated and non-isolated V2X. The isolated V2X, on the right side, prevents Telematics vulnerability from reaching the V2X. On the other hand, the non-isolated V2X, on the left side, opens a door for wide-scale remote attacks through the cellular link, not requiring proximity or physical access. Furthermore, if the same CPU is hosting V2X and Telematics, its breach would place V2X at risk. Mixing non-safety communication channels with V2X, which serves for safety, is a bad design decision.


Cellular modem integration with V2X opens attack vectors
V2X can't be used safely
Integrated Telematics +V2X
Attack is possible



Autotalks CRATON2 offers the optimal V2X offload solution. The integrated CPU assures the smallest solution size. Furthermore, the solution is pre-integrated and pre-tested for minimizing the integration efforts and risks.