TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Cybersecurity in the Age of V2X

follow us: @tataadvanced

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

What is V2X?

- Stands for Vehicle-to-Everything
- Vehicular communication technology which enables vehicles to converse with the moving parts of the traffic and external systems like pedestrians and streetlights
- Designed to improve traffic efficiency by providing warnings for upcoming traffic congestions, proposing alternative routes and preventing accidents
- Comprises different communication technologies including Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrians (V2P) and Vehicle-to-Devices (V2D)
- Both, DSRC (Dedicated Short-Range Communications) and C-V2X (Cellular to Everything) can be used to meet the target performance for V2X
- Offers 360-degree situational awareness

Factors Driving the Growth of V2X

- Increasing environmental concerns
- Intense competition among car manufacturers
- Demand for real-time traffic and incident alerts for increasing public safety

Future Prospects of V2X

- As per the *IHS Markit,* a leading business research firm, the number of vehicles equipped with a V2X system is expected to reach as high as $11.2 million in 2024.
- According to statista.com, it is expected that the global V2X market will reach to around 6 billion U.S. dollars by 2025.
- As suggested by *MarketsandMarkets* Research Pvt Ltd, North America is estimated to be the largest V2X market during the forecast period (2017-2025). European region is estimated to be the second largest market.

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Why Security A Major Concern in V2X communications

- ITS output specifically depends on V2X communications as it is responsible for exchange of data between underlying communication technologies. This data includes information and warnings from on-board sensors, such as current position and speed of the vehicle.
- V2X also facilitates communication between roadside units (RSUs) & traffic monitoring systems (gather and deliver warnings about hazardous situations).
- With help of wireless communications and IoT technologies, the vehicles can now easily communicate with any smart device and share information. This makes vehicular networks more susceptible to different types of cyber-attacks: internal or external attacks.

Threat Landscape for V2X Communications

There are five key areas where we need to emphasise for ensuring V2X security. These are Confidentiality, Integrity, Availability, Authenticity and Non-repudiation.

Threats on Confidentiality

- Eavesdropping attack
- Location Tracking

Threats on Integrity

- Alter messages or inject false messages
- Replay attack
- GPS Spoofing attack

Threats on Availability

- Blackhole & Greyhole attacks
- Flooding attack
- Jamming attack
- Coalition and Platooning attacks

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Threat on Authenticity

- Certificate replication attack
- Sybil attack
- Masquerading attack or impersonation attack

Threat on Non-repudiation

- Repudiation Attack

Security Solutions

In order to mitigate all the possible risks having potential to damage the security of the V2X communication, we need to ensure successful implementation of appropriate security services. Some of the security solutions are suggested below:

- Cryptography-based
- Behaviour-based / Trust-based
- Identity-based