Building Secure Routes: Cybersecurity in the Era of Connected Transport

AGENDA

- About Irdeto
- The era of connected mobility
- Cyberthreat landscape
- Building your cybersecurity strategy

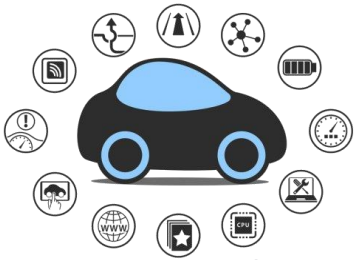
IRDETO'S RICH HERITAGE IN SECURITY

- Over **50 years** of security expertise
- **Over 6 billion** devices and applications secured
- Inventor and key patent holder of **whitebox cryptography**
- **ISO 9001** and **ISO 27001:2013** certified for key generations throughout Irdeto production centers
- Serving **400+** customers in **75+** countries
- Nearly **1,000** security experts employed
- 70% of employees are in **engineering/ research/ development**
- **13+** locations globally

New era of Connected Mobility

Electrification

Connected Vehicles



Autonomous driving

Mobility-as-a-Service

era of disruptive innovation

What's next for the connected era?

Secured Assets

Technology is now common for mobility & supply-chain but the advancement has also increased the risk of cyberattacks. Threat can come in any shape and size, including consumer data breaches, Denial-of-Service (DoS) attacks, malicious exploit attempts, intellectual property theft and the safety of drivers and passengers - making it inevitable to secure your digital assets.

Cyber Threat Landscape

- **Assets**
  Vehicles, paid in car features/services, customer personal data, company confidential information, intellectual property, employees, communication delivery infrastructure and buildings

- **Threats**
  Hardware/software hacking, service theft, payment fraud, phishing, social engineering, ransomware, malware and DDOS

- **Threat actors**
  Hackers and cybercriminals

- **Focus**
  Safety, data confidentiality, availability and integrity

Five Pillars to Secure Your Connected Assets

Anomaly or Intrusion Detection

End-Point Protection

Network Protection

Device & Credentials Management

Cybersecurity Services

Anomaly & Intrusion Detection

•Detects any anomalies and intrusion in networks.
•Both IT and OT.
•Notifies of anomalous traffic and traffic patterns to further investigate and identify possible attack attempts

•Example: Monitors a control network of a manufacturing line and alerts for any unexpected traffic so that it can be further investigated

Network Protection

•Protects networks.
•Traffic analysis, filtering and segregation.
•Both IT and OT.

•Example: Protects a control network of a manufacturing line and prevents any unauthorized incoming or outgoing traffic (say, from the Internet or corporate office WiFi)

End-Point Protection

•Protects endpoints.
•Integrity verification, self-healing.

•Example: Like anti-virus software for embedded devices. The difference is that whereas PC anti-virus looks for known unwanted software, end-point protection makes sure that only known wanted software is present on an embedded device.

Device & Credentials Management

•Manages the solution.
•Remote inventory, configuration, diagnostics and update.
•Security Credential & Certificate Management for the Full Lifecycle of Trusted Identities in Connected Embedded Devices

•Example: Allows for remote access to and management of the solution. Credentials are the device's "passport" to other networks, devices and services that are populated on the device when it is manufactured and updated when they expire.

How to integrate a cybersecurity strategy

4 Treat cybersecurity as an ongoing process

3 Improve current measures

2 Assess your cybersecurity measures

1 Fully understand the threat

THANK YOU