Security in V2V and V2N Communication

Overview

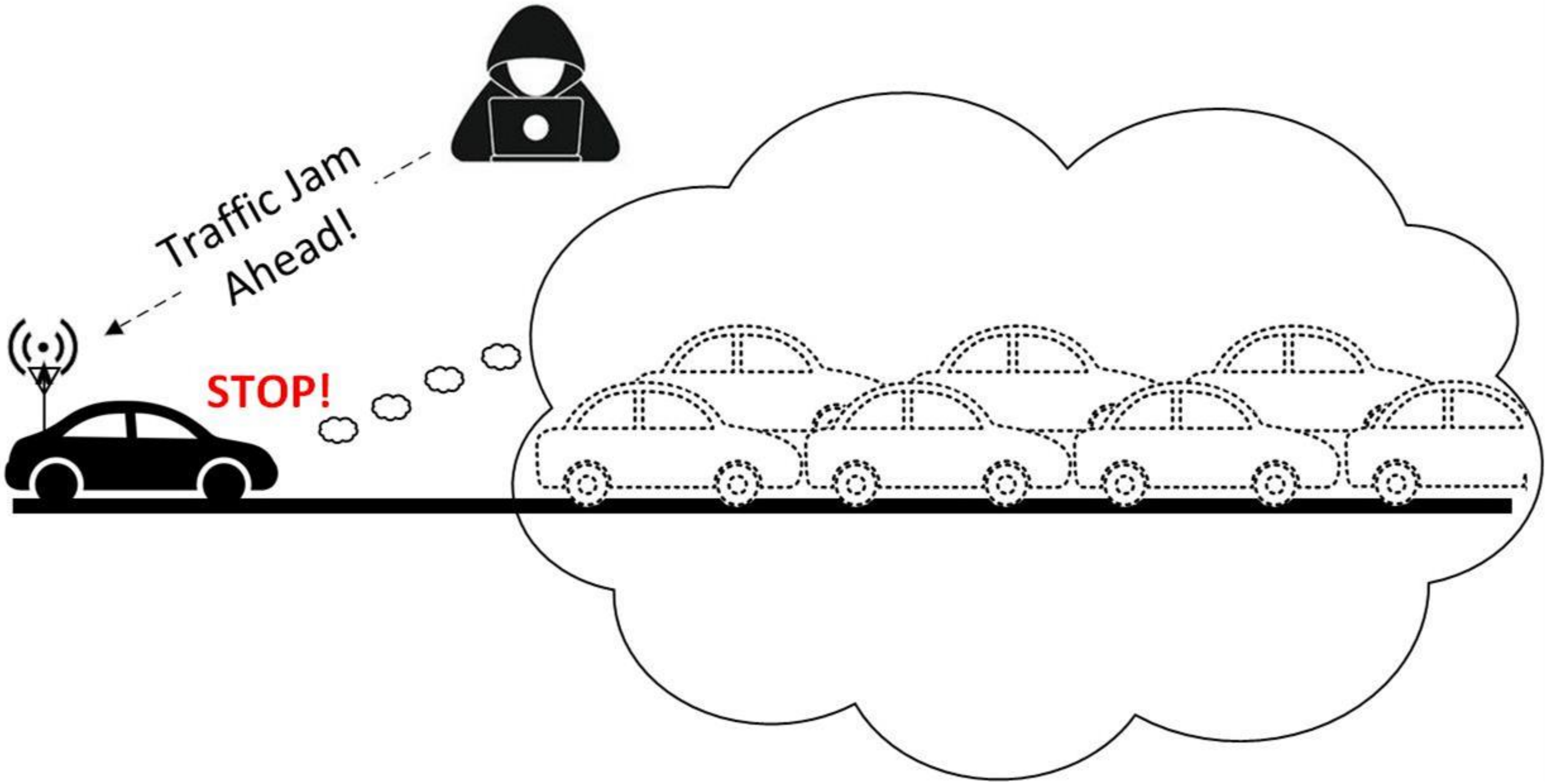
- **V2V Security: More Technologies, More Threats** | 3
- **V2V Security: Current and Future Protocols** | 8
- **V2V Security: Requirements and Standards** | 14
- **V2V Security: Vehicular Public Key Infrastructure (VPKI)** | 20
- **V2N Security: An Overview** | 25

V2V Security:
More Technologies, More Threats

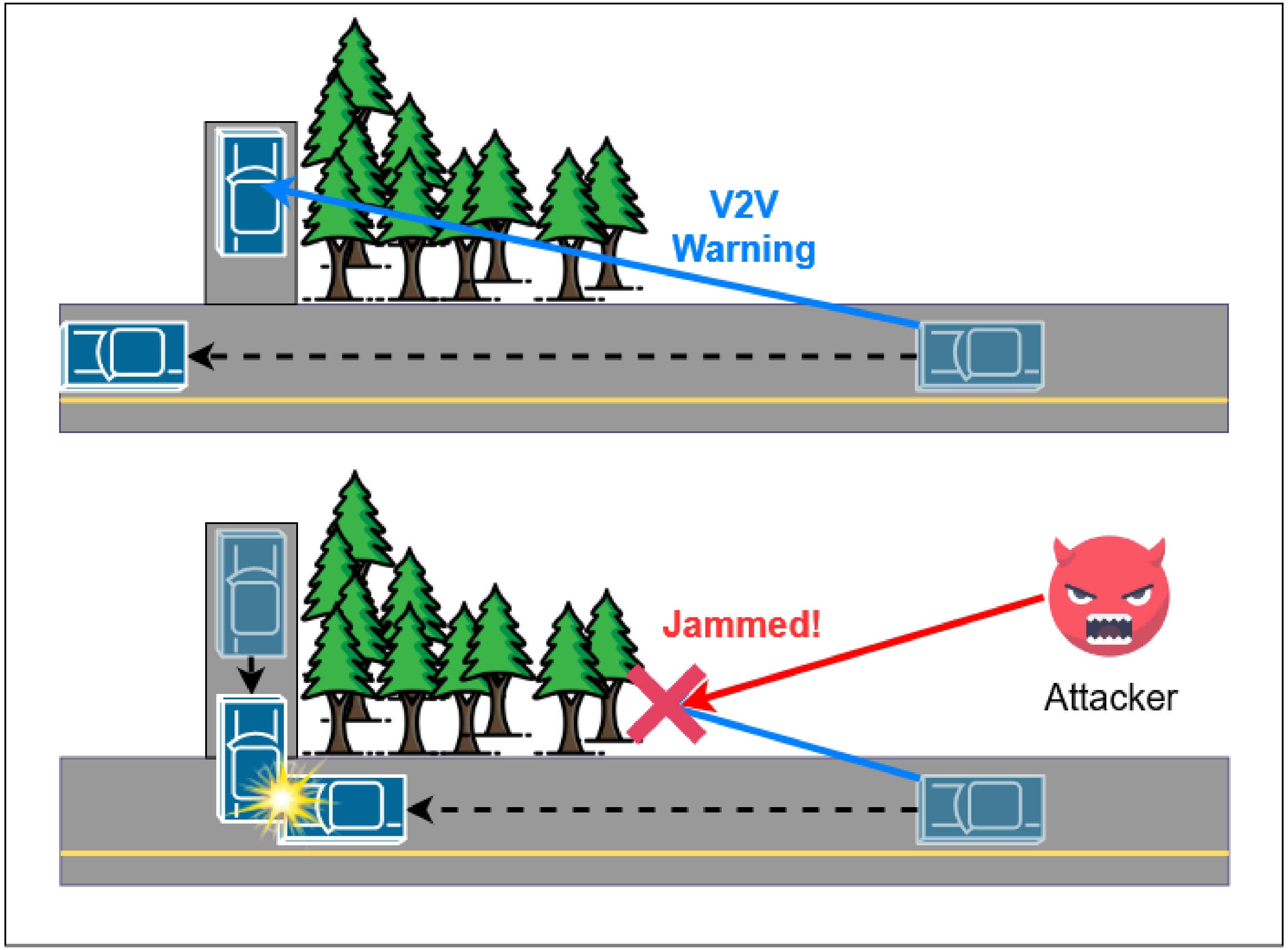
CVs Introduce New Concerns

- V2X communications directly impact safety
  - Attacks against BSMs may be extremely dangerous
  - Vehicles might react (swerve, stop, etc.) based on BSMs
- DoS → potential for widespread disruptions
  - Traffic gridlock, manipulation
  - Force road closures (for safety) by attacking V2I RSUs
- Privacy considerations
  - Vehicle tracking = person tracking

BSM Spoofing Attack



BSM Jamming (DoS) Attack



V2V Security Requirements

1. Authentication - verify messages are from trustworthy and legitimate devices
2. Integrity - verify messages are not modified between sender and receiver
3. Detect and remove misbehaving units
4. Protect privacy - no unnecessary tracking
5. Security must persist for vehicle lifetime (~15 years)

V2V Security:
Current and Future Protocols

Security in Current V2V Protocols

- First-generation V2V protocols have no built-in security
  - 802.11p, LTE-V2X
- No authentication → replay, man-in-the-middle attacks
- No integrity checks → message modification attacks
- Extremely vulnerable to denial-of-service (DoS)
  - Jamming attacks are highly efficient and effective

DSRC - 802.11p Has No Security

- Security is specifically not included
  - Standard leaves security to upper-layer protocols
- 802.11p is > 10 years old → many known attacks
- Extensive literature on DoS attacks against 802.11p
  - Jamming has been widely studied, extremely effective

LTE-V2X (Also) Has No Security

- Traditional LTE has lots of security!
  - But this requires access to the LTE network ☹
- No security at all in Sidelink Mode 4 (for V2V)
  - → No SIM or network attachment
  - ∴ No authentication, integrity checking, or encryption
- However, there are privacy benefits from not having a SIM (Subscriber Identification Module)

V2V Security Improvements in NGV

- NGV → Next-Generation V2X protocols
  - 802.11bd, NR-V2X and 5G C-V2X
- Physical-layer security (PLS) techniques are possible
  - Technological advancements like multiple-antenna devices
- Still no V2V security beyond the PHY layer
  - Encryption, authentication, etc. remain left to upper layers

V2V Security: Requirements and Standards

Recall - V2V Security Requirements

1. Authentication - verify messages are from trustworthy and legitimate devices
2. Integrity - verify messages are not modified between sender and receiver
3. Detect and remove misbehaving units
4. Protect privacy - no unnecessary tracking
5. Security must persist for vehicle lifetime (~15 years)

V2V Security Standards

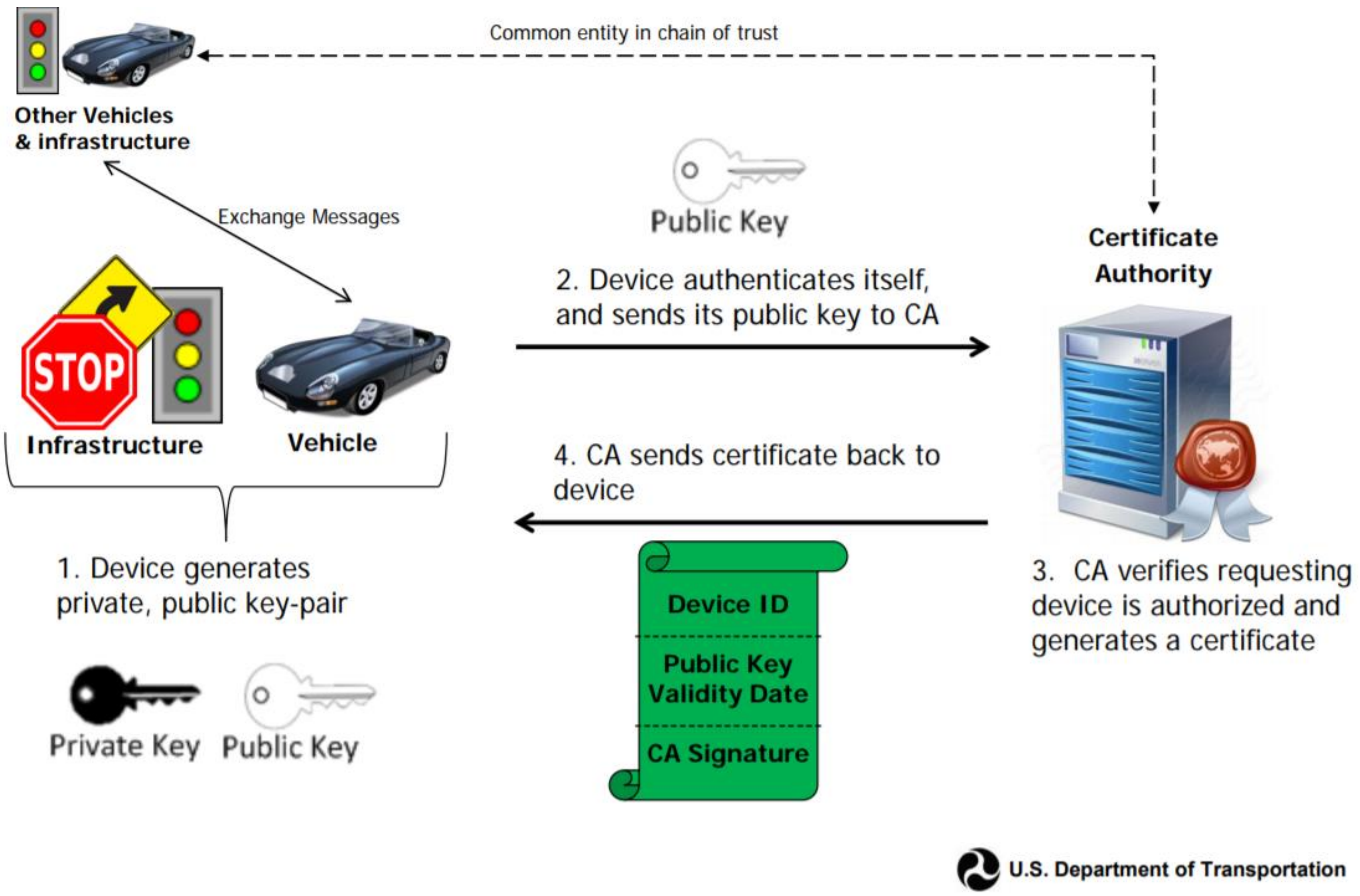
- Security is always "left to the upper layers"
- IEEE 1609.2 (2016)
  - Processes for secure messages (transmit and receive)
  - Protection from eavesdropping, spoofing, alteration, replay, …
  - Protect privacy
  - Amended by IEEE 1609.2a (2017), 1609.2b (2019)
    - Improvements, errata and minor additions
- 1609.2.1 (2020) – Cert. Mgmt. for End Entities
  - How to request and receive certificates on vehicles, RSUs, etc.

IEEE 1609.2-2016

- Mechanisms for secure V2V message exchange
- Digital signatures for authentication and integrity
  - Elliptic Curve Digital Signature Algorithm (ECDSA)
- Signatures are authenticated with certificates
  - IEEE 1609.2.1 (2020)
  - Requires vehicular public key infrastructure (VPKI)

V2V Security: Vehicular Public Key Infrastructure (VPKI)

VPKI Architecture

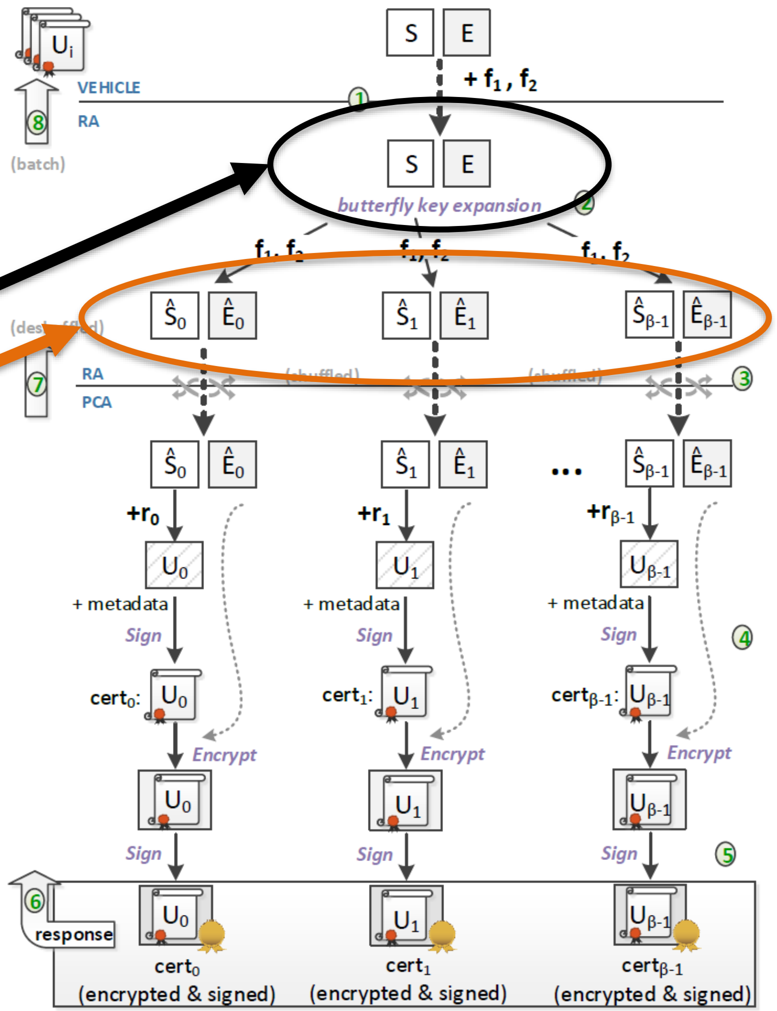


VPKI - The Problem of Scale

- ~270 million registered vehicles in the US in 2018
  - Vehicles are pre-loaded with up to ~3000 certificates
  - May need to manage up to 1 trillion (!!) certificates
  - This is just for vehicles – even more certs needed for V2I, V2N
  - Efforts taken to address this are untested (but promising)
- Who will manage the certificates?
  - Plans tend to be bloc- or nation-specific (E.U., U.S., China, …)
  - What about driving internationally?

Addressing the Problem of Scale

- Instead of pre-loading all keys, pre-load some and derive the rest!
- Butterfly keys use one seed keypair to derive all future keys
- Significantly reduce overhead
  - Reduce # of required key reloads
  - Make the VPKI scalable



M. A. Simplicio, E. L. Cominetti, H. K. Patil, J. E. Ricardini and M. V. M. Silva, "The Unified Butterfly Effect: Efficient Security Credential Management System for Vehicular Communications," *2018 IEEE Vehicular Networking Conference (VNC)*, 2018

Protecting Privacy in V2V

- V2V messages are broadcast and (usually) unencrypted
  - Very easy to track a vehicle and its driver(s)
  - Location tracking, behavior analysis, …
- Using one certificate to sign messages long-term is bad
- 1609.2 requires pseudonym certificates instead
  - Short-term certificates derived from private-key certificate
  - Cannot be linked to vehicle's real, permanent identity
  - Used to sign V2V messages
  - Each pseudonym certificate is used for no more than 5 minutes

V2N Security: An Overview

LTE-V2X Network Mode Security

- V2N mode can leverage LTE security mechanisms
  - Evolved Packet System Authentication and Key Agreement (EPS-AKA) protocol
  - Authentication, integrity checking, and encryption provided
- Privacy loss from attachment to LTE core network
- Still vulnerable to conventional LTE attacks
  - IMSI catching, GUTI disclosure, ...
  - Privacy concerns are especially prevalent

V2N Security in NR-V2X

- Many improvements on LTE-V2X
- Privacy is emphasized
  - Concealed and/or encrypted identifiers
- Primary and secondary authentication
  - Support 3rd party application integration
- Communication with non-cellular networks
  - Cross-technology communication (Wi-Fi, IoT, …)

Trusted Non-3GPP Access

- Allow devices to securely contact the 5G Core network via non-cellular protocols like WLAN or WiMAX
- Centralize authentication processes in 5G Core
- Improved V2I and V2D device diversity
  - Non-cellular devices (e.g., IoT) can act as RSUs
- EAP-AKA or 5G-AKA can be used for authentication

Secondary Authentication

- AKMA – Authentication and Key Management for Applications
  - For third-party applications and services
  - Use cellular authentication to bootstrap application-layer security/key derivation (generic bootstrapping architecture – GBA)
- Obviate the need for PKI or hard-coded credentials
  - Greatly reduce complexity of VPKI design and deployment