Privacy and Identity Management

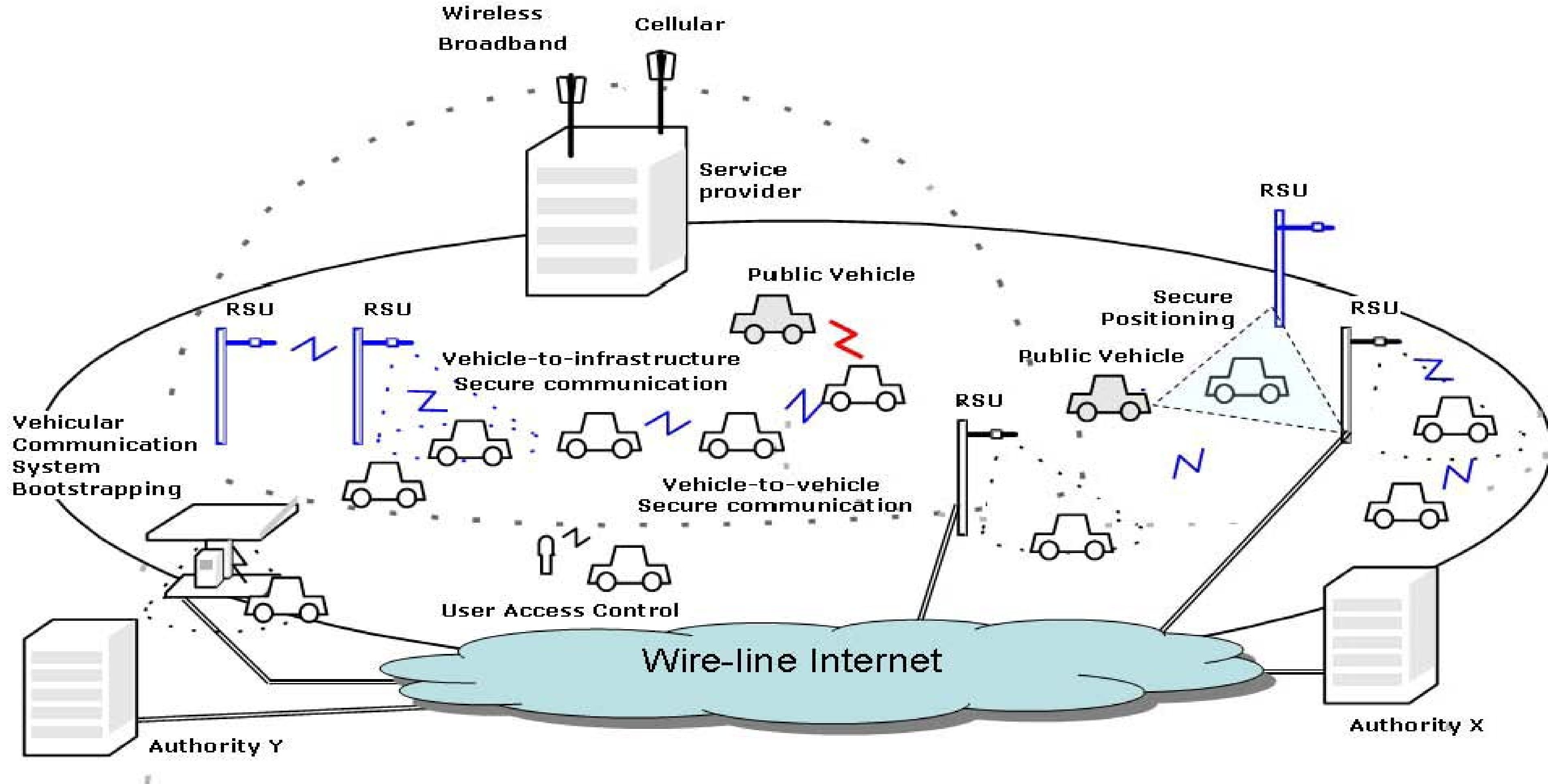
in Secure Vehicular Communication (VC) Systems

Panos Papadimitratos

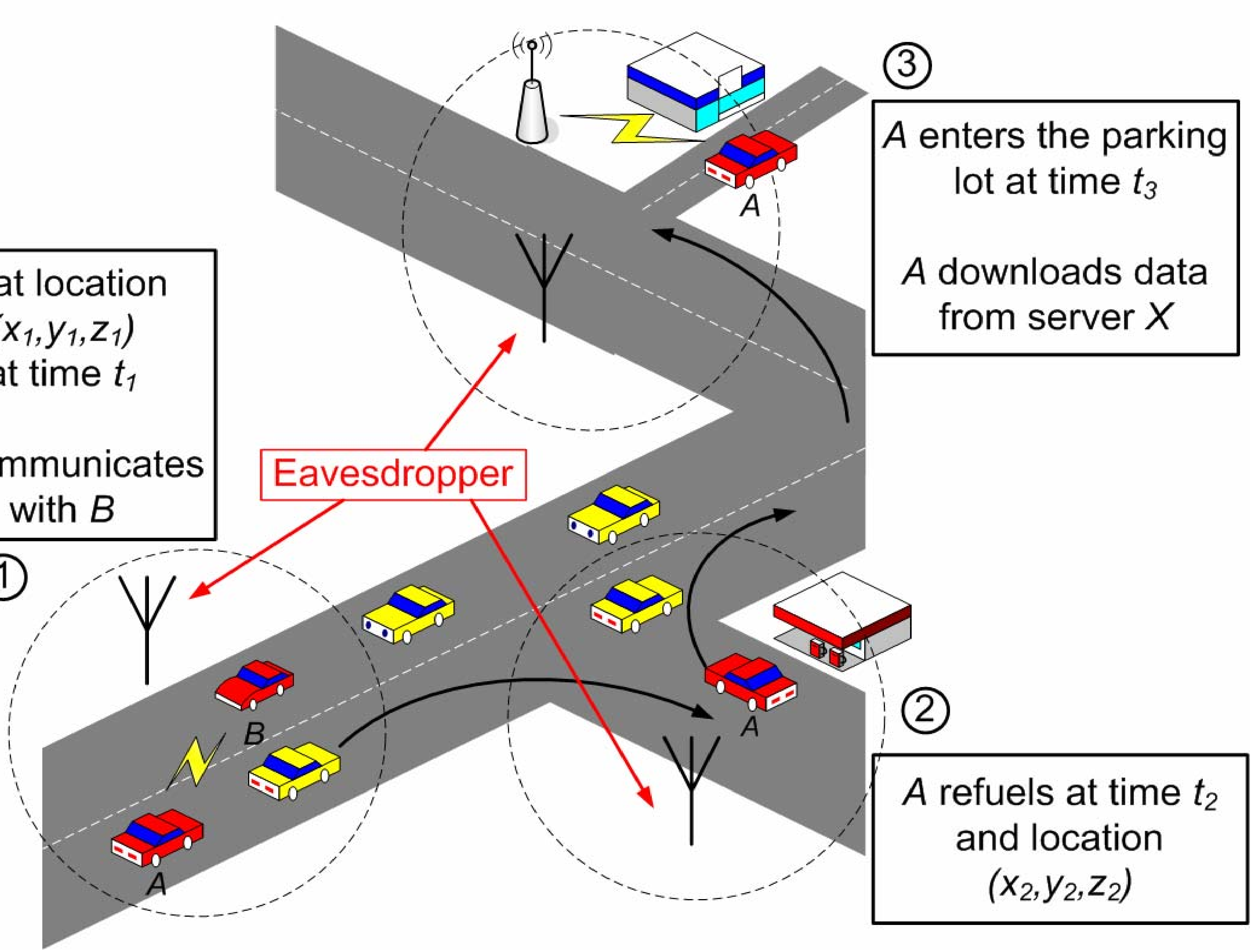
panos.papadimitratos@epfl.ch

EPFL

Secure VC Architecture Overview
An Illustration



Exploit: Vehicle and User Tracking



A at location
(x_1,y_1,z_1)
at time t_1

A communicates
with *B*

A refuels at time t_2
and location
(x_2,y_2,z_2)

A enters the parking
lot at time t_3

A downloads data
from server *X*

Pre-VC Transportation Systems

- Administered by public organizations
  - City, County, State Authorities
- Participants
  - Vehicles
  - Drivers
- Rigid identity management processes
- Liability

Pre-VC Transportation Systems
(cont'd)

- Drivers and vehicles already identified in multiple ways
  - Drivers
    - Name
    - License number
    - Mailing address
    - Date of birth
  - Vehicles
    - Vehicle identification number (VIN)
    - Registration number
    - Technical information
      - Type
      - Model
      - Color

Secure Vehicular Communication Systems

- System participants
  - Users
  - Network nodes
    - Roadside infrastructure
    - Vehicles; private, public
  - Authorities
    - Servers at the wire-line part of the network
    - Infrastructure acting as a gateway to/from the wireless part of the vehicular network
- Focus on network operation and device communication
- Binding users to vehicles is an important issue
  - Many-to-many relationship

Secure Vehicular Communication Systems (cont'd)

- Relation between "physical" and VC identities
  - Integration - Adaptation
  - Extension
- VC system identity
  - "Physical world" attributes
  - Network identifiers
    - At different layers of the protocol stack
  - Service identifiers/credentials
  - Cryptographic keys and credentials

Problem statement

- Secure vehicular communication systems
  - Identity management
  - Privacy protection
    - Anonymity
- Why?
  - VC systems may facilitate antisocial behavior
  - Attackers will always be present
  - User requirement
  - Deployment violating rights of individuals
- Challenge
  - Are available privacy-enhancing technologies appropriate for the vehicular communications environment?
  - Security is at odds with privacy
    - Not only due to the need for liability attribution,

Towards VC Privacy

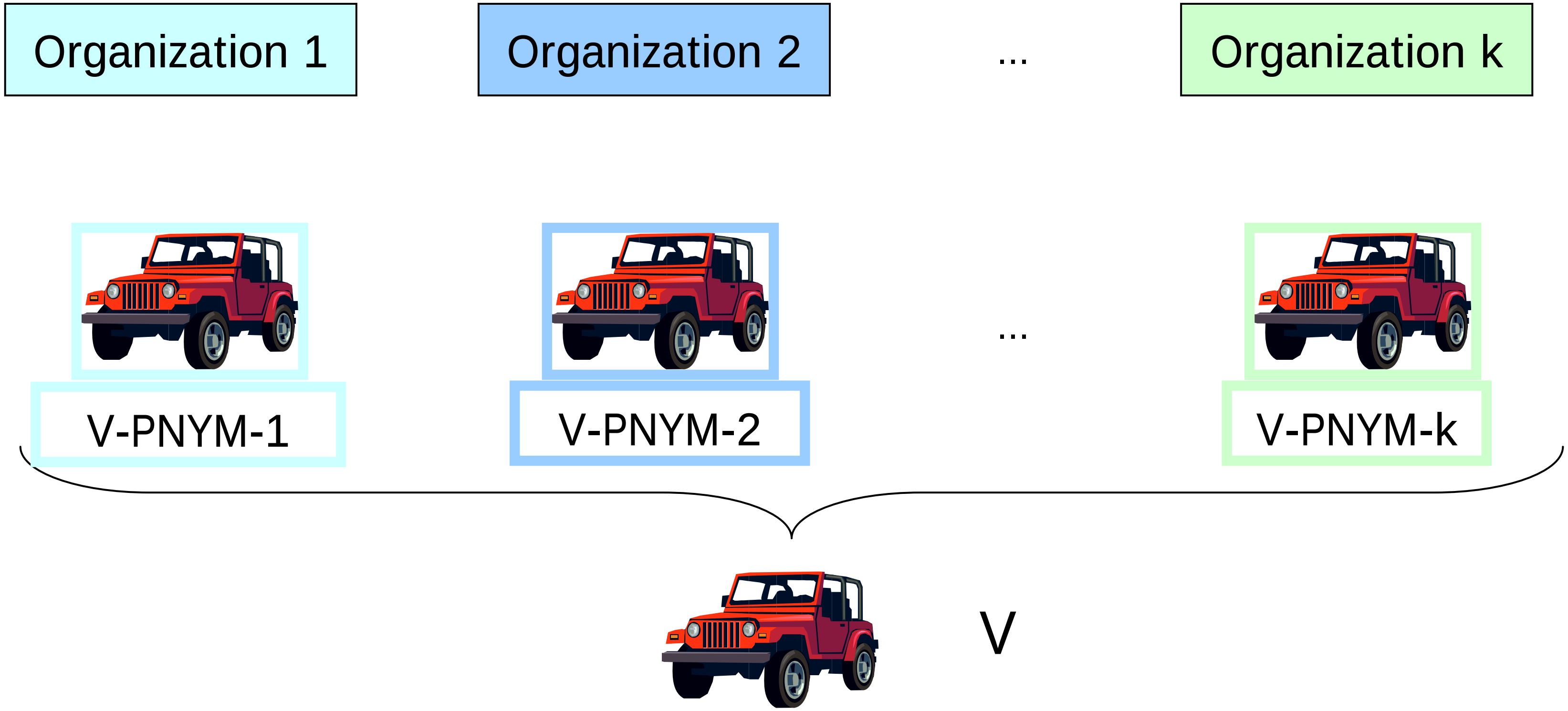
- Approach 1:
  - Protect sensitive data
  - Define processes and policies for privacy protection
  - Minimum private information disclosure on a need-basis only
  - Fine-grained control mechanisms for system entities to regulate private information disclosure

Towards VC Privacy (cont'd)

- But authentication implies identification
  - Cryptographic keys and credentials are necessary
  - Credentials, i.e., certificates, identify their subjects
- Examples
  - Service access
  - Area access control

Towards VC Privacy (cont'd)

- Approach 2:
  - Partitioning of identity into multiple partial identities (pseudonyms) each associated with a subset of attributes



Organization 1

Organization 2

...

Organization k

V-PNYM-1

V-PNYM-2

...

V-PNYM-k

V

Towards VC Privacy (cont'd)

- Approach 3:
  - Remove all identifying information from the credentials
  - Introduction of the "pseudonym" concept
    - D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM 1981
    - D. Chaum, "Security without identification: Transactions to make big brother obsolete," Comm. ACM 1985
  - Many other pseudonymous/anonymous schemes with diverse characteristics followed
  - Recently, application in VC contemplated by many research efforts, e.g., NoW, UUlm, EPFL

Towards VC Privacy (cont'd)

- Approach 4:
  - Certification authority (CA)
    - Long-term basic unique identities
  - Anonymous/Pseudonymous credential issuer(s)
- Accountability
  - Resolution of pseudonyms/anonymous credentials to long-term identities
  - Well-defined policies on the conditions that warrant (anonymity) revocation
  - Separation of privilege

Points of caution (cont'd)

- Sharing of credentials
  - Node/user A should not be able to use pseudonyms/anonymous credentials issued to node/user B
- Credential forgery
  - One or more users should not be able to forge pseudonyms/anonymous credentials
- Pseudonym linking
  - Any observer of communication (transactions) should not be able to link pseudonyms/anonymous credentials issued by distinct organizations
  - Any two or more organizations should not be able to link pseudonyms they issued to the same node/user

Points of caution (cont'd)

- Pseudonymity/anonymity cloak enables attacks
  - Attackers can inject misleading data
  - If anonymous, attackers can inject a large volume of false data
  - Unless an appropriate defense mechanism is implemented, such an attack can remain undetected for a long period of time

Points of caution (cont'd)

- VC patterns are not 'transactional'
  - Broadcast, multicast, anycast, geocast
  - Potentially any node can be a verifier

- VC systems are not user-centric
  - Vehicles play a central role
  - Vehicles could be identifiable in different ways
    - E.g., Individual subsystems of the vehicle

Points of caution (cont'd)

- Communication cannot be regulated or controlled by the node/user
  - Safety messaging and applications will be 'always-on'
- Frequent/high-rate/continuous communication
  - Dependent on network characteristics (e.g., density)
- Performance overhead can be critical
  - Even though anonymity is a prerequisite for private vehicles only
    - Infrastructure and public vehicles do not need to be anonymous

Points of caution (cont'd)

- Unlinkability at the network and data link layers
  - Impact on system performance
- Eliminate 'weak links'
  - Coexistence/inter-operability with other wireless communication systems, e.g., cellular, WiMax

Current efforts

- We have been developing a solution based on well-accepted building blocks (e.g., cryptographic primitives) and concepts (e.g., anonymized certificates/pseudonyms)

- At the same time
  - Established a liaison with the PRIME project
  - Collaborating with IBM, exploring additional research issues and future solutions

Conclusions

- Within VC, privacy and identity management are largely open problems
  - VC systems have unique characteristics; not just another mobile wireless communication technology to access the Internet

- Assumptions and requirements for identity management and privacy can strongly influence the overall architecture of VC systems