A Highly Available and Dynamically Scalable Vehicular Public-Key Infrastructure (VPKI): VPKI as a Service (VPKIaaS)

Hamid Noroozi, Mohammad Khodaei and Panos Papadimitratos
Networked Systems Security Group
KTH Royal Institute of Technology
www.ee.kth.se/nss

Background

Figure 1: Secure and privacy-protecting V2N and/or V2I (V2X) communication [3]

Figure 2: A Vehicular Public-Key Infrastructure (VPKI) Architecture [4]

• Vehicle registration with its home Long Term Certification Authority (LTCA), obtaining an X.509 certificate
• Anonymous ticket acquisition from the LTCA
• Anonymous certificate(s)/pseudonym(s) acquisition from any Pseudonym Certification Authority (PCA)
• Resolution process initiation by Resolution Authority (RA) (conditional anonymity)

Challenges and Objectives

Figure 3: LTCA servers under a DDoS attack [4]

• High Availability
  - Self-healing
  - SLA improvement
• Dynamic Scalability
  - Consistent performance on higher load
  - Partial resilience against DDoS
  - Resource efficiency on dynamic load

Cloud-Native Approach

Figure 4: PCA servers

• Architect VPKI in Microservices [5]
• Plan to scale in/out services
  - Handle race and deadlock conditions
  - Automate scaling in/out
  - Define load and health in metrics
  - Publish metrics

Containers Orchestration

Figure 5: Cloud Native Approach

• System definition in Topology and Orchestration Specification for Cloud Applications (TOSCA) [7]
• Service orchestration
  - Service registry
  - Load balancing
• State Sharing (Using Raft) [6]
• Publishing Key Performance Indicator (KPI)

Figure 6: Containers orchestration scheme

Performance evaluation

• Load test
  - Increase load steadily
  - Stress test
  - Intense load try to break
  - Chaos monkey test [8]
  - Negative test
• Benchmark test
  - Resource planning
  - Large-scale Vehicular Communication (VC) deployment

Future work

• Disaster Recovery as a Service
  - Geo-Replication
  - Recover after failure with data loss
• Compromised/Malicious internal VPKI entities

References