Aerolink™

Security for connected vehicle: successes and challenges

William Whyte, Chief Scientist

2015-03-05

SecurityInnovation®
EMBEDDED SECURITY BUSINESS UNIT

About Security Innovation

- Authority in Software Security
  - 15+ years research on vulnerabilities
  - Security Testing methodology adopted by Adobe, Microsoft, Symantec, McAfee, and others
  - Authors of 16 books, 4 co-authored with Microsoft
  - Security partner for Dell, Microsoft, Cisco, HP, IBM, PCI SSC, FS-ISAC, NXP, and others
  - 9 Patents

- Helping Organizations Secure Embedded Software
  - EMBEDDED SOFTWARE SECURITY TESTING
  - EMBEDDED SOFTWARE SECURITY TRAINING
  - EMBEDDED SYSTEMS SECURITY

cisco FUJITSU ING hp SONY Microsoft ERICSSON StateFarm DELL Ryder amazon.com Google intel Nationwide FedEx BARCLAYS AS INSTRUMENTS symantec

Security

Aerolink

SI Expertise

- Unparalleled Software Vulnerability Expertise
  - 10+ years of research on security vulnerabilities
  - Hundreds of technical assessments on world's most dominant software and computing platforms
  - Security testing methodology adopted by Symantec, Microsoft, McAfee
- Future-Proof Cryptography (6 patents)
  - Resistant to quantum computing attacks
  - Adopted as IEEE and X9 standards
- Working in Connected Vehicle security since 2003
  - Aerolink is market-leading implementation of both EU and US communications security standards
- Complete Solution Set
  - People. Training for excellence and self-sustainability
  - Process. Consulting to help deliver secure products
  - Technology. Products and services to deploy secure software systems

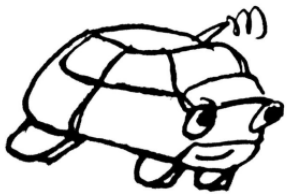
symantec. SONY
MassMutual FINANCIAL GROUP EMC² where information lives
DELL ING
CREDIT SUISSE
BARCLAYS
Microsoft

Security

Aerolink

Communications Security: Threats

- Cars can communicate to improve mobility, reduce accidents etc but…

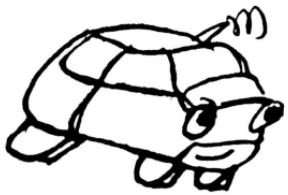


Threats: Confidentiality

- Cars can communicate to improve mobility, reduce accidents etc but…
  - Eavesdroppers might overhear sensitive data

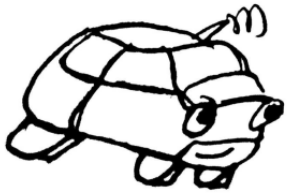
Threats: Authenticity, Integrity

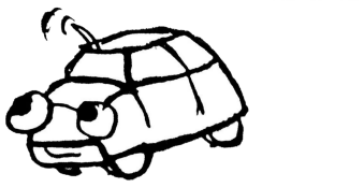
- Cars can communicate to improve mobility, reduce accidents etc but…
  - Eavesdroppers might overhear sensitive data
  - Impersonators might send false messages, reducing trust in system (or worse?)



Threats: Authorization

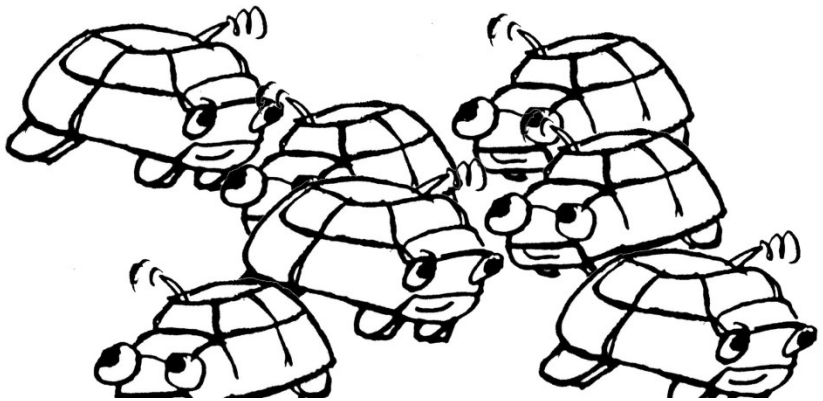
- Cars can communicate to improve mobility, reduce accidents etc but…
  - Eavesdroppers might overhear sensitive data
  - Impersonators might send false messages, reducing trust in system
  - … or pretend to have more privileges than they're entitled to





Threats: Privacy

- Cars can communicate to improve mobility, reduce accidents etc but…
  - Eavesdroppers might overhear sensitive data
  - Impersonators might send false messages, reducing trust in system
  - … or pretend to have more privileges than they're entitled to
  - Someone might record you at different places...

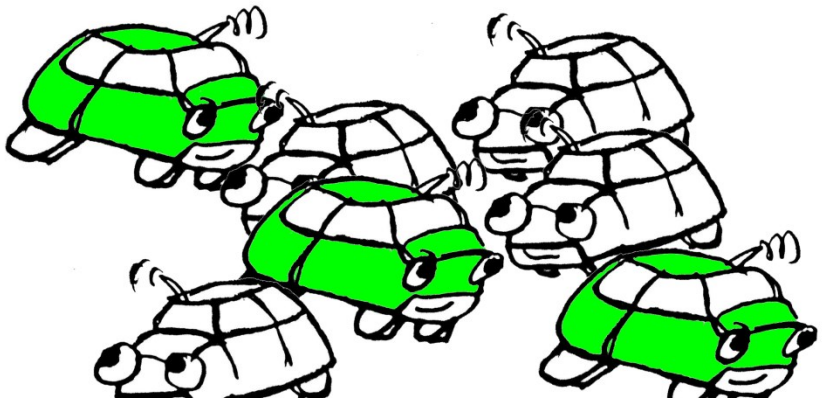


Security

Aerolink

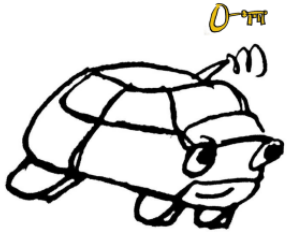
Threats: Privacy

- Cars can communicate to improve mobility, reduce accidents etc but…
  - Eavesdroppers might overhear sensitive data
  - Impersonators might send false messages, reducing trust in system
  - … or pretend to have more privileges than they're entitled to
  - Someone might record you at different places, discover each recording is you, and blackmail you or worse
    - C-ITS-specific threat!



Successes: Encryption

- Defeat eavesdropping
- Each device has a key that other devices can use to encrypt to it

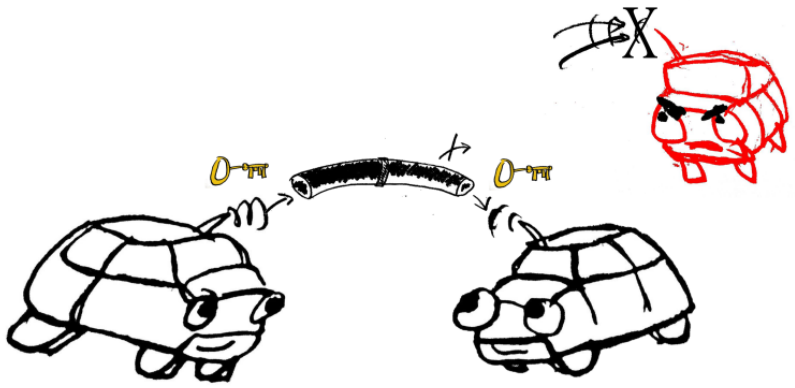


Security

Aerolink

Successes: Encryption

- Defeat eavesdropping
- Each device has a key that other devices can use to encrypt to it
- This creates an encrypted “pipe” that eavesdroppers can’t break through

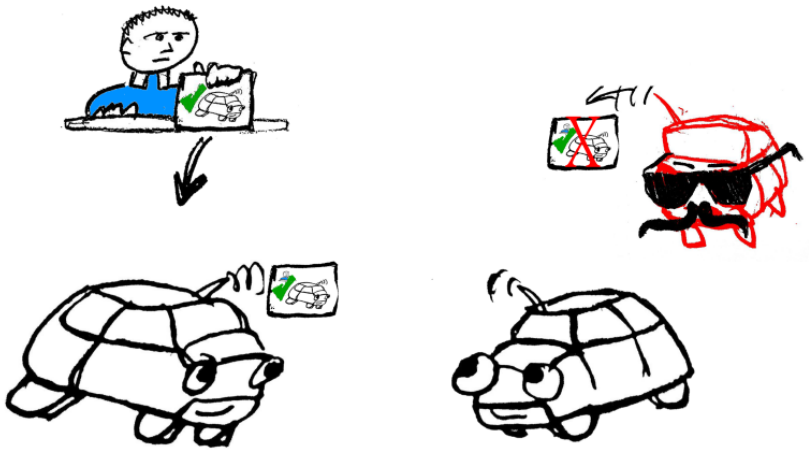


Security

Aerolink

Successes: Authentication / Integrity

- Each device has a credential that it cryptographically binds to a message
  - Demonstrates it originated a given message and the message has not been altered
  - Credential is called a “certificate”
  - Cryptographic binding is called “signing”
  - Credential is issued by a Certificate Authority or CA

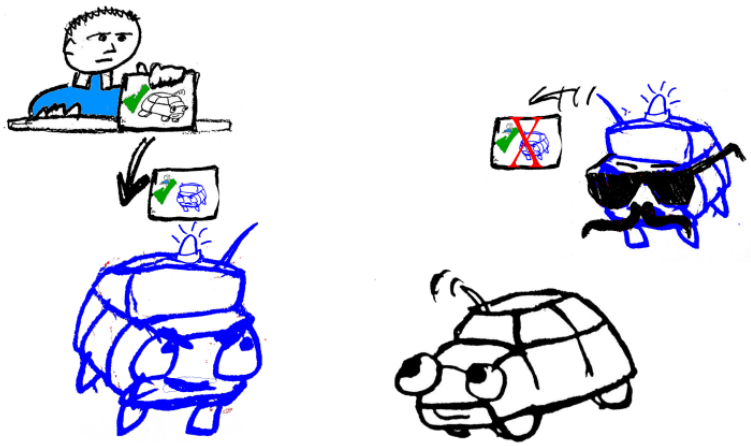


Security

Aerolink

Successes: Authorization

- Each device has a credential that it cryptographically binds to a message
- Credentials state your permissions
- If you don't have a police car certificate, you can't claim to be a police car

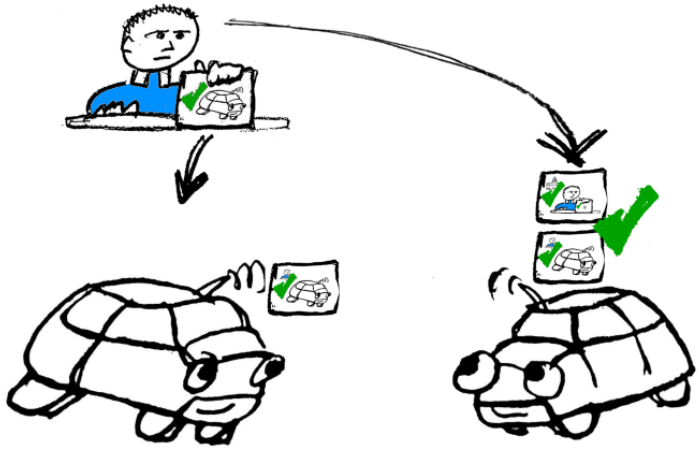


Security

Aerolink

Using credentials (1)

- How does the receiver trust received credentials?
- The CA has a certificate itself which it binds cryptographically to the device's certificate
- The receiver knows the CA certificate
  - Checks that the CA certificate authorizes and is bound to the device's certificate
  - Checks that the device's certificate authorizes and is bound to the message
  - Trusts the message!

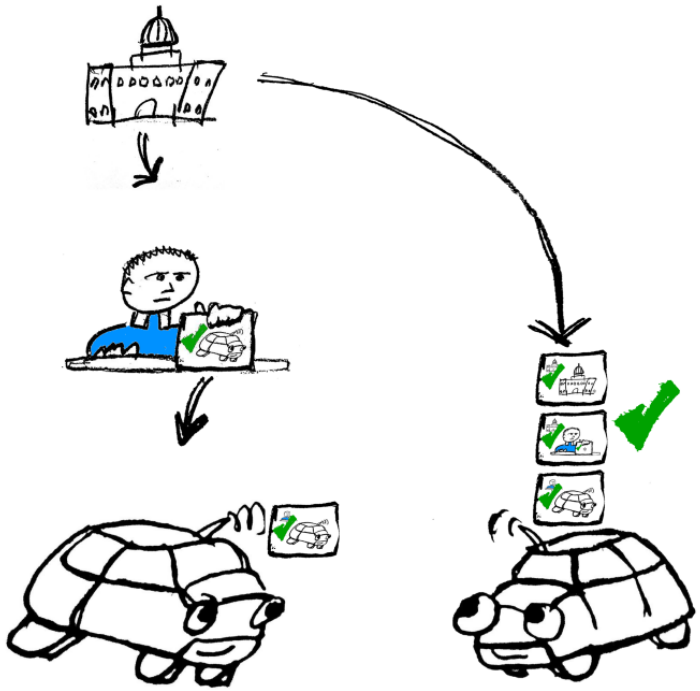


Security

Aerolink

Using credentials (2): PKI

- How does the receiver know the CA certificate?
- CA certificate might be known already
- If it's new, the receiver can construct a *trust chain* back to a *root CA*.
- There's a relatively small set of root CAs
  - These can authorize an arbitrarily large number of intermediate and end-entity Cas

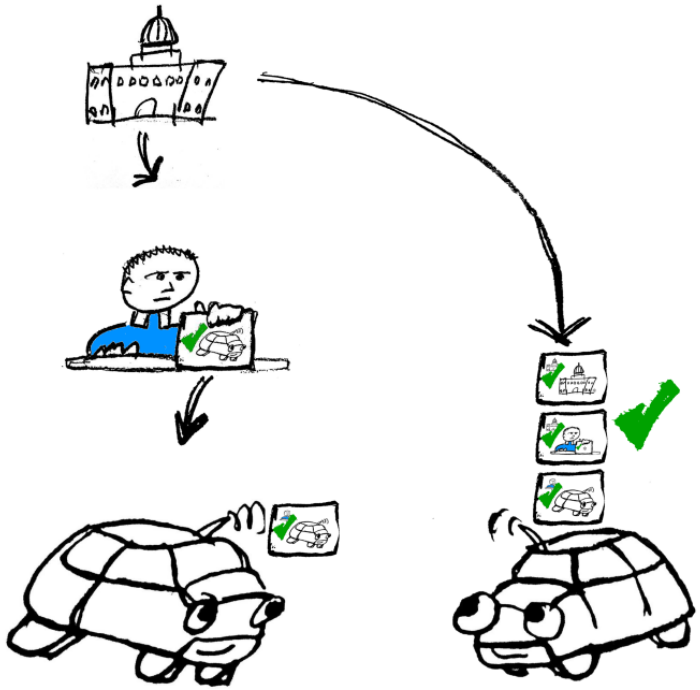


Security

Aerolink

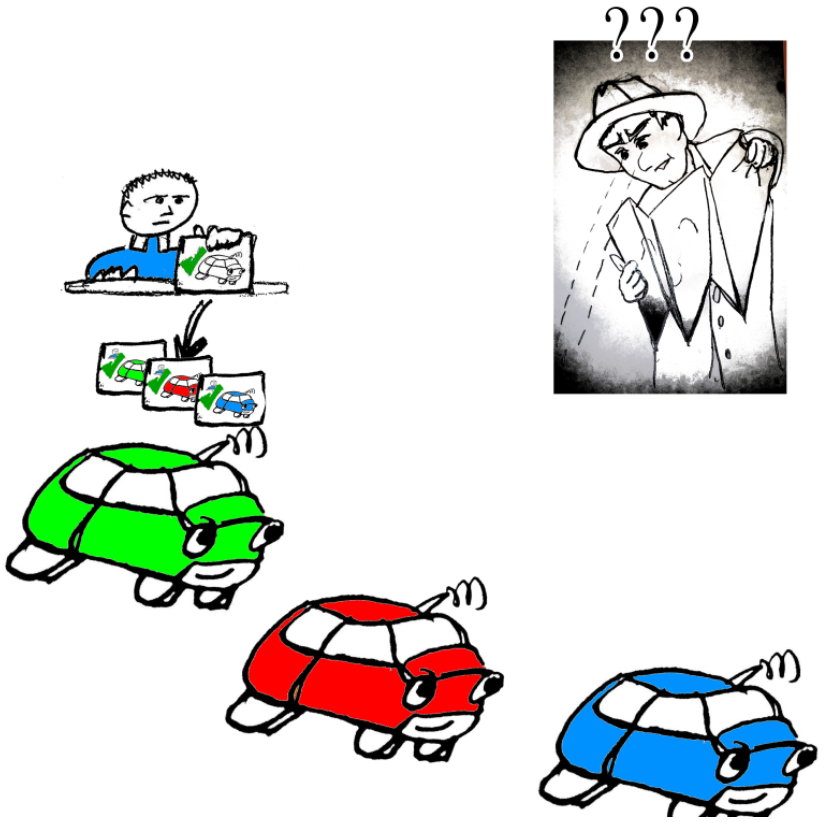
Using credentials (3): Bad actors

- A device that sends false messages should no longer be trusted
- Misbehavior Detection functionality detects false messages
- An enforcement function removes the bad device's privileges
  - Either its credentials are "revoked" via a Certificate Revocation List (CRL)
  - Or it uses its existing credentials till they expire but then does not get any more



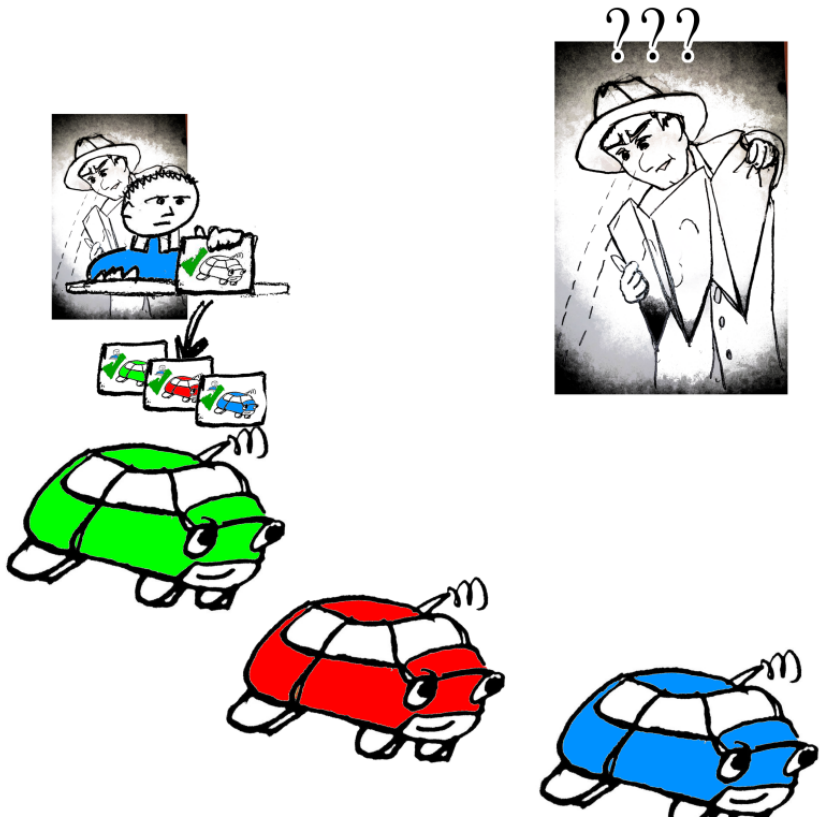
Successes: Anti-linking

- Devices can change identifiers from time to time, disrupting linking by all but the most powerful eavesdroppers
- This is enabled by issuing many different certificates to each device



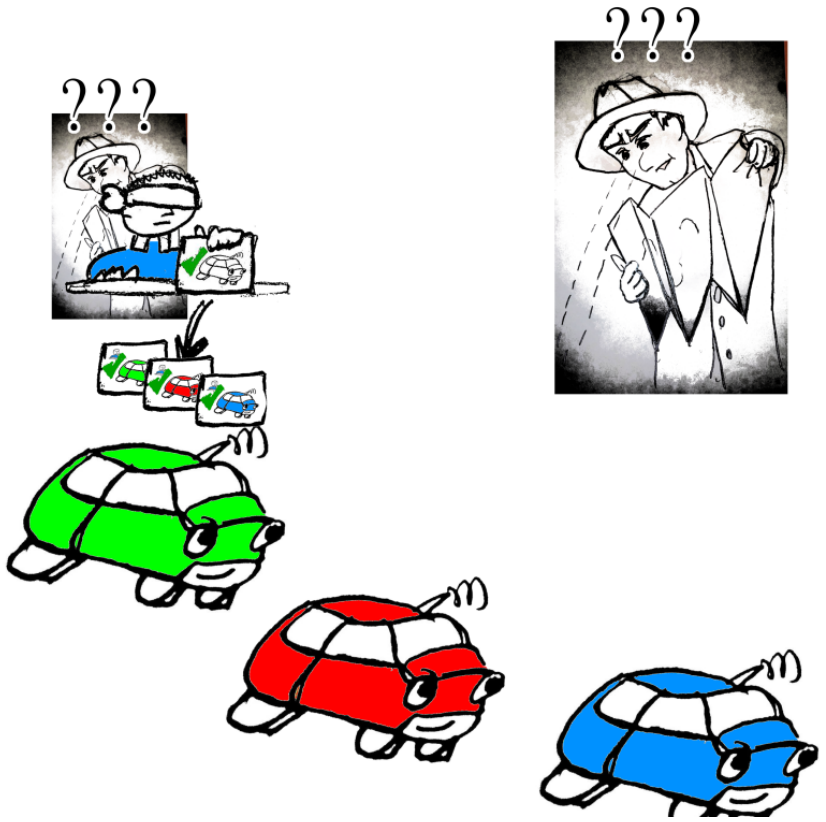
Successes: Anti-linking

- Devices can change identifiers from time to time, disrupting linking by all but the most powerful eavesdroppers
- This is enabled by issuing many different certificates to each device
- Of course, this means a CA could link if it knows which certificates go to which device



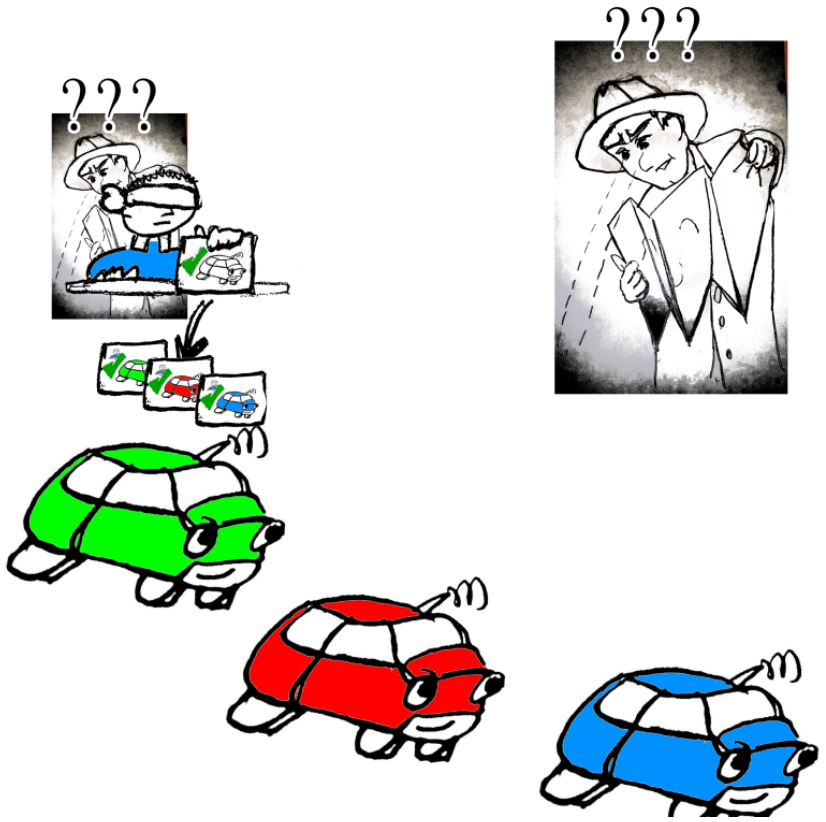
Successes: Anti-linking

- Devices can change identifiers from time to time, disrupting linking by all but the most powerful eavesdroppers
- This is enabled by issuing many different certificates to each device
- Of course, this means a CA could link if it knows which certificates go to which device
- … so the (US) system “blinds” the CA, preventing insiders as well as outsiders from linking



Successes: Anti-linking

- Devices can change identifiers from time to time, disrupting linking by all but the most powerful eavesdroppers
- This is enabled by issuing many different certificates to each device
- Of course, this means a CA could link if it knows which certificates go to which device
- … so the (US) system “blinds” the CA, preventing insiders as well as outsiders from linking
- This is done while keeping CRLs relatively small



Security

Aerolink

Successes!

- Standards have been defined
  - Communications
  - Credential management
- Technology has been successfully field tested
- Projects are underway to build PKIs
  - In Europe and USA
- OBEs in Europe and the US are hardware compatible

Security

Aerolink

Remaining challenges

- PKI governance
- Privacy
- Secure implementations
- Multiple applications
- Cross-border issues and harmonization of trust
- Interoperability across borders

PKI governance

- Who runs the PKI?
- How is it paid for?
- What is the business structure?
- Where does liability reside?

Privacy

- Are the technological countermeasures for privacy good enough?
- Does it matter?
- What happens as the system supports more applications?
- How can we prevent data that's gathered being misused by corporations, law enforcement, national security etc?
  - If people turn off the system, no safety-of-life benefits

Cybersecurity

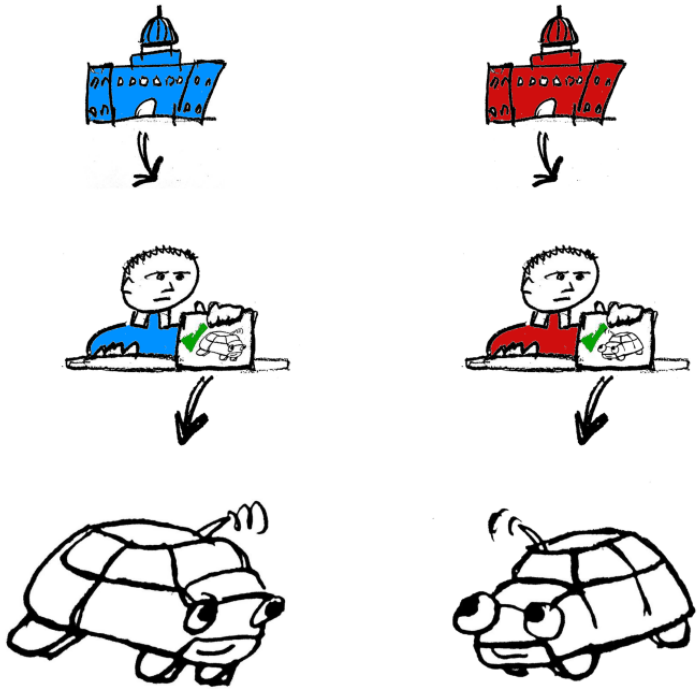
- Vehicles are becoming networked
- Communications security of system seems solid
  - Well reviewed, field tested
- However, this creates new entry points into the car
- Implications for security in IVN:
  - Messages coming in should not be command messages
  - Messages going out should come from authenticated components
- NHTSA (National Highway Transportation Safety Administration) is currently working on cybersecurity policy
  - Investigative phase at the moment
  - May turn into regulation in the future

Multiple applications

- Will applications prioritize correctly?
- Can different applications harm privacy when they run together?
  - Is this a problem that C-ITS needs to come up with a solution to?
- Will governance bodies for all applications be willing to be governed by the existing SCMS?

Cross-border issues and harmonization of trust

- How do devices authorized by one SCMS trust devices authorized by other SCMSes?
  - Cross-certification?
- What happens if a new SCMS is started?
- Will there be too many root CAs?
- What happens if an SCMS is no longer trusted?

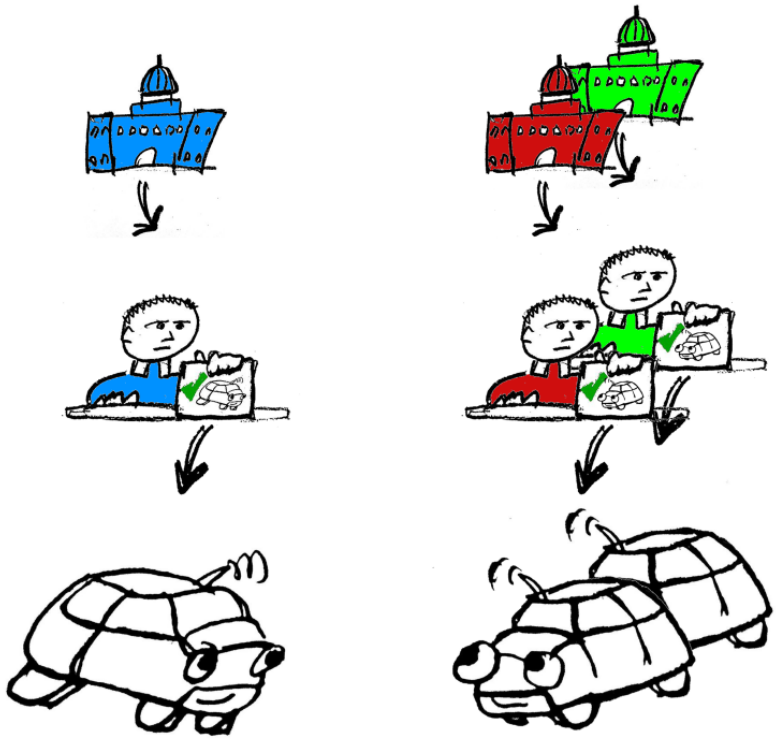


Security

Aerolink

Cross-border issues and harmonization of trust

- How do devices authorized by one SCMS trust devices authorized by other SCMSes?
  - Cross-certification?
- What happens if a new SCMS is started?
- Will there be too many root CAs?
- What happens if an SCMS is no longer trusted?

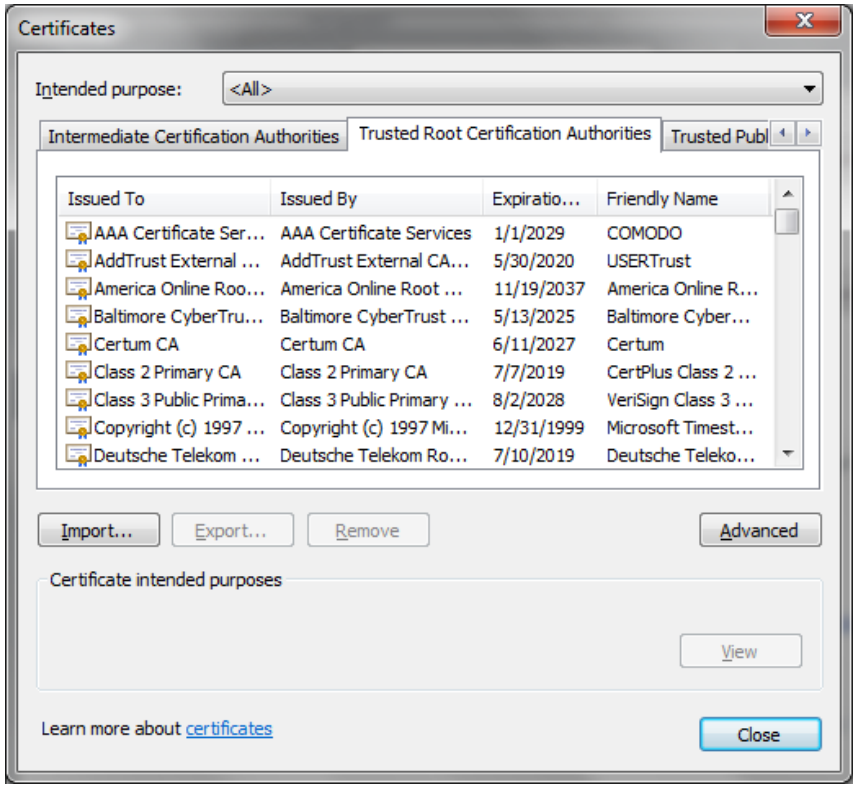


Security

Aerolink

Cross-border issues and harmonization of trust

- How do devices authorized by one SCMS trust devices authorized by other SCMSes?
  - Cross-certification?
- What happens if a new SCMS is started?
- Will there be too many root CAs?
- What happens if an SCMS is no longer trusted?

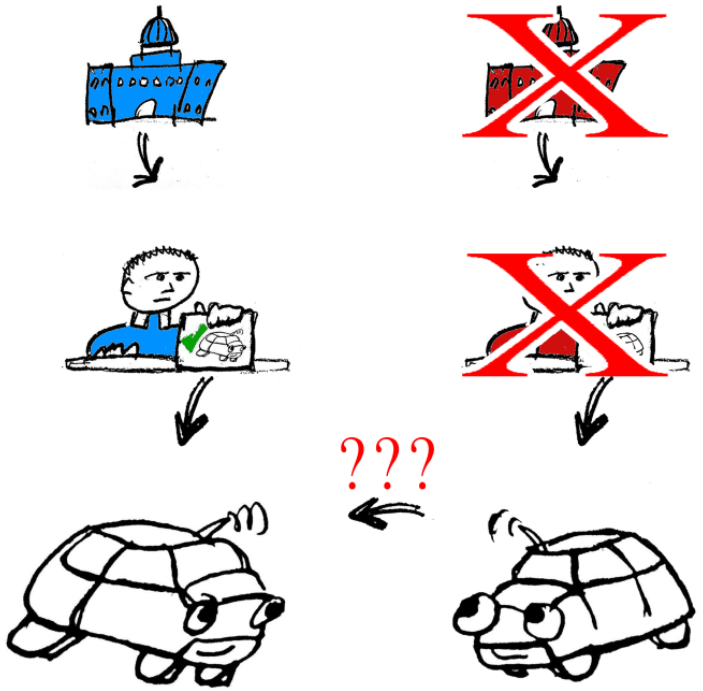


Security

Aerolink

Cross-border issues and harmonization of trust

- How do devices authorized by one SCMS trust devices authorized by other SCMSes?
  - Cross-certification?
- What happens if a new SCMS is started?
- Will there be too many root CAs?
- What happens if an SCMS is no longer trusted?



Trust and interoperability across borders

- What might change at a border?
  - Channel frequencies
  - Security protocol used (IEEE 1609.2 (US) v ETSI TS 103 097 (EU))
  - Uses of channels – safety v non-safety v control
  - Trusted roots
  - Privacy policies
- Cars mightn't go across major borders frequently but other C-ITS devices might
  - Shipping containers
  - C-ITS enabled smartphones

Security

Aerolink

Future-proofing

- How will we cope with software bugs?
- How will we cope with hardware that turns out to have a security flaw?
- How will we cope when quantum computers break elliptic curve cryptography?

Priorities: a personal list

- Harmonization of policies that might change across borders
  - Along with ways of communicating changed policies
- Standardized protocols for big SCMS changes
- Develop platform security requirements that take into account the fact that devices will be in the field for 30 years
  - Encourage industry to adopt and make public demonstrations of their commitment to secure coding practices
  - Come up with plans for managing “patch Tuesday” events seamlessly and securely
  - Get the world’s cryptographers working on post-quantum signature algorithms

Conclusions

- Lots of issues remain to be resolved
- But all are possible given the will and focus
- Exciting times!