CORA Connect for Automation & Mobility – an executive summary

CORA is a step beyond encryption that is unbreakable; **it is a 'probabilistic' approach to security** that is several thousand orders of magnitude stronger than current forms of encryption. CORA incorporates "Chaos Maps" to further 'randomize' the readable data and initial boundary conditions.

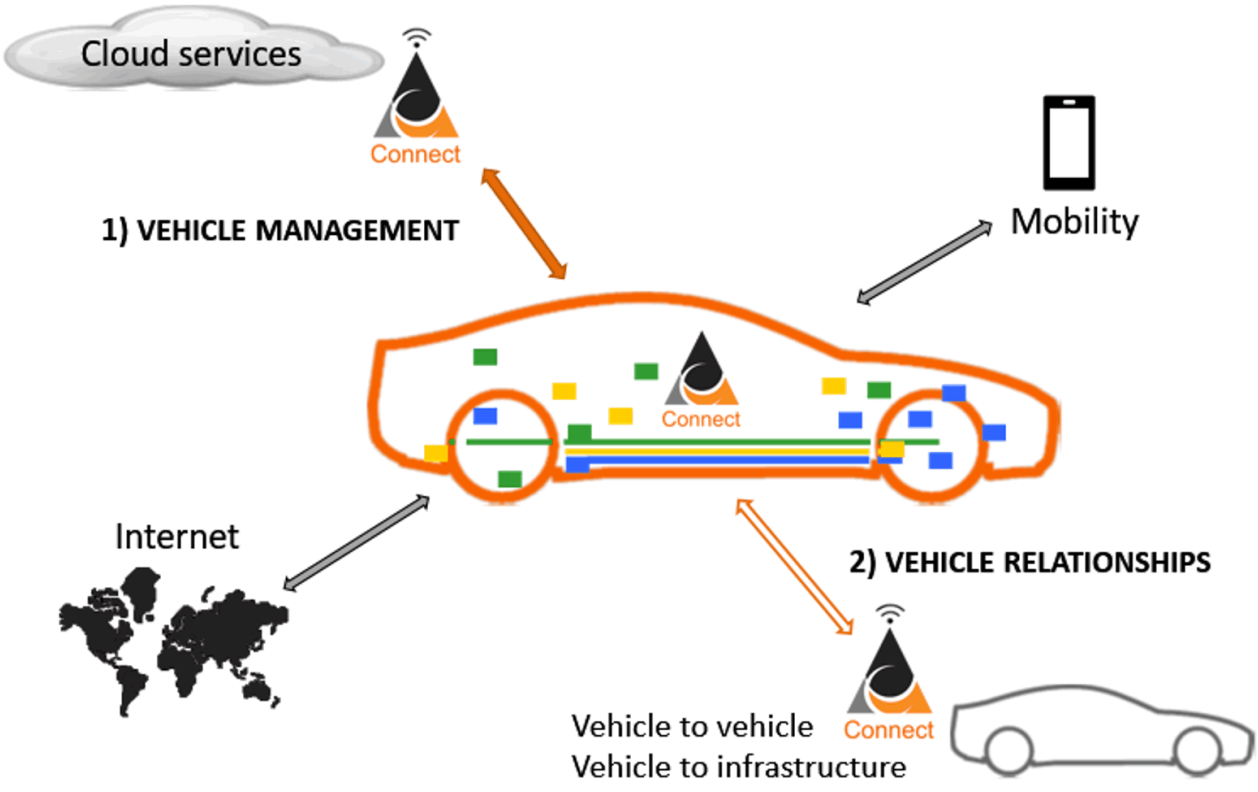
Memory, processing power, mathematically proficient experts and highly motivated, intelligent, cyber criminals are abundant in our global environment. **CORA removes the dependency on prime numbers** and ring or curve selection. Moreover, the incomprehensibly large numbers required for a brute force attack cannot be accomplished by any number of networked optical/quantum computers, or specialized hardware devices.

Scope

The application of CORA to connected and autonomous vehicles is ideally suited to both of these critical pathways:

1) Vehicle management (operations):
   a) Internal – buses, sensors, controls, operations
   b) External – updates, repairs, big data, access to vehicle
2) Vehicle relationships (*PKI proposals are focused on this pathway*):
   a) Vehicle to Vehicle
   b) Vehicle to Infrastructure

Figure 1- Abstraction of CORA for vehicle operations and V2V communication.



©2017 CORA Cyber Security Inc. All Rights Reserved

Timing

The National Highway Traffic Safety Administration (NHTSA), Department of Transportation (United States DOT), are working on the Federal Motor Vehicle Safety Standards for V2V Communications. They are still calling for alternate proposals and anticipate having a rule in effect by 2019. A transitional implementation is expected by 2021 with a full implementation projected for 2025 (new vehicle production).

Vehicles today are computers on wheels. Most have "update capability" and some of these are wirelessly implemented. Vehicles have been "connected" for well over a decade (navigation, road side assistance, etc.).

Vehicles have been hacked, and hijacked. The need for 'unbreakable security' is evident for V2V, and for, vehicle management and operations. CORA is capable of securing both of these needs without compromising the owner's right to privacy.

Numerous issues have come to the fore, including liability, confidence, privacy and the "right-to-repair". CORA addresses these issues by providing maximum flexibility while simplifying the design and implementation of its proposed security standards. Moreover, this implementation is '**privacy positive**' and can be implemented without identifying the particular vehicle, owner or driver.

Context

PKI requires reliable and persistent online connectivity, and the proper management of credentials and private keys.

The proposed standard of using **PKI for** V2V is **much more complicated and convoluted** than is in use with conventional 'open networks', including the internet. Furthermore, PKI proposals for V2V involve extremely difficult logistics for properly implementing and securing this emerging technology.

With so many intelligent people who are highly motivated to violate cyber security; **every level of complexity**, every node and connection, **represents a link in a chain that is a potential point of failure** - a target, attack, insertion, violation or breach.

Connectivity will at times be an issue, which introduces additional attack vectors. There are devices that can affect connectivity and others that can eavesdrop on communications. The proposed **PKI** involves many **liabilities**, ranging from **privacy** concerns, to ransom type attacks; what if a cybercriminal chooses to 'apparently corrupt' another vehicles certificates/connectivity; will there be legal / financial liabilities associated with being 'blacklisted' in such a 'complex' environment?

Managing and rotating certificates / keys on a time sensitive scale is a logistics nightmare. If there was an ideal environment where all parameters may be controlled, it might be possible; a moving vehicle operating wirelessly without globally available and reliable bandwidth, is not such an environment. **CORA increases security while reducing the dependency on 'connectivity', and eliminating the burden of rotating certificates** through CORAcsi's implementation of 'adaptation'.

CORAcsi's "adaptation" (CORA Block Control Arrays may be continuously modified and/or permuted) is 'privacy positive' while providing all the benefits of rotating keys, without their complexity or large footprint.

©2017 CORA Cyber Security Inc. All Rights Reserved

Side by side Comparison

	PKI	CORA
SCMS (Policy & Technical)	✓	✓ (Policies must be written)
FIPS-140 L3 storage	• Long term device enrollment certificate • Short term pseudonym certificates (hundreds) • RA, Intermediate CA and PCA certificates • RA address • System configuration files • Root CA certificate • All system private keys • The System Certificate Revocation List • All unsent misbehavior reports	• Long term PMK (Primary Management Key) • 2 Long term ACs (Access Code) • 2-3 variable UCMs (Universal Chaos Maps) • 2-3 CBCAs (CORA Block Control Arrays)
Government	• Root authority • Numerous connection to multiple other modules (CRLs, Misbehavior authority)	Universal Management: • Creates and manages UCMs • Creates and manages Ids
OEM	Vehicle relationships: Due to the complexity, the lines are convoluted (blurred): • Certificate management: Certificate Authority (multiple layers) • Registration & Enrollment: Device configuration manager	Vehicle relationships: • Handled by CBCA (adapt and respond) – escalated if necessary Vehicle management: • Creates and manages PMKs • Creates and manages ACs • Implementation of CBCAs • Manage collisions (misbehaviors)
Suppliers (OBE): • Tier 1 • Tier 2	**Certificates/Keys** 1) Complicated rotation of a **limited number** of certificates/**keys**. 2) Each certificate adds to memory. 3) Must handle CRL lists and activities. 4) Numerous connections between many authorities and modules.	**CBCAs** 1) **Millions** of permutations (rotations) with a **single CBCA** 2) Smaller memory footprint. 3) Adaptation, and challenge-response options, for misbehaviors

Conclusion

CORA represents a **less convoluted** and **more secure** implementation for connected and autonomous vehicles; one in which the driver/owner's **identity and privacy** are **protected**. CORA isn't about 'preventing the hack', but rather, CORA 'nullifies the hack'.

CORA is ideal for both vehicle management (operation), and vehicle relationships (V2V).

If interested in exploring CORAcsi's paper for Automation and Mobility, then please use *the Contact Form available at CORAcsi.com, located in the CORAcsi submenu*.

©2017 CORA Cyber Security Inc. All Rights Reserved