Defensive Cyber Architecture for Vehicles & System-of-Systems

Anne Nowlin, COO
ENT Technologies, Inc.

Cyber vulnerabilities of in-vehicle electronic data networks have been documented by researchers, and even led to the costly recall 1.4 million Jeeps by Chrysler in 2015. Modern cryptographic countermeasures used in enterprise information systems such as trusted identity and access control have not been applied to these systems, which remain completely open and unregulated. Furthermore, legacy CAN bus systems inherently trust information coming from the controllers, under the assumption that they are invulnerable to outside access.

Our increasingly networked world of things has proven this latter assumption to be incorrect, as proven in multiple tests among researchers across the world. Both remote attacks through open systems (such as on the Uconnect system in the Jeep attack), and local attacks through physically accessible open and unsecured ports provide attack vectors that can be leveraged against the system, including critical systems such as brakes and steering. In military ground vehicles, additional critical systems such as battle management and fire control are also in need of protections.

The root security problems, as identified by Trend Micro (p. 7)[1] are:

- First, any device connected to the CAN bus is allowed to read and write without any regulation. There is no authentication or access control mechanism.

- Secondly, all data coming from the CAN bus is trusted because the security model assumes that an attacker will never gain unauthorized access to the CAN bus.

- Lastly, there is no way to distinguish a genuine error message from a crafted one. In other words, it's impossible to know whether a device (e.g., infotainment) is truly faulty or if it's been compromised and is now going "off bus" because of an attacker's command.

These security problems all come down to lack of cryptographic authentication in the system. Given these inherent problems, simply applying after-the-fact measures such as an intrusion detection system, while certainly better than no measures at all, does not address the root problem of security in the system. We therefore propose a solution using the lightweight software protocol, Entity Network Translation (ENT), which addresses the basic weaknesses, or lack of security aspects, identified by Hoppe et al in their paper "Security threats to automotive

[1] Maggi, F. (2017). A Vulnerability in Modern Automotive Standards and How We Exploited It (Tech.). doi:https://documents.trendmicro.com/assets/A-Vulnerability-in-Modern-Automotive-Standards-and-How-We-Exploited-It.pdf

CAN networks – practical examples and selected short-term countermeasures." [2] These security aspects are:

1. Authenticity: All ECU's should be identified and verified that they are authentic.

2. Confidentiality: Communication between ECU's should be protected from view by unauthorized parties.

3. Integrity – Ability to verify the incoming message is the same as the original message sent to the bus.

4. Non-repudiation – proof that the sender did or did not send a message, and that a receiver did or did not receive the message.

5. Authorizations / Access control – granular, directional access control of each controller is provided by the ENT protocol, such that systems will only recognize messages that a) are from authorized controllers, and b) provisioned to send messages to them, and will ignore all other messages. Diagnostic or maintenance access is inaccessible during normal driving operation.

Further phases could also extend use of the protocol to maintenance functions by adding the protocol to maintenance software interfaces so that only authorized equipment/personnel are authorized for access.

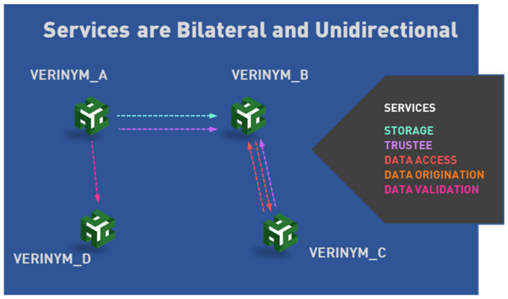
Approach to the Problem

The ENT protocol (ENT) is a lightweight software asymmetric-key-based protocol built on a scientific breakthrough called Relational Key Infrastructure (RKI). RKI can be thought of as a superset of PKI – that is, it can mimic the hierarchical topography of PKI – but unlike PKI, it is completely decentralized, so there are no calls back to a Certificate Authority, revocation list, or other mechanisms of a traditional PKI system.

ENT operationalizes RKI concepts with automatic key management, including issuance, revocation, and rotation. In ENT, identity is represented by data objects called Verinyms. Verinyms can represent identity of anything in a network, including components, devices, data, software and users.

Authorizations / Access control Through Services

Verinyms not only contain key material, but also its trusted relationships with other peer verinyms, plus the types of transactions it is explicitly provisioned to exchange with those peers. In ENT, we refer to different types of transactions as "services" or trust dimensions. Services include delegated control, data access, storage, routing, content distribution, etc. We call this agreement



[2] Hoppe, T., Kiltz, S., & Dittmann, J. (2011). Security Threats to Automotive CAN Networks – Practical Examples and Selected Short-Term Countermeasures. *Reliability Engineering & System Safety,96*(1), 11-25. doi:https://doi.org/10.1016/j.ress.2010.06.026.

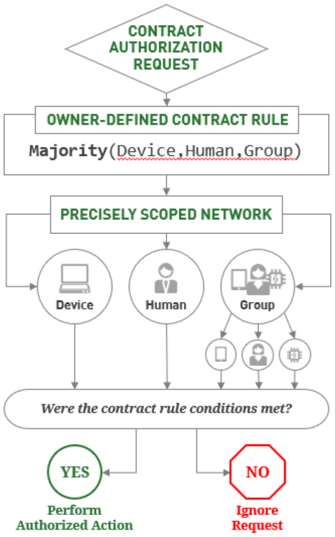
between two peer verinyms to exchange a service a “contract.” Contracts are **bilateral** – that is, an offer to provide or consume a service has to be matched by an agreement from the peer to consume or provide the requested service before the contract is enacted. Additionally, contracts are **bi-directional**. That is, an agreement by verinym A to provide data to verinym B does not mean that verinyms B also provides data to verinym A. This provides a mechanism for very granular control of risk and privacy.

Authentication

Contracts are used to create extremely strong trust and resilience in systems. Contracts form micro-networks with “authorization circuits” that define which whitelisted peers are authorized to authenticate network actions, and by what rules.

We refer to these authorization circuits as “n”-factor authentication. In a PKI-style implementation, only one network peer would be required to authenticate the action – comparable to the up-chain key. For increased resiliency and fault tolerance, however, we recommend that the system architect choose multiple peers in the correct Boolean configuration to assure that the system retain its ability to maintain both positive and negative control.

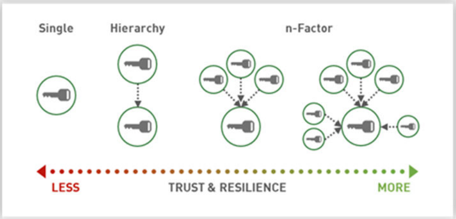
A) **Positive control** (that is, to assure that what you want to have happen, happens)
B) **Negative control** (that is, to assure that what you *don’t* want to have happens, does not)


CONTRACT AUTHORIZATION REQUEST
OWNER-DEFINED CONTRACT RULE
Majority(Device,Human,Group)
PRECISELY SCOPED NETWORK
Device
Human
Group
Were the contract rule conditions met?
YES
Perform Authorized Action
NO
Ignore Request

Concept: Verinym Contracts

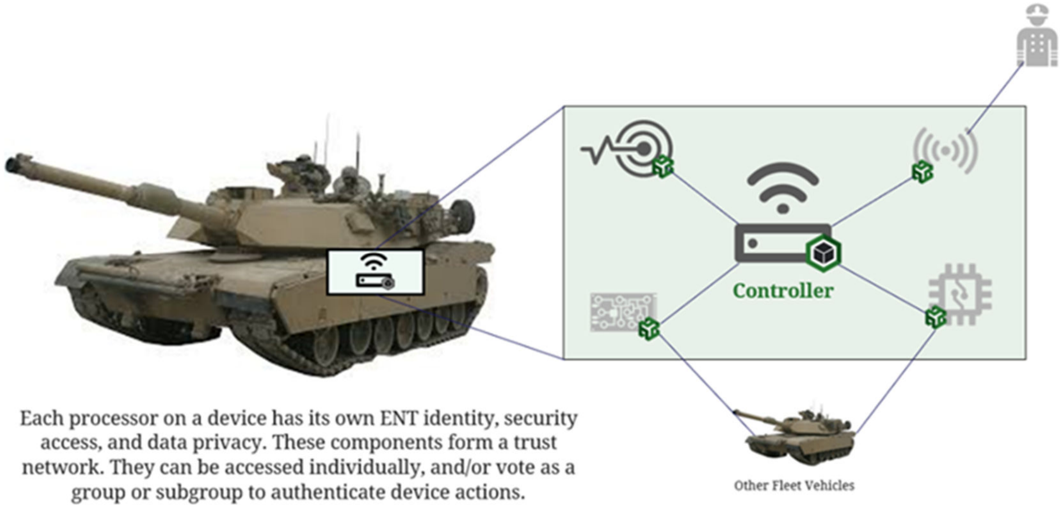
A contract is a Boolean statement in a verinym. It defines a discrete micro-network that performs a specific, authenticated network operation.

RKI methods allow the crypto key lifecycle to be defined locally by network peers.



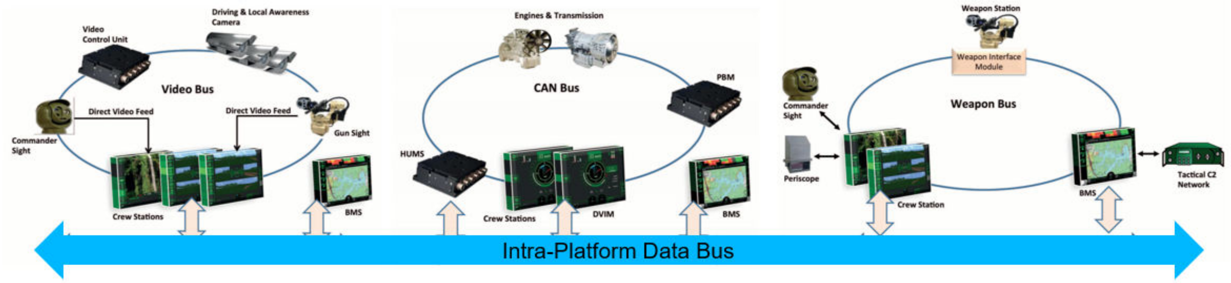
With RKI, trust & resilience scales exponentially – at the entity level, with no need for a third-party or gatekeeper.

Contracts can be used to help inure cyber-physical devices against cyber intrusion by creating an authorization circuit whereby components or sub-systems cross-authenticate each other. This prevents a spoofing attack which would allow access to the whole system and compromise of other subsystems. The vehicle can also then be authenticated as a whole to interact with extra-vehicle platforms.



Each processor on a device has its own ENT identity, security access, and data privacy. These components form a trust network. They can be accessed individually, and/or vote as a group or subgroup to authenticate device actions.

A topology should be chosen to maximize the trust and resiliency within the system, while minimizing the computational load. A correctly architected topology should achieve the goal of fully authenticating the systems and sharing session keys within a few seconds of bootup. Using the bilateral and unidirectional capabilities in ENT, a topology can be created where every subsystem is fully authenticated, but interactions between systems are limited only to precise data that needs to be exchanged, and all other messages are ignored.



Confidentiality (Encryption)

Data services in ENT can be used to exchange symmetric keying material for encryption. This allows each processor/controller to share current session keys for rapid encryption/decryption of data. Encryption can be used to obfuscate messages on the wire which helps mitigate certain types of attack vectors.

Data Integrity

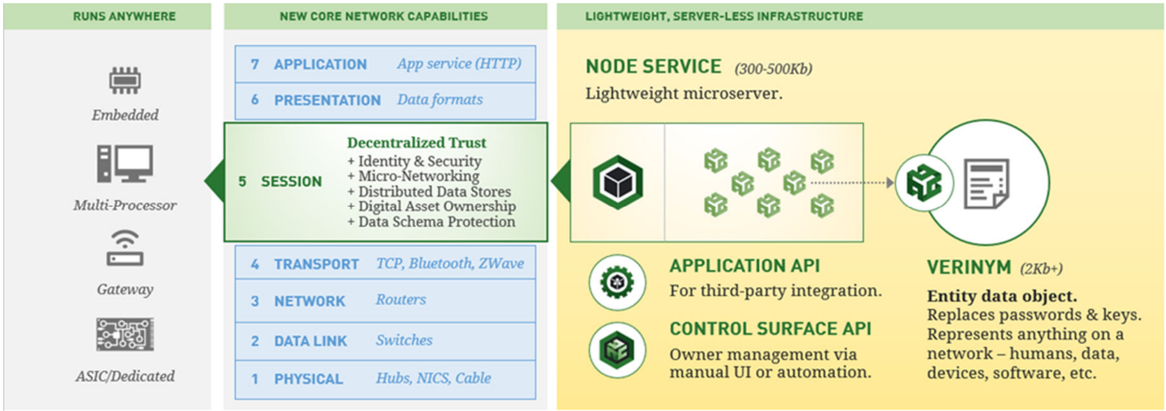
Along with managing the symmetric key, ENT can hash the data and send a message authentication code (MAC – the hash + the encryption key) to the receiving verinym peer which matches the incoming data with the MAC and decrypts.

Auditing and Non-Repudiation

ENT uses chain hashing for non-repudiation. The storage service can be used for auditing. A history of transactions is stored via the chain hash on the designated peer(s) for future auditing purposes.

Operation and Integration

ENT operates at the session layer (and lower) of the network stack, creating the opportunity to iterate infrastructure and communications forward quickly, and separately from the application and data layers, which themselves can then iterate quickly without concern for programming in the underlying infrastructure.


RUNS ANYWHERE
Embedded
Multi-Processor
Gateway
ASIC/Dedicated
NEW CORE NETWORK CAPABILITIES
7 APPLICATION App service (HTTP)
6 PRESENTATION Data formats
5 SESSION
Decentralized Trust
+ Identity & Security
+ Micro-Networking
+ Distributed Data Stores
+ Digital Asset Ownership
+ Data Schema Protection
4 TRANSPORT TCP, Bluetooth, ZWave
3 NETWORK Routers
2 DATA LINK Switches
1 PHYSICAL Hubs, NICS, Cable
LIGHTWEIGHT, SERVER-LESS INFRASTRUCTURE
NODE SERVICE (300-500Kb)
Lightweight microserver.
APPLICATION API
For third-party integration.
CONTROL SURFACE API
Owner management via manual UI or automation.
VERINYM (2Kb+)
Entity data object.
Replaces passwords & keys.
Represents anything on a network – humans, data, devices, software, etc.

ENT consists of 4 lightweight components:

1. Node Software: An "ENT Node" is an executable computer software program that executes within a multi-process-capable operating system such as Linux, BSD, Windows, etc. The node executes code that performs cryptographic, network and data operations. Network operations are managed at the session layer of the network, typically by opening multiple IP/port TCP channels to peer nodes and runs in parallel with other OS network services. This is very similar to other server protocols, such as HTTP, IMAP, etc. The node manages data objects, called "Verinyms" that represent logical actors such as personnel, devices, addressable data, and autonomous agents.

2. Verinyms™: Verinyms are data objects managed by an ENT Node and can loosely be compared to PKI certificates. Verinyms contain key information, whitelisted peers, service policies, relational maps (called contracts) and a single, optional access-controlled data payload. Verinyms are multi-capable logical actors, and represent identity for any unique identity within an ENT network – humans, data, devices, components, software, etc.

3. Application API. Allows data access to Node-hosted verinyms for third-party integration.

4. Control Surface API. Provides verinym management access for third-party integration.

ENT is inherently “edge-less” (that is, each verinym is at the center of its own network of peers), and “domain-less,” so it can also be used for extra-vehicle communication and cross-domain network transactions, with gateways to legacy systems if necessary. Using the directional aspect of contracts ensures that transactions only go in the direction intended, and the bilateral nature of the contracts plus the trustee service (ownership of the verinyms) ensures that each party remains in complete control of their own entities at all times. Because control of each verinym can be placed in its local context, it enables command and control to be pushed out into the tactical arena where appropriate, and to agilely iterate access policies in real time by highly trusted peers.

Benefits of the approach

- It does not interfere with data formats, protocols, or application layers, and it overlays the logical topology (does not determine it) so it is ideal for compliance with open and modular architectures.
- It does not add any additional hardware, so it does not preclude any future adoption of a different solution for authentication, should a better one be discovered.
- It has minimal SWaP-C impact, with a lifecycle cost an order of magnitude less than PKI solutions.
- It is extensible to extra-vehicle communications with ground systems, C2, infrastructure, etc.
- It is agile, so the topology can be changed in real time based on evolving needs, including authentication between joint forces or coalition partners (through a gateway, or if adopted, on the partner’s platform).
- It can be updated remotely with complete authentication and privacy, and it can be used to manage other remote or local authentic configuration updates as well, if desired.