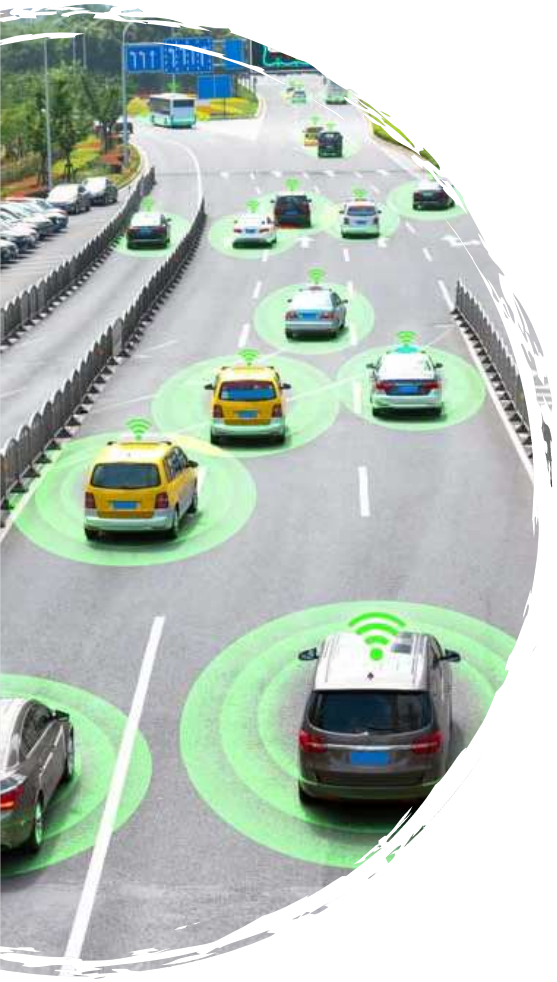
Security Conference

ETI - Zero Trust's Role in Enabling Network Visibility

Presented by: Scott W CADZOW

C3L

17th October 2023



Overview

A review of the ETI problem

What network visibility means

What Zero Trust means

The impact of ETI and ZT on system design

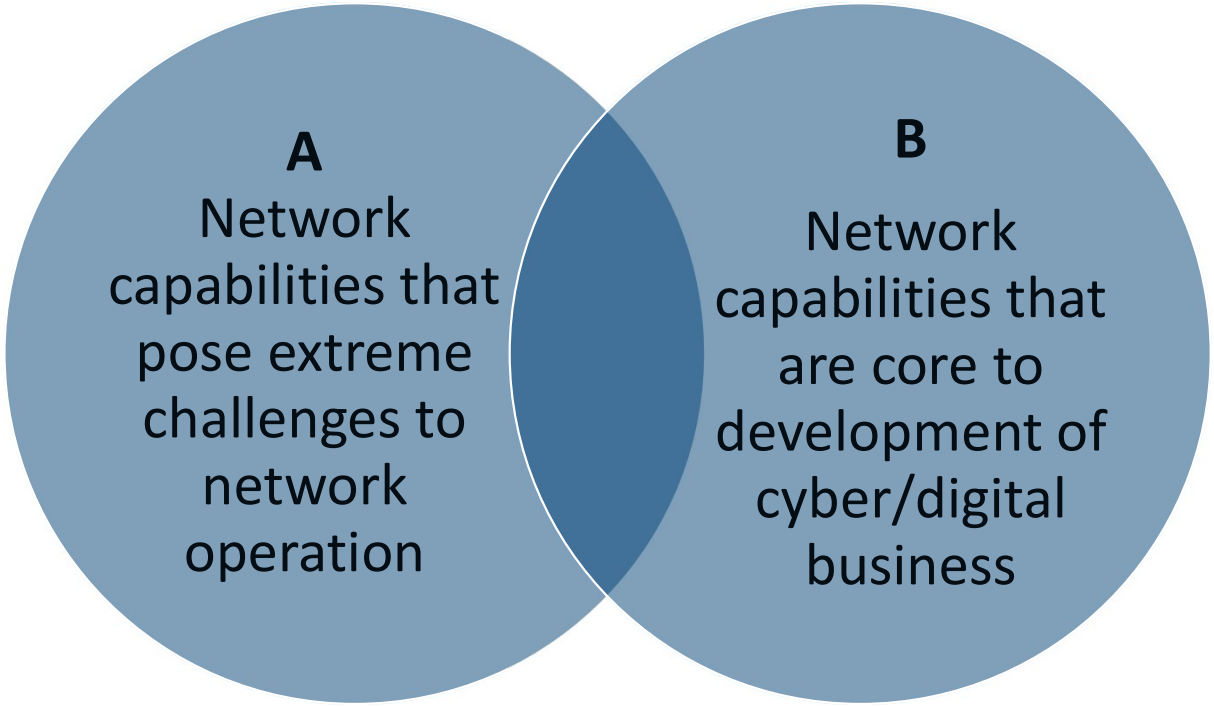
The impact on regulatory compliance

Some conclusions

A review of the ETI problem and network visibility

- Primarily the concern is to prevent the “going dark” problem
- The use of encryption has become the default approach to enhance the security of communications
  - Very often encryption is a synonym of anything using cryptography
- Encryption exposes users to threats from malicious traffic:
  - Traffic not recognized as a result of being hidden behind encryption can no longer be filtered out by the network operator to protect the end user.
  - End-to-end encryption can restrict the ability of network management, anti-fraud, cyber security, and regulatory monitoring systems to manage data and communications flowing into, through, and out of networks.
  - Encrypted traffic is masked from authorized inspection
  - Encryption of itself does not protect the end points from attack

The intersection of the two elements, A, representing network capabilities that, when content and headers are encrypted, pose extreme challenges to network operation, and B, representing Network capabilities that are core to development of cyber/digital business, should be minimized, whilst always seeking to eliminate A. In addition, the relative scale of B should always be significantly greater than A



Purpose of ETI’s work

ETI’s role is to enable reasonable **authorised** access to data, such as images, without ETSI making a value judgement on the content - ensuring the network operator is not complicit in transferring illegal content.

Assuring network operators that they have reasonable access to each protocol layer header to allow for network capabilities to be optimized

This is part of the many obligations under the Digital Markets Act, the Cyber Resilience Act, and many other regulatory or moral tools to ensure the protection of users of networks.

What does Zero Trust mean?

- Makes “security by default” an active choice
  - Making a session secure cannot be a passive thing
  - Why is element x in my system and what is it doing?
  - Verify every claim of every element in my system
  - If it’s not verified it is not trusted and the system is therefore not trusted
  - If there’s an active element in the system that has no verifiable function it should be removed
- Check and verify every aspect of every link, and its content, that has potential to be malicious

Terminology

Link is maybe too simple but is meant to encompass everything between Alice and Bob. So this must include content from one to the other, the identity of each, the timing of the link. The link established covers everything.

Trust is similarly both too simple and too abstract but is intended to convey the concern that when Alice trusts Bob, in a particular context (including time and location), that Alice is assured that Bob will do only and exactly what Alice has entrusted Bob to do. This means the link (as deep and wide as the context requires) between Alice and Bob has measurable assured trust.

What does Zero Trust mean?

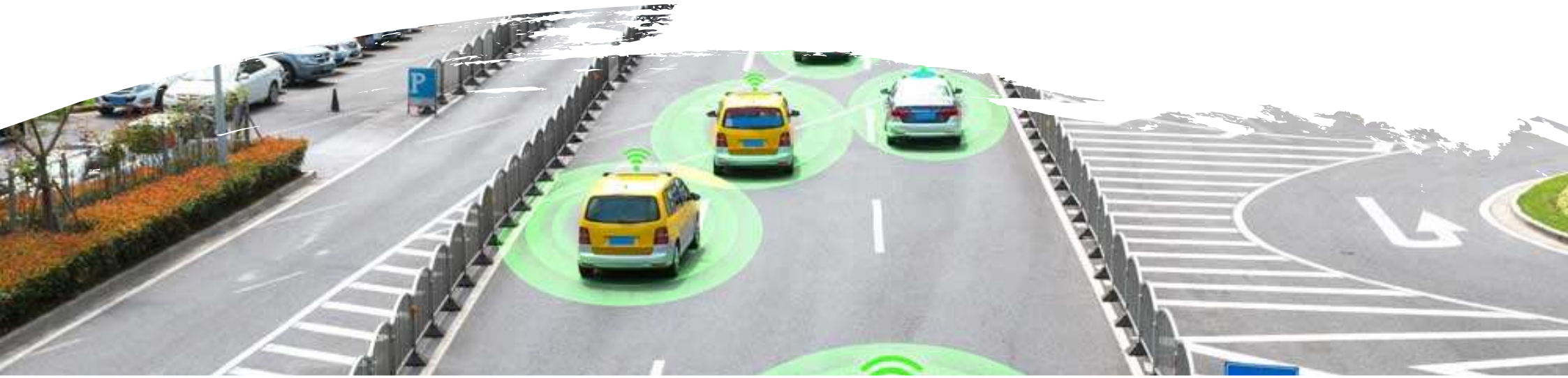
- Each link has a binary trust rule
  - Is it trusted? True or False
  - How is it trusted? That's the detail we'll look at later
- The system has a simple "AND" trust model
  - The logical ANDing of the trust of every link in the system (i.e. system trust requires that every link is trusted)
- The proofs of trust make the system security open (transparency requirement) and explicable (extended transparency)

ZTA - impact on system design

Requires every element to be able to identify and have a 3rd party attest to their function.

Requires that hardware roots of trust exist in every hardware element and that all software on top (that performs an identified function) is linked to it.

Requires that all software elements are validated at all times, assuring their conformance with their expected “normal” behaviour.



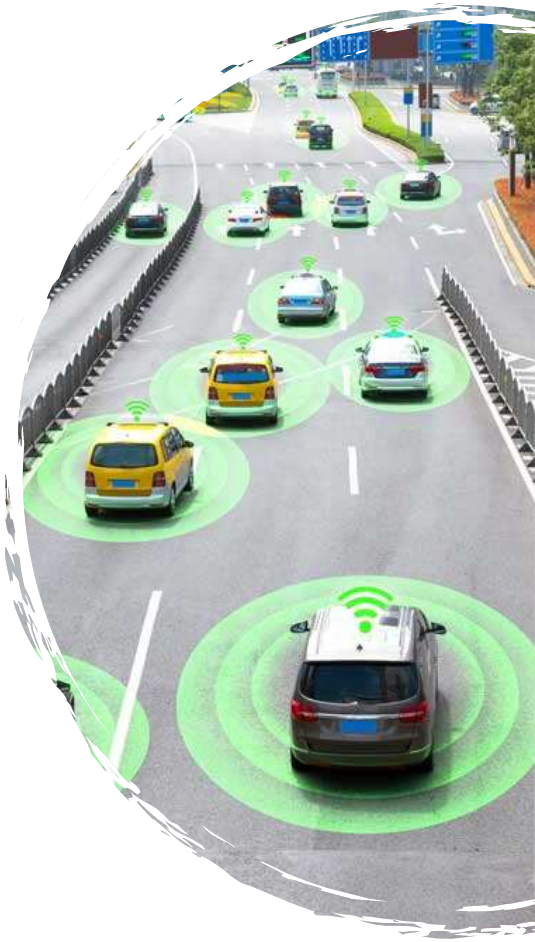
Impact on regulatory compliance

Networks are impacted by a lot of Cybersecurity regulation:

- Cyber security act (CSA)
- Cyber resilience act (CRA)
- Network and Information Security Directive 2 (NIS2)
- Radio Equipment Directive (RED)
- Etc.

Most of these regulations have a fairly simple security model → Prove any claim of security

- The rationale for ZTA is that every link at every layer has to prove it provides the required security association (by sequentially performing identification, authentication, keying, then action).
- The consequence is that proof to regulation is enabled both statically and dynamically (runtime)



To summarise

- ETI is looking at transparency and explicability
- ETI recognizes the need for encryption as a business and personal tool in the protection arsenal
- ETI also recognizes that to achieve transparency and explicability you need to trust everything in the connection
    - Hence ZT is key to ETI’s goals
- ZT’s required proofs of trust make the system security transparent and explicable

Thank you for your attention

Follow us on: