technica engineering

AUTOMOTIVE NETWORK SECURITY.

Myths Debunked.

Dr. Lars Völker

2020-09-17

TECHNICA ENGINEERING

AUTOMOTIVE NETWORK SECURITY MYTHS DEBUNKED

TABLE OF CONTENTS

INTRODUCTION

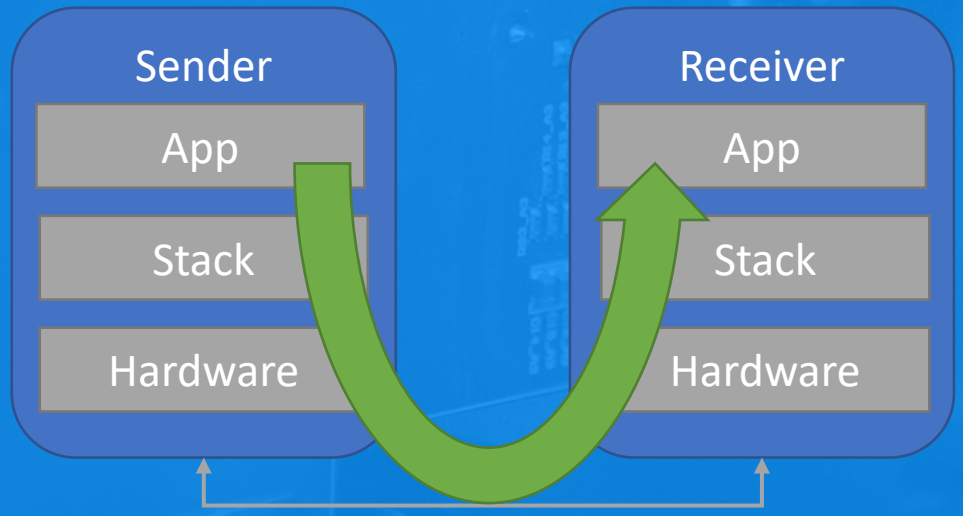
- Automotive and Security:
  - The Security use cases in the Automotive world was limited until vehicles got more connected and more complex.
  - Based on the limited Security use cases, the Security know-how was limited too.

- Security and Automotive:
  - The Automotive industry was somewhat unknown to Security researchers.
  - While the product is very interesting for attacks, most attacks seen so far are very limited by the limited understanding of the automotive technology and architectures. Even E2E CRCs stopped attacks in the past.

- This talk tries to narrow this gap by discussing some “myths” today.

MYTH #1: ONLY APP-TO-APP SECURITY IS SECURE

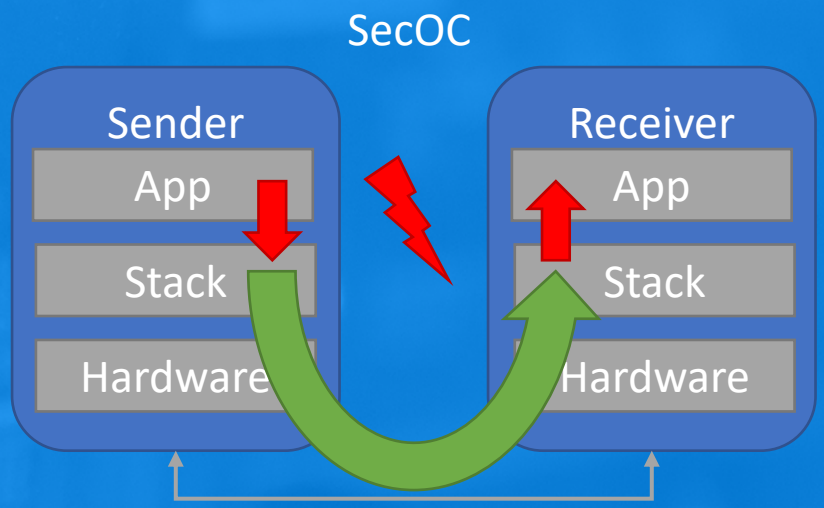
- Myth: Only security between applications (end-to-end Security) is secure.
- What is “end-to-end Security”?
  - Many actors in the automotive world seem to define this the same way as the end-to-end principle in safety solutions, like the E2E library. This tries to minimize the code outside the E2E solution.
  - Let's assume the security reaches from application to application.
- Which network security solution would offer such “app-to-app” security?



MYTH #1: ONLY APP-TO-APP SECURITY IS SECURE (2)

- Secure On-board Communication (SecOC) is an AUTOSAR-based application security ”extension”.

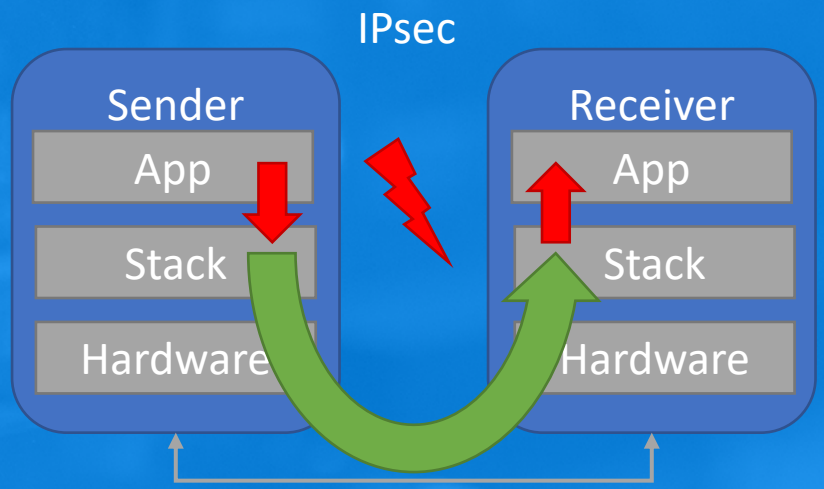
- Is SecOC app-to-app secure?
- SecOC is implemented inside the communication stack!
- No!



MYTH #1: ONLY APP-TO-APP SECURITY IS SECURE (3)

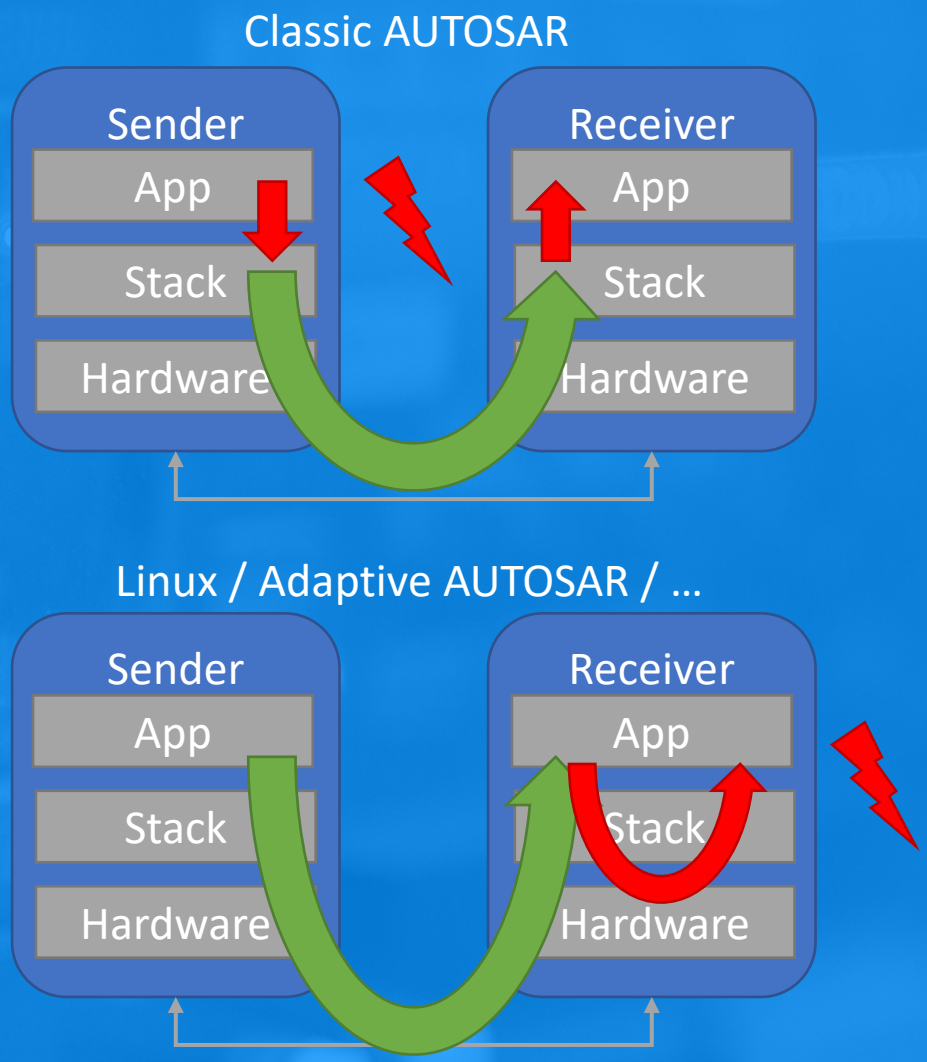
- IPsec is defined by the IETF in a series of RFC (RFC4301 et al). IPsec can protect all communication on top of IP and support two protocols (AH and ESP) in two modes (tunnel and transport).

- Is IPsec app-to-app secure?
- IPsec is implemented in the communication stack.
- No!



MYTH #1: ONLY APP-TO-APP SECURITY IS SECURE (4)

- What about TLS?
  - TLS can be linked to application in the “IT world”. So is TLS “app-to-app” secure?
- In Classic AUTOSAR? No, here TLS lives in the stack!
- On Linux, TLS can be linked to the App. But hardware acceleration for the cryptography or TLS itself is a shared resource!



MYTH #1: ONLY APP-TO-APP SECURITY IS SECURE (5)

- End-to-End Security meaning “application-to-application” security:
  - Cannot be achieved with standardized solutions (SecOC, IPsec, TLS, …)!
  - Cannot be achieved with shared resources like crypto acceleration!
  - Does not make sense on an embedded system without memory protection!

- What might make sense is “end-to-end” as no intermediate nodes.

- However, maybe the concept is not about the security solution but about the access control?

- Make sure that your “end to end security” definition makes sense!

MYTH #2: ACCESS CONTROL INSIDE APPLICATIONS

- Myth: “Access control only works, if the security ends in the application”.

- The fundamental idea is that you cannot trust the information of the layers below because everything can be spoofed (IPs, Ports, …).
  - On the Internet, this is probably true.
  - Your browser is an application and how much does it want to trust the OS?
  - When the user is needed to check (expired) certificates, you probably want to limit to just a service.

- But is this true for in-vehicle networks?

MYTH #2: ACCESS CONTROL INSIDE APPLICATIONS (2)

- The situation of in-vehicle networks is quite different!
  - Inside the vehicle, the OEM can control most parts and is not limited as before.
  - It is possible to limit communication in the network (e.g. by VLANs).
  - It is possible to ensure that the IPs and Ports cannot be spoofed.

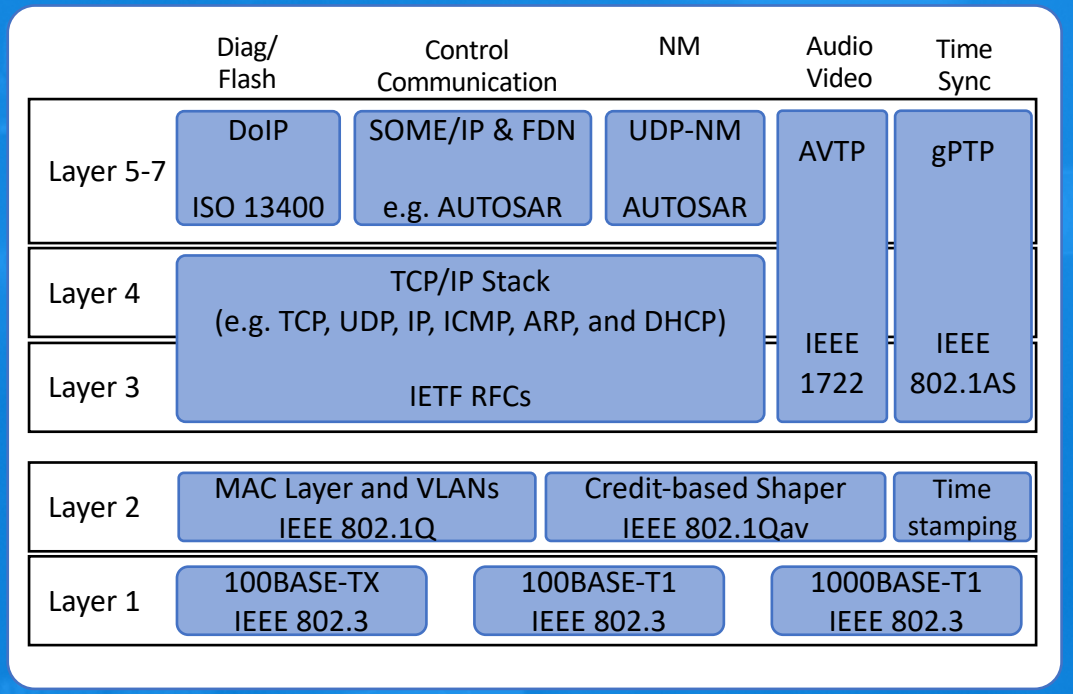
- Example: Using hop-by-hop MACsec combined with strong filtering on Ethernet Switches:
  - You can enforce VLANs and IPs.
  - This allows effective firewall on hosts (and in the network).
  - This allows to implement strong ACLs at many places!

- Access Control can be distributed, if your holistic Network Security Design works!

MYTH #3: EVERY PROTOCOL NEEDS SECURITY

- Myth: Every protocol needs security build in!
- Do you need it in e.g. ARP too?
- Only on the application layer?
- For DoIP it seems to make sense since it reaches outside the car.
- What about Network Management?

- We need a different point of view.



MYTH #3: EVERY PROTOCOL NEEDS SECURITY (2)

- Lets first check the attacker model!
- External attackers can modify traffic on links and replace ECUs. Which protocols they can attack depends on the Network Security you run. MACsec can protect all protocols above!
- Internal attackers can try to use ”services” not allowed. This can be easily stopped by Access Control! They do not have to be “inside” the protocol.

- What is true: “For every relevant protocol, ACLs and/or Filtering needs to be supported” (but not necessary inside it).

- Make sure you have enough Access Control and Filtering!

MYTH #4: IDS/IPS ARE MOST IMPORTANT

- Myth: IDS/IPS are the most important Security features!
- Detecting Intrusions can be valuable for …
  - …understanding what attacks happen.
  - …making sure that large scale attacks can be stopped fast.

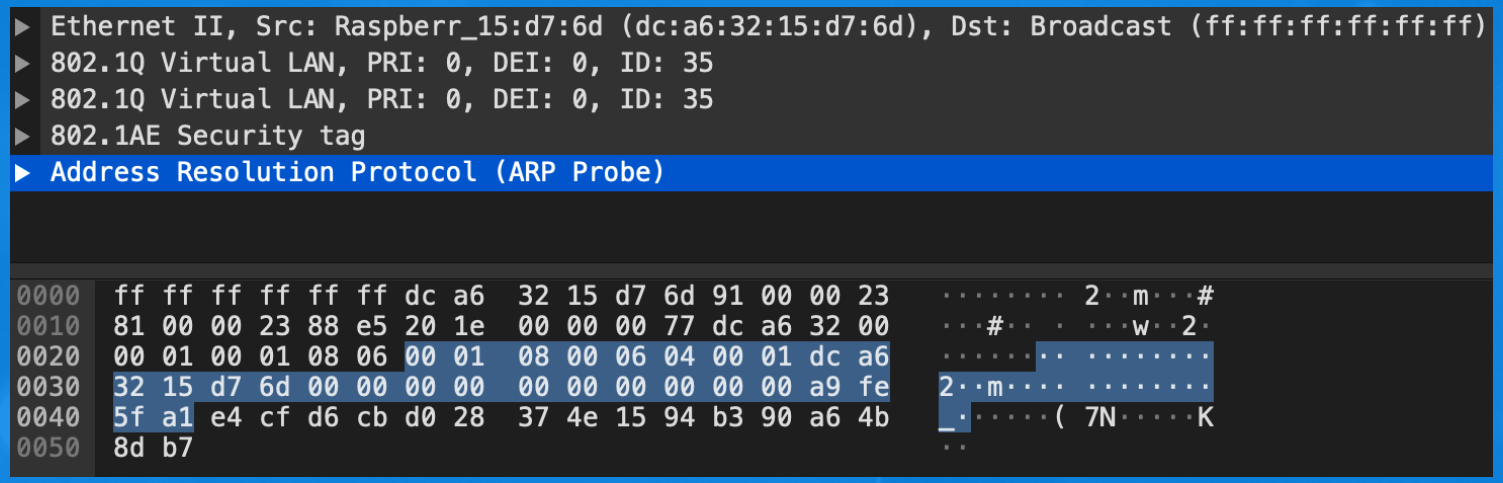
- However: IDS and IPS currently seem to be the security features with the biggest marketing budgets but limited technical depth.
- Start with creating the path to transport “events” from vehicles to your backend. Then incrementally add “events”. Look at your data.
- Intrusion Prevent System (IPS) try to **actively** stop attacks. Do you want this in Autonomous Vehicles go crazy?

- IDS is only one tool in your security toolbox! Create a strategy for it!

MYTH #5: SECURITY DOES NOT ALLOW TESTING!

- Myth: When introducing Network Security solutions you cannot test anymore because all traffic is encrypted, and you cannot read it.

- SecOC is authentication only (no encryption!) and IPsec, TLS, and MACsec support Authentication only.



Our auth-only MACsec patch for Wireshark will be part of Wireshark 3.4.

MYTH #5: SECURITY DOES NOT ALLOW TESTING! (2)

- But authentication only Network Security does not let me change messages anymore!

- To allow changing messages, two main approaches exist:
  - Add a secure process to turn Security on and off.
  - Add a secure process to share keys between test system and ECU.

- Bonus: Bugs in the code, lower security. Security requires to test!

- Network Security allows testing! Know your tool chains and design your process!

MYTH #6: WITH SECURITY, NO AGILE DEVELOPMENT

- For Security, you analyze the requirements in order to identify the needed Security mechanisms to add. This does not work, since adding Security takes time.

- Solution: Speed up your process by doing the opposite!
  - Always design in generic Security mechanisms (e.g. protect all traffic).
  - Check with new features/applications, if the generic security is enough.
  - Analyze Security to confirm that you have enough Security!
  - Stop discussions like “is this security mechanism really needed” since you cannot know the answer yet!

- Understand that Security is an enabler for features. Don’t minimize it!

SUMMARY

- Security in Automotive is new and the unknown may be misunderstood. For many IT Security experts, Automotive is new and unknown too.

- This talk discussed some common myths of Automotive Security:
  1. Only Security between Applications is really secure!
  2. Access Controls needs to be inside applications!
  3. Every Protocol needs Security!
  4. IDS/IPS are the most important in Security!
  5. Security does not allow Testing!
  6. With Security, No Agile Development!

- Teach Security to Automotive engineers and vice versa.

STAY CONNECTED

Dr. Lars Völker
Technical Fellow
Lars.Voelker@technica-engineering.de
+49 (0) 175 1140982

Technica Engineering GmbH / Leopoldstraße 236 / 80807 Munich / Germany