Building Automotive Cybersecurity From the Inside Out

Chuck Brokish
Director, Automotive Business Development
Green Hills Software
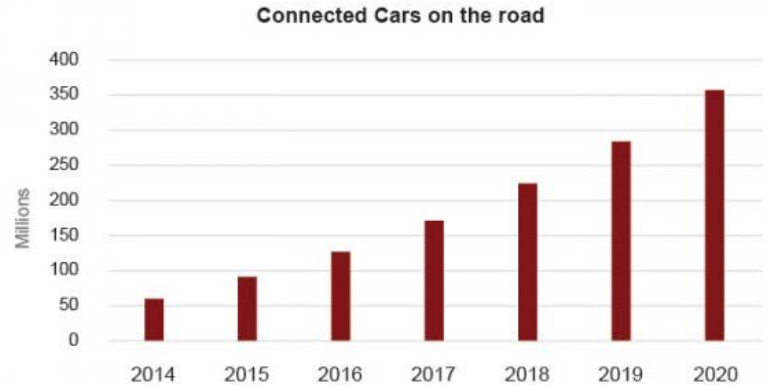
Future Networked Cars

March 8, 2018

Why is security priority #1?

- Because the software in these cars is replicated
- They all have the same flaws
- Across hundreds of thousands or millions of units
- A single exploit can simultaneously impact ALL of those units

➔ Mass Production = Mass Destruction

Connected Cars on the road

© Copyright GroupM Next

Safety vs. Security:
Book-ends to a robust system
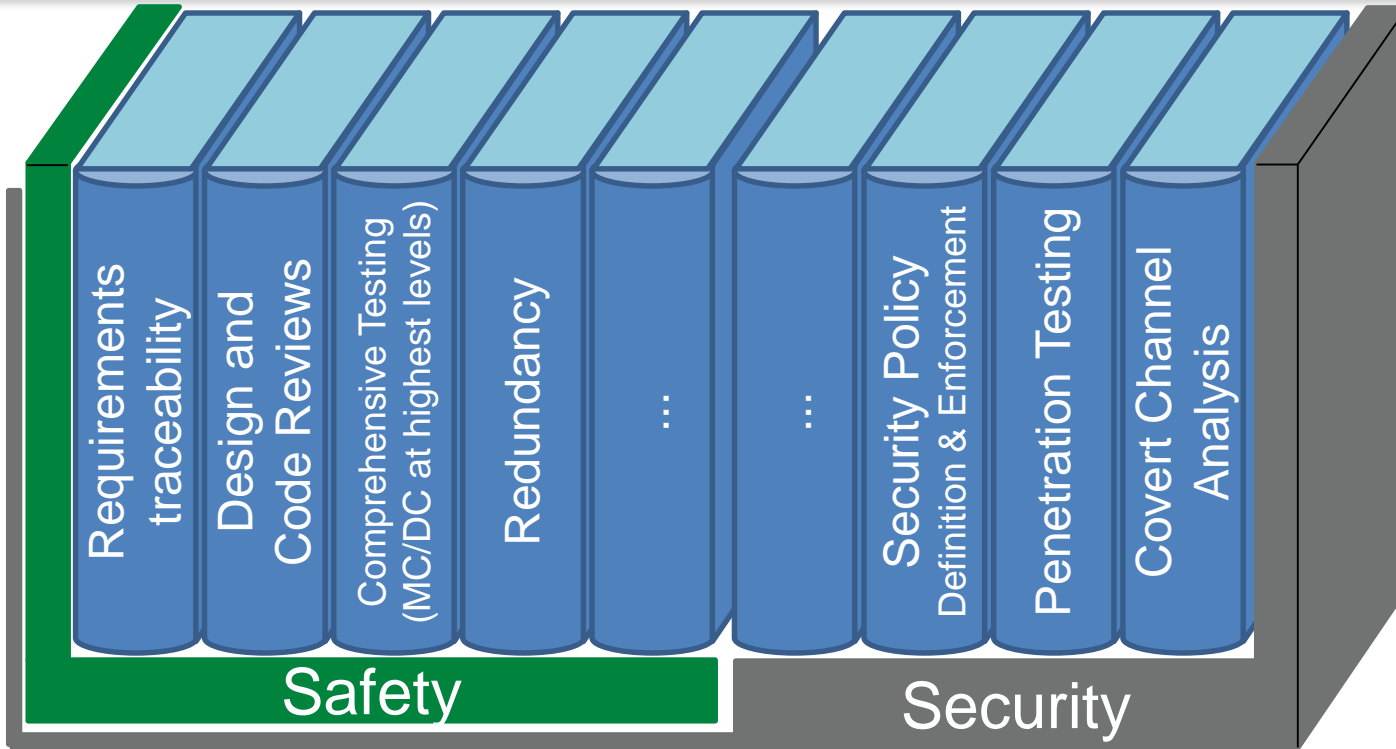
Safety
- The system behaves according to the requirements in all cases. *(It does what it is supposed to do.)*

Security
- The system behaves according to the requirements in all cases **and** does nothing else. *(It does not do anything it is not supposed to do.)*

Books (left to right):
- Requirements traceability
- Design and Code Reviews
- Comprehensive Testing (MC/DC at highest levels)
- Redundancy
- ...
- ...
- Security Policy Definition & Enforcement
- Penetration Testing
- Covert Channel Analysis

Safety | **Security**

Inside Out Security

- ❑ Many security architects approach the problem of securing a system from the outside looking in
  - ▪ Look for entry points into the system
  - ▪ Establish a perimeter
  - ▪ Layer additional defense strategies in case the outer layers are defeated
- ❑ Inside out security starts by identifying the critical components in the design and isolating those components from non-critical components
  - ▪ Assume that non-critical components will be compromised
  - ▪ Utilize strong separation principles
    - • Hardware separation
    - • High robustness software separation
  - ▪ Minimize Complexity

Common Criteria Security Definitions

- ❑ High Robustness specification
  - ▪ Protecting "classified and other high-valued information"
  - ▪ Against "sophisticated threat agents"

- ❑ Medium Robustness specification
  - ▪ "assumed non-hostile and well managed user community"
  - ▪ Requiring protection against…"inadvertent or casual attempts to breach the system security"
  - ▪ "not intended to provide protection against determined attempts by hostile and well funded attackers"