A Model-Driven Methodology for Automotive Cybersecurity Test Case Generation

SRCNAS/STRIVE WS @ IEEE EURO S&P' 21
September 6, 2021

Stefan Marksteiner, Peter Priller
The Need for Industrialized Automotive Cybersecurity Testing

- **UNECE**
  - Regulation R.155
  - Mandates cybersecurity and cybersecurity management
  - Requires testing of measures
  - Adopted in EU, Japan and Korea
  - Effective in EU for new types 2022 and for all new vehicles 2024

- **ISO/SAE 21434**
  - Cyber security management system for automotive systems
  - Risk-based approach
  - Also demands testing, however, does not specify details
  - To be supplemented for testing by ISO PWI 8477 (V&V) and ISO/SAE PWI 8475 (CAL &TAF)

=> Need for automated testing
Why Black Box Testing?

- Providing an attacker’s view
- Long supply chain – source might not be available
- Unwillingness (or inability) to disclose internals
Cyber Testing Manually

Tedious and Costly
Holistic Testing

- System level
- Including architecture
- Conducted on the communications networks inside an actual system
System Reconnaissance

- Use a variety of interfaces
  - Wireless UIs (WiFi, BlueTooth,..)
  - Wired UIs (USB,)
  - Diagnostic (OBD)
  - Wiretapping (CAN, LIN)
- Active (sending messages)
- Passive (listening only)

- More complete picture of the SUT
- Ability to segment attacks
Fingerprinting

- **Passively:**
  - Deviation
  - Kurtosis
  - Clock skew
  - ...

- **Actively:**
  - Sending (CAN) messages
    - Well formatted
    - Malformed

- Attribute a component according to the detecting interface
Model Generation

- Use (abstract) automata learning to learn a *behavioral* model
- Use model checking for test case generation
Variant Management

- Without a priori knowledge, a plethora of candidate models is available
- This set is narrowed down with every piece of information
- Each test case touches a number of assumed components, allowing for gathering data for fingerprinting
- Test cases will not only be chosen according to a potential attack vector, but also considering pivot elements to exclude or verify an optimal number of candidate models
Attack Model

- Augmenting the system model with attack information
  - Using CVE information
  - Using other public sources (Auto-ISAC, research, darknet)
  - Analysis - see previous presentation of this workshop ;)
- Should occur both component and function-wise
Attack Tree

- Assign cost to attacks on a specific component
- Shortest path (per cost) => most feasible attack
- Shortest path will be tested first, in conjunction with variant management considerations
- Test pass if the cost of the shortest path is above a certain threshold => sufficiently secure
Conclusion

- Concept for holistic zero-knowledge testing of automotive systems
- Combining fingerprinting and attack trees for test case generation
- Coping with variants that result from fuzziness
Thank you for your attention!

Thanks!

Stefan Marksteiner¹, Peter Priller²

¹ Senior Technology Scout Cyber Security, AVL List Gmbh, stefan.marksteiner@avl.com
² Principal Technology Scout Embedded Systems, AVL List Gmbh, peter.priller@avl.com

This research has received funding from the program “ICT of the Future” of the Austrian Research Promotion Agency (FFG) and the Austrian Ministry for Transport, Innovation and Technology under grant agreement No. 867558 (project TRUSTED) and within the the ECSEL Joint Undertaking (JU) under grant agreement No. 876038 (project InSecTT). The JU receives support from the European Union’s Horizon 2020 research and innovation programme and Austria, Sweden, Spain, Italy, France, Portugal, Ireland, Finland, Slovenia, Poland, Netherlands, Turkey. The document reflects the author’s view only and the Commission is not responsible for any use that may be made of the information it contains.