NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
SYSTEMS ENGINEERING (SE) MINI-SYMPOSIUM
AUGUST 21-22, 2013 - TROY, MICHIGAN

Cyber Security: An Evolving Systems Engineering Requirement

Mike Ridge
Center for Advanced Vehicle Environments (CAVE)
Battelle Cyber Innovation Unit
430 National Business Pkwy, Suite 350
ANNAPOLIS JUNCTION, MD 20701

Forrest Shull
Division Director
Fraunhofer Center for Experimental Software Engineering
5825 University Research Court, Suite 1300
College Park, Maryland 20740-3823

Abstract

Increased connectivity, burgeoning functionality, as well as surging software and integration complexity all conspire to blur the lines for requirements sourcing and implementation of new Ground Vehicles.

Introduction

The addition of computer controls and external network access to ground vehicles has added to the systems engineering burden in vehicle design cycles. Information Assurance requirements that previously never applied to these platforms are now a significant complication. This fact is complicated even further by the addition of sensor and mission packages to the vehicles.

The importance of cybersecurity controls in ground vehicles has sometimes been downplayed, on the assumption that attackers would have to physically connect to the in-vehicle computer network. If this is the case, then many simpler, non-computerized attacks become of greater concern. However, researchers have recently shown that, in the commercial automotive domain, attack vectors exist which allow malicious inputs to be delivered to the in-vehicle networks via indirect physical access, short-range wireless access, and long-range wireless access. Moreover, in analyzing the utility of such attack vectors to attackers, researchers have also shown that these vectors can allow control of in-vehicle systems as well as the exfiltration of sensitive information about the vehicle itself and its occupants[1].

What are the Basic Issues?

Connectivity and CANBUS

Since 1996 the common method to access the computers in cars has been the OBD II connector, typically located under the dash. It was initially a requirement for diagnostics and emissions testing. This access allowed a healthy market for consumer products that could connect via this port and provide access to the

[1] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. 2011. Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX conference on Security (SEC'11). USENIX Association, Berkeley, CA, USA, 6-6.

computers in the automobile. Even insurance companies have used this port to monitor risk behavior and reduce premiums where appropriate. The network(s) this connector interfaces with typically runs the CANBUS protocol, a resilient, real-time control network operating over twisted pair cabling. Wireless connectivity being added to vehicles changes the risk environment as one no longer needs physical access to the vehicle to potentially expose the CANBUS networks.[2] Even the insurance telematics unit designed to evaluate risk exposes a new attack surface.

Increased Functionality

Software/Firmware update capability and third party application support in the vehicle systems all increase the attack surfaces. And many cars support multiple methods to link your phone and personal computer to the vehicle (all of which introduce their own security issues). Personal information is also now stored on vehicles, be it GPS data, contact lists, calling information, browser history, and even black boxes which can distinguish which key was used. Increased automation will also be impacted by risks exposed to the sensors that enable it.[3]

Software Complexity

Auto manufacturers integrate and assemble components from component manufacturers. These component manufacturers supply a product compliant to the specifications provided, meanwhile time is ticking and late functionality (required to meet market surveys) is added. The software complexity of the resultant product is tested and regression tested.[4] But the days of testing all paths through integrated software are fleeting.

OK…let's pretend I agree, but, why should TARDEC care?

1. ***The re-application risk is already large and is growing.***
   Today, these are the same component pieces that are re-used in Military vehicles, who are adding their own wireless connectivity. Electronic Control Units (ECUs) developed for the commercial markets typically use algorithms that require they be kept secret to be secure, as opposed to implementing a real key management system.[5] This is something that both DIACAP and FISMA Certification and Accreditation (C&A) systems would not allow. C&A would also require authentication and perhaps confidentiality on the CANBUS

[2] Carjacking goes digital, 'white hat' hackers demonstrate, Jim Finkle, Reuters 7/29/2013 http://www.nbcnews.com/technology/software-experts-attack-cars-release-code-hackers-meet-6C10773444

[3] Texas students fake GPS signals and take control of an $80 million yacht, Eric Berger, Monday, July 29, 2013 http://blog.chron.com/sciguy/2013/07/texas-students-fake-gps-signals-and-take-control-of-an-80-million-yacht/?cmpid=hpfc

[4] This Car Runs on Code, IEEE Spectrum, By Robert N. Charette, February 2009 http://m.spectrum.ieee.org/green-tech/advanced-cars/this-car-runs-on-code/0

[5] Scientist banned from revealing codes used to start luxury cars Lisa O'Carrol, the Guardian, 26 July 2013 http://www.theguardian.com/technology/2013/jul/26/scientist-banned-revealing-codes-cars

networks, depending upon architectural exposure.

2. ***Current Commercial Products need augmentation/changes to re-use, but are also changing naturally due to market forces.***
   Using the Joint Light Tactical Vehicle (JLTV) CONOP[6], the reuse of commercial stability control and braking system components will certain help build a better JLTV but also insert an attack vector via supply chain and network access. Also the easiest way to support the requirement for Common Operating Picture and situational awareness means integrating vehicle systems into the requisite DoD network to supply GPS positioning, fuel state and other vehicle status items. Integrated sustainability features like those for commercial products could substantially impact required maintenance time – but it too becomes an attack surface, something already believed to have happened in the aviation community.[7]
3. ***A DoD Certification process requires the use of NSA[8] and FIPS[9] approved cryptography (where appropriate).***
   Implementations of either are not available in the automotive market today. Meaning the complete cost of development/upgrade/sustainment will be borne by DoD.

OK… I am an OEM – why should I care?

1. Most commercial Original Equipment Manufacturer (OEM) crypto implementations ignore Kerckhoff's Principle[10] (which reminds us that one should design systems on the assumption that the enemy will become familiar with them) and use security though obscurity principles. In a world of closed/isolated networks, this can work, but the world is changing and is no longer adequate to even protect underlying intellectual property, let alone more malicious activity. Change is necessary.
2. DoD is not the only market that will demand this as markets for local, state and federal governments are starting to see these issues too. And let's not forget foreign sales.
3. Insurance companies could reasonably adjust rates based upon the ability of a manufacturer to resist (or not) remote attacks, as these attacks could affect both vehicle safety and theft.

[6] Joint Light Tactical Vehicle (JLTV) Concept of Operations CDD v3.6, 6 Jan 2012, https://contracting.tacom.army.mil/majorsys/jltv_emd/JLTV%20CONOPS%20v3.6.pdf

[7] Schneier on Security, August 23, 2010 http://www.schneier.com/blog/archives/2010/08malware_contrib.html

[8] NSA: Suite B Cryptography / Cryptographic Interoperability http://www.nsa.gov/ia/programs/suiteb_cryptography/

[9] FIPS: Cryptographic Module Validation Program (CMVP) http://csrc.nist.gov/groups/STM/cmvp/

[10] http://en.wikipedia.org/wiki/Kerckhoffs%27s_principle

OK – I'm listening – what can we do?

The field of system engineering security is a complex one, but we focus on a few important take-aways for "building security in" to systems:

1. System engineers need to recognize the dynamic nature of the issue, and that to resolve these concerns for all involved requires development of secure architectures, as well as Integrated Development Processes (Tier 1 through lifecycle support).
2. Mechanisms need to be developed for monitoring and enforcing secure system management, anomaly detection and control, including system key management.
3. Systematic development processes need to be deployed that include security considerations in design reviews (as is currently done for system safety).

Certainly, more research and practical experience is required to improve our understanding of secure systems development. Equally clearly, important best practices in this domain include:

- The need to identify key SMEs who should participate in early-lifecycle design reviews. There is currently no substitute for human judgment and expertise regarding risks and attack vectors. Nevertheless, just having the appropriate experience brought to bear in a review is insufficient; important analysis has to happen upfront regarding questions of where in the system (on which components / subsystems) those reviews should be focused; what are the most important issues to focus on; how to ensure that the experts provide sufficient coverage of the important issues. Some work on this has already begun for software-intensive systems but more work is needed to focus on systems security issues specifically[11, 12].
- Given the status of the systems engineering discipline, it is not possible to demonstrate in the early lifecycle stages whether or not the final system will be secure. But numerous hints abound in those early stages that can indicate when the final system *can't* achieve a desired level of security. These issues should be monitored and when anomalies are detected, a deep dive into the data followed by potential corrective action should follow. Early warning indicators can be relatively easy to measure; the important thing is whether they trigger a deeper analysis that can be more revealing. Examples may include whether specific requirements for security exist at all; whether the number of security-related requirements make sense for the size and complexity of the system; whether

[11] Shull., F., Feldmann, R., Seaman, C., Regardie, M., and Godfrey, S., "Fully Employing Software Inspections Data," Innovations in Systems and Software Engineering - a NASA Journal, 2010.

[12] NASA Technical Standard NASA-STD-8739.9, "Software Formal Inspections Standard."

those requirements can be traced to elements of the system design; etc.[13]

- There is a need to share information about the types of attacks that do happen and learn from them. The issues of most potential concern (and that reflect any important attacks that have already happened) should not be left to the experience of the individual SMEs and reviewers to know about; rather, such issues should be compiled, managed, and should feed into any V&V techniques applied to the system[14]. Since security in general is such a dynamic topic, periodic updates are necessary to ensure that the issues at the top of the list continue to be the ones of most concern and the focus of the resources spent on V&V. Moreover, there needs to be a direct connection between such lists and the quality-checking activities that are applied.

REFERENCES:

Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. 2011. Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX conference on Security (SEC'11). USENIX Association, Berkeley, CA, USA, 6-6.

Joint Light Tactical Vehicle (JLTV) Concept of Operations CDD v3.6, 6 Jan 2012, https://contracting.tacom.army.mil/majorsys/jltv_emd/JLTV%20CONOPS%20v3.6.pdf

Scientist banned from revealing codes used to start luxury cars
Lisa O'Carrol, the Guardian, 26 July 2013
http://www.theguardian.com/technology/2013/jul/26/scientist-banned-revealing-codes-cars

Carjacking goes digital, 'white hat' hackers demonstrate
Jim Finkle, Reuters 7/29/2013
http://www.nbcnews.com/technology/software-experts-attack-cars-release-code-hackers-meet-6C10773444

NSA: Suite B Cryptography / Cryptographic Interoperability
http://www.nsa.gov/ia/programs/suiteb_cryptography/

FIPS: Cryptographic Module Validation Program (CMVP)
http://csrc.nist.gov/groups/STM/cmvp/

This Car Runs on Code, IEEE Spectrum, By Robert N. Charette, February 2009
http://m.spectrum.ieee.org/green-tech/advanced-cars/this-car-runs-on-code/0

Texas students fake GPS signals and take control of an $80 million yacht, Eric Berger, Monday, July 29, 2013
http://blog.chron.com/sciguy/2013/07/texas-students-fake-gps-signals-and-take-control-of-an-80-million-yacht/?cmpid=hpfc

Schneier on Security, August 23, 2010
http://www.schneier.com/blog/archives/2010/08malware_contrib.html

[13] L. Layman, V. R. Basili, M. V. Zelkowitz, A Methodology for Exposing Risk in Achieving Emergent System Properties, Fraunhofer Center for Experimental Software Engineering Technical Report 11-101.
http://www.fc-md.umd.edu/sites/default/files/Publications/ReportsAndPresentations/PRi%20Methodology.pdf

[14] http://bsimm.com/online/intelligence/am/