2016 guide for automotive software development
Mark these words: at the beginning of 2016, journalists will say that the top overall automotive story for 2015 was cybersecurity. Each month, there was a new vulnerability, report, patch update, or demonstration of just how insecure our connected cars are. From in-vehicle infotainment system hacks to penetration through wireless vehicle services, the number of potential attack vectors grew with every new vehicle model, with drivers caught in the web. Yet the investment into improving cybersecurity at a fundamental level — the software itself — paled in comparison. **It’s not hard to figure out the reasons why.**

According to a Ponemon Institute survey of cross-tier automotive developers, 50 percent of the respondents answered that they’re either unsure or disagree with this statement: *Automotive software development teams have the skills necessary to combat software security threats.*

That’s a staggering number, considering that these same teams are delivering systems that monitor, control, and protect all aspects of our vehicles. Further answers highlight the disconnect between the potential risks and the chosen investments, with over 50 percent of developers not convinced that their company makes secure software development a priority or convinced that they have the enabling technologies to support it.

At this point, it’s clear that everyone from the manufacturer to the driver wants secure software but can’t define a roadmap to success. The answer lies in targeting the one point in the entire development process that has the single biggest impact on all aspects of code and the above survey results have already revealed the answer: the developer.

---

50% of developers are unsure or disagree with this statement: 

*Automotive software development teams have the skills necessary to combat software security threats.*
WATCH FOR SIGNS OF RISKS

AUTOMOTIVE NEWS

LAWMAKERS WORRY MALICIOUS HACKERS COULD TAKE CONTROL OF YOUR CAR

FIAT CHRYSLER U.S. TO RECALL VEHICLES TO PREVENT HACKING

YOUR BMW OR BENZ COULD ALSO BE VULNERABLE TO THAT GM ONSTAR HACK

PROGRESSIVE INSURANCE DONGLE HACKED

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY - WITH ME IN IT

AUTOMOTIVE NEWS
VEHICLE ATTACK SURFACES

- Airbag Control Unit
- Instrument Cluster/Telematics
- Transmission Control Unit
- Engine Control Unit
- Anti-Lock Braking System
- Tire Pressure Monitor
- Keyless Entry/Anti-Theft
- Dynamic Stability Control
- Vehicle-to-Vehicle Communications
LOOK AT THE DATA YOU’RE ALREADY FACED WITH

1000s OF BUGS

Security vulnerabilities

CUSTOMER DEFECTS

SAFETY REQUIREMENTS

NOW LOOK AT WHAT THEY’RE SAYING

Only 41% say secure software is a priority at their organization*

51% consider security an add-on feature*

1 in 5 vehicles will have some form of wireless network connection by 2020**

90% think it is difficult to secure automotive applications*

* 2015 Ponemon survey of automakers and suppliers

** Gartner report “Predicts 2015: The Internet of Things”
All of the supply chain needs to be secure, not just your code but the code of the packages included in your software.

Follow a well-known security standard applicable to your domain.

Educate the development team, provide security based training.

Automate security and functional safety testing.
Bringing the benefits of automated testing into the modern development world of continuous integration and Agile methodologies has proven to be effective for many organizations, allowing them to deliver more robust features at a faster pace. These strategies put the burden of common or complex development tasks onto tools that perform in the context of frequent check-ins and builds.
**THE ROAD AHEAD**

**NEED TO KEEP UP WITH DEVELOPMENT VELOCITY**
Rapid feedback required

**PARING DOWN VULNERABILITY RATES**
Include testing and security requirements in functional user stories

**DELIVER MORE ROBUST FEATURES AT A FASTER PACE**
Have specific acceptance criteria in the definition of done

- **43%** of automakers have Agile as part of their culture**

If only **50%** of software vulnerabilities were removed prior to production, costs would be reduced by **75%***

---

*Gartner report “Now is the time for security at the application level”

**Agile in Automotive – State of Practice 2015, Kugler Maag Cie**
HOW CAN TESTING WITH **STATIC CODE ANALYSIS** HELP?

- **CORRECT**
  - CODE BEFORE CHECK-IN
- **CHECK**
  - STANDARDS COMPLIANCE
- **ANALYZE**
  - ON INCREMENTAL BUILDS
- **CREATE**
  - CUSTOM CHECKERS
- **IDENTIFY**
  - ISSUES ON THE FLY
- **INTEGRATE**
  - INTO CI TOOLS

See how SCA works - request a free trial.

WATCH this webinar on how to navigate your way to Agile automotive software development.
DISCOVERING THE **TOP 2015 AUTOMOTIVE SECURITY VULNERABILITIES**

- Access control
- Memory buffer problems
- Information exposure
- Cryptographic issues
- Improper access control
- Code
- Numeric errors
- Resource management errors
- Improper input validation
- Code injection

Watch Andy Gryc and Jeff Hidreth countdown the **top 10** vulnerabilities.

Dive in with a **deeper analysis** of each vulnerability.
The cornerstone of embedded development is software, and software is where most errors are introduced. Not only has the volume of delivered automotive code increased, the complexity and variety of architectures, platforms, and protocols has increased too. This pushes the number of permutations of state, behavior, interactions, and outputs well beyond a development team’s capabilities to test effectively.

The most crucial step towards better automotive security is to transform development teams such that they understand vulnerabilities and, more importantly, know how to build an efficient test framework to detect vulnerabilities. Developer education is key here;

a relatively small investment in training and processes is the difference between a team that hides from the realities of cybersecurity risk and one that’s smart enough to choose the right techniques and tools to combat risk — many of which have already proven to be successful in other industries.

A simple test is to ask developers if they know how to restrict memory reads and writes to specific locations, thereby preventing improper access to data. While the answer may be simple, it’s the first step towards understanding that protection, and not performance, is the key to security.
It's safe to say that some developers would balk at new standards, especially without the education that goes with them, so the second familiar test technique solves three problems at the same time; efficiency, adoption, and training. Automated testing is something that automotive developers have used for years, proving to be an effective way to offload common, complex, and often cumbersome work onto a controllable framework. Adapting existing automated test tools to include security verification adds little to no burden on the developer, in terms of execution, but provides useful education around good secure coding practices when a test fails. It's this unique win-win environment that makes automated testing so valuable (and acceptable) to developers.

Educating developers and bringing new tools up to speed may take more time than some suppliers have, so it's worthwhile to investigate two familiar test techniques up front and adapt them to automotive security. First, automotive teams have been using coding and safety standards, such as MISRA and ISO 26262, for some time now but some organizations are starting to see how security standards can help in the same way. Adopting common, community-driven security standards such as OWASP and CWE takes advantage of expert security guidelines to quickly educate development teams on secure coding principles and provide a ready-to-use measure of how secure their code actually is. If these standards prove insufficient, creating in-house, application-specific standards also creates a consistent, measurable guideline for application security testing.
WHERE DO I START?

Read why software security needs to begin with flaw-free, standards-compliant code.

Learn the top 5 best practices for delivering secure in-vehicle software.

Read about static code analysis in an agile world.

Discover what automakers really think about cybersecurity.
For more information, please visit:

www.roguewave.com