Safety is Important, Security as Well

Helen Buchumensky, **Karamba Security Ltd**
Thomas Liedtke, Steffen Herrmann, **Kugler Maag Cie**

Special Thanks to Andrei Donciuc**, Kugler Maag Cie**

Forbes Top 25 IoT Startups 2019

Gartner Cool Vendor 2018

Automotive AWARDS | 3 TIME WINNER 2017+2018+2019

WINNER Tech CARS Awards auto connected car news

Karamba Security

Nice to Meet You!

Helen Buchumensky

- Director of Program Management, Karamba Security
- ASQ Certified Manager Quality and Organizational Excellence
- VDA 6.3 Certified Process Auditor
- IATF 16949, ISO9001 Certified Auditor
- BSc Industrial Engineering & MBA, Organization Behavior

Thomas Liedtke

- Principal Consultant at Kugler Maag Cie
- Expert Area Leader, Security
- Certified IT Security Commissioner and certified Privacy Commissioner
- Provisional Scrum Master, trainer and speaker for project management and safety
- PhD in Computer Science and Mathematics

Steffen Herrmann

- Managing Consultant at Kugler Maag Cie
- TÜV Rheinland certified Functional Safety Engineer (Automotive)
- intacsTM certified Principal Assessor and Instructor
- Co-author of books and speaker at conferences
- Dipl.-Wi.-Ing Industrial Engineering and Management

ISO26262:2018 2nd Edition, Road vehicles -- Functional Safety

Karamba Security

…The organization shall institute and maintain effective communication channels between functional safety, cybersecurity…

*(a) in the case it is identified that a **cybersecurity issue might violate a safety goal***
*(b) or in the case a **cybersecurity requirement might compete with a safety requirement***

ISO26262:2018
Part 2, 5.4.2.3

Science Fiction?

The Fate of the Furious 2017

A New Reality

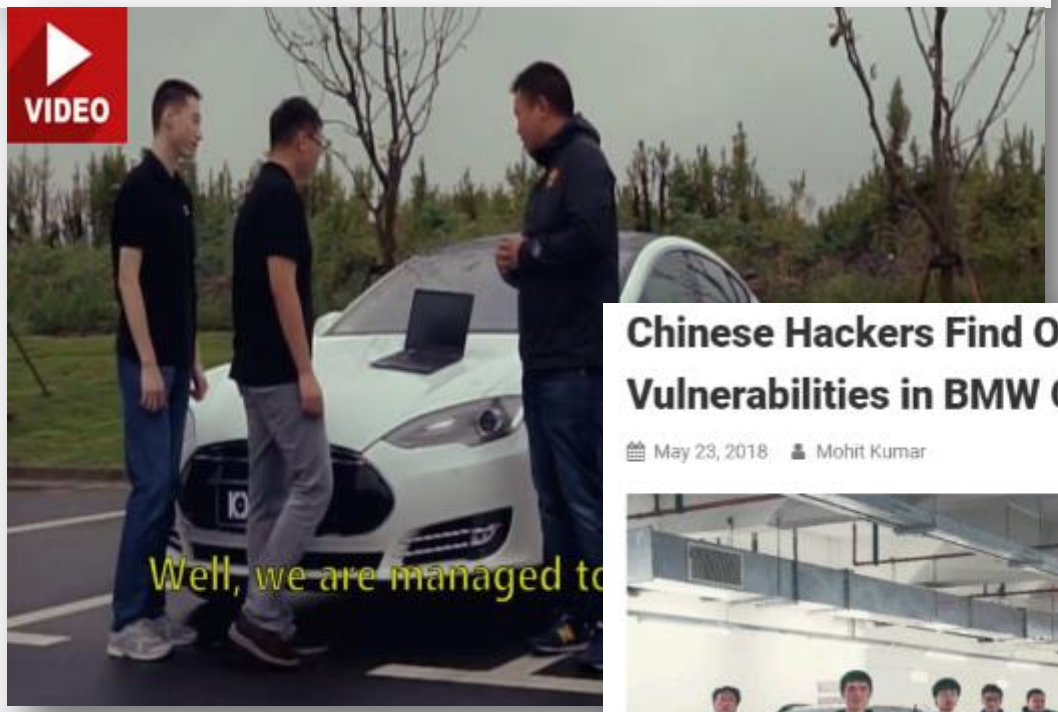
ANDY GREENBERG SECURITY 07.21.15 06:00 AM

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

I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Researchers Demonstrate How They Remotely Hacked A Tesla

BY MICHAEL KARKAFIRIS | SEPTEMBER 20, 2016



Chinese Hackers Find Over a Dozen Vulnerabilities in BMW Cars

May 23, 2018 Mohit Kumar

NEWS

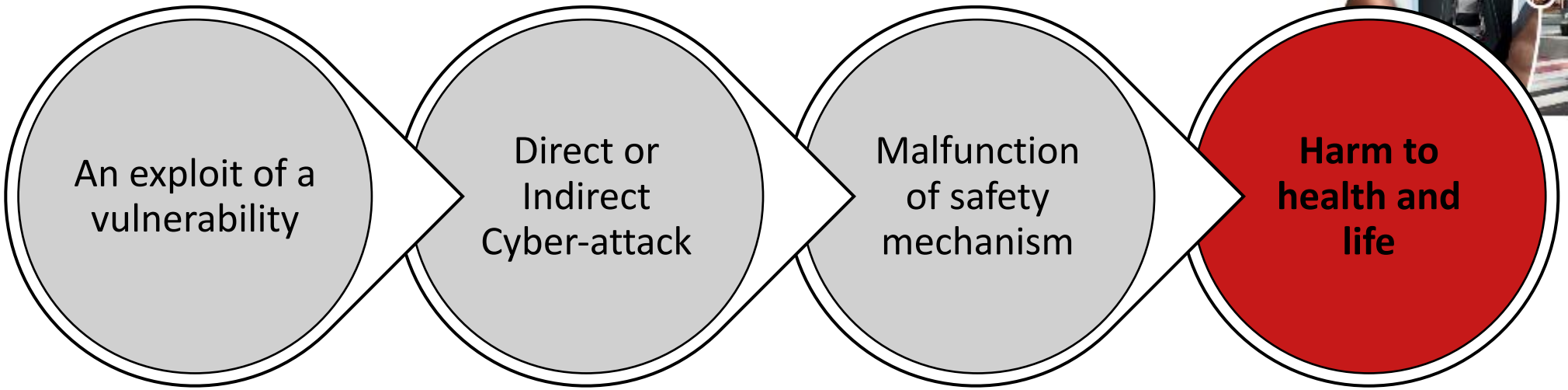
Car hackers find remotely exploitable vulnerabilities in Volkswagen and Audi vehicles

Researchers discovered flaws in the Audi A3 Sportback e-tron and the Volkswagen Golf GTE that make the vehicles vulnerable to remote hacking.

Safety Critical Systems are also Cybersecurity Critical

Karamba Security

- A misbehavior of a **Safety-critical** system may cause harm to health and life.
- An exploit of a vulnerability of a **Cybersecurity-critical** system may lead to financial, operational, privacy, or **safety** losses.



Automotive Regulation for Cybersecurity

Karamba Security

NHTSA	Cyber security risk management framework applied to modern vehicles, 2014
SAE INTERNATIONAL	SAE J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems“ 2016
AUTO-ISAC Automotive Information Sharing and Analysis Center	Auto ISAC “Automotive Cybersecurity Best Practices” 2016
enisa	Cyber Security and Resilience of smart cars 2017
	UNECE Proposal for a Recommendation on Cyber Security 2019
ISO/SAE 21434	Road Vehicles -- Cybersecurity engineering (under development)

When Cybersecurity meets Safety

The Show Must Go On

”Safe State or not? That is the question”

Security

- Fail operational: keep operational even if you know you’re hacked
- DoS: If you have shut down, the hackers have won
- Safe State → only when a safety-critical incident appears
- Heuristics relates more to detection than to prevention (the emergency braking should not be blocked)

Safety

Without SOTIF (if driver backup is there)

- Before anything bad happens → Safe State
- A shut-down car in the parking lot is a safe car.

With SOTIF (no driver backup is there)

- Performance (degraded) still necessary

→ Avoid false positives

The Show must go on

”Safe State or not? That is the question”

Update, Update, Update

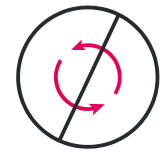
“Learn from your disclosed vulnerabilities”

Security

- Likes to update, update, update…
  - Constant need for updates over lifetime in order to stay secure
  - Worst case: Every successful attack leads to an update in order to avoid similar attacks from re-occurring
- Simple update process is mandatory
  - Vehicles must be reached for update
  - OTA itself is a weakness
- Known vulnerabilities are ticking time-bombs

Safety

- Never change a running system.
- Effort for impact analysis and re-certification is disproportionate to do it for every attack.
- Keep it as encapsulated as possible.



→ Don’t rely on updates

Update, Update, Update

“Learn from your disclosed Vulnerabilities”

Be Informed – 24/7 – Worldwide

How much do you have to know?

Security

- Field monitoring activities for cybersecurity are essential
  - Incident reporting is crucial
  - Tracking and resolution in order to communicate safety-related cybersecurity field incidents and functional safety
- If a vehicle is owned by an individual a party is necessary to be responsible to support in case of security issues
- How to handle vintage cars?

Safety

- Regular maintenance is sufficient
- Field monitoring must be implemented
- Safety incidents → Reported issues must be analyzed for safety criticality
- Vehicle owner is responsible for performing maintenance but cannot be forced

-> Field monitoring is required

Be Informed – 24/7 – Worldwide

KUGLER MAAG CIE
besser mit uns

Karamba Security

How much do you have to know?

Safety Resources are Sacred

“Resources are rare”

Security

- Cybersecurity implementation needs resources
- The more Cybersecurity you want, the more resources you‘ll need

Safety

- Networks and ECUs are Resource-constrained
- Determine:
  - Network overload
  - RAM footprints
- Cybersecurity cannot violate Safety-system resources
- Be aware of the extent of processing overhead on:
  - Bus
  - CPU
  - Memory

-> Careful Resource Management

Safety Resources are Sacred

“Resources are rare”

Can’t Live with Her, Can’t Live without Her

Without cybersecurity protection, safety is at risk:

➔ Cyber attack could lead to safety mechanisms malfunction

With cybersecurity protection, safety is at risk:

➔ Contradiction of needs and requirements

Is there a recipe for how these two important concepts can live together in one system?

Cybersecurity Approaches vs Safety Constraints

Karamba Security

Secure SW Development Secure Coding

+ Make hacker's life difficult
- Do not prevent the attacks
- Legacy code
- No field monitoring

SAFETY PASSED REDUCTION ONLY

Blacklisting

- Update-dependent

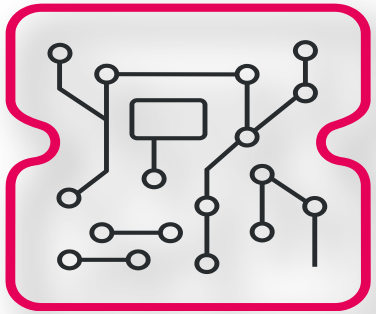
SAFETY FAILED

Behavior Analysis (Artificial Intelligence)

+ Monitoring
- False Positives
- Performance

SAFETY PASSED DETECTION ONLY

Software Integrity (Whitelist)

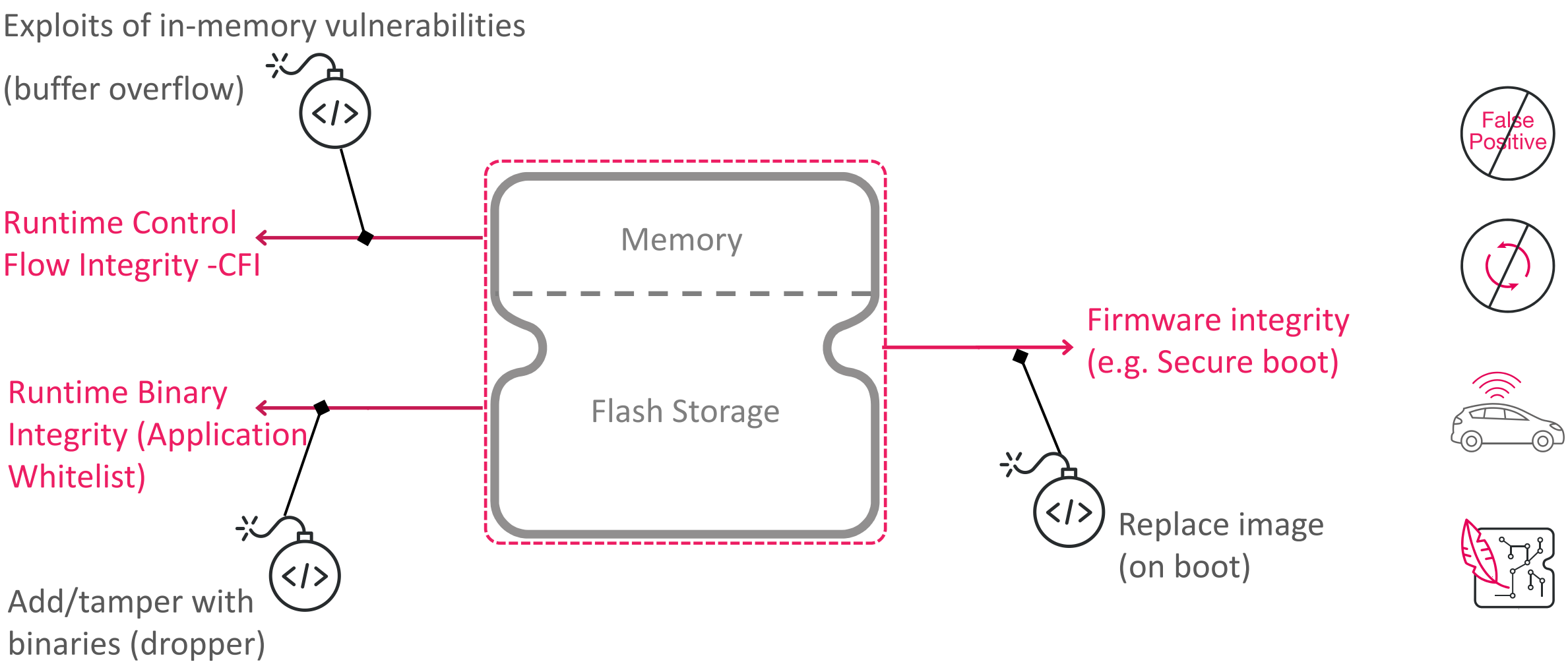


+ Prevention capabilities
+ Zero False Positives
+ Zero day protection

SAFETY GRADE PREVENTION

Software Integrity Layers for Safety-critical Systems

Karamba Security



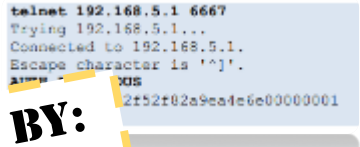
Jeep Cherokee Hacking by Chris Valasek and Charlie Miller

Karamba Security

1 Attack Surface Research

2 Define Target (Uconnect System)

3 Locate O… (D-Bus)



RISK REDUCED BY: GOOD PRACTICES

4 Success to login anonymously "Foot in the Door"

5 Uconnect is under control!

6 Start Jailbreaking: Reverse Engineering IOC

7 Execute a script change v850 to "Update mode"

PREVENTED BY "WHITELIST"

8 Reprogram the device using …ular network

9 Reboot the system with Malicious Firmware

PREVENTED BY: "SECURE BOOT"

10 Gain full control, including steering

[Full Report: https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf](https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf)

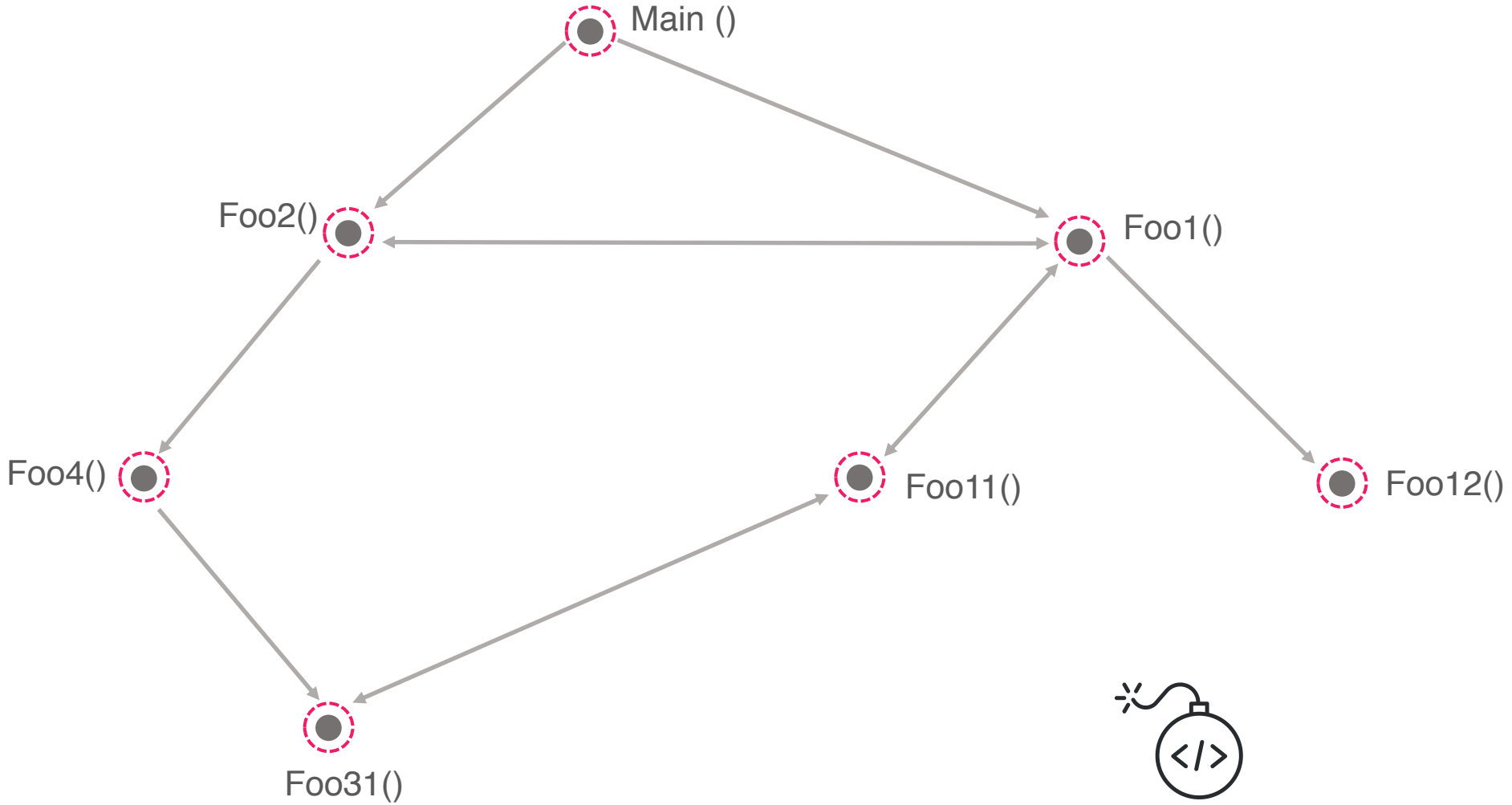
BMW Assessment by Keen Lab: 14 Vulnerabilities Found

*"After some tough reverse-engineering work on TCB's firmware, we also found a **memory corruption vulnerability** that allows us to bypass the signature protection and achieve **remote code execution** in the firmware. "*

https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/

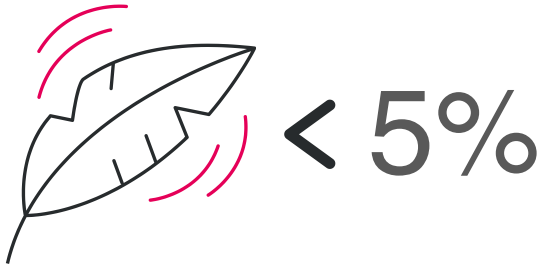
Control Flow Integrity- How does It Work?

Karamba Security



A Key Trade-off: Performance Impact

- Academic research: Proven safeguard but not considered practical due to performance overhead
- In mutual SAE paper, Karamba and DENSO demonstrated[1] software run time integrity meeting ECU constraints of less than 5% impact on:
  1. CPU overheard
  2. Root FS size
  3. RAM Usage



[1] https://www.sae.org/publications/technical-papers/content/2018-01-0016/

Under Attack – 3 steps

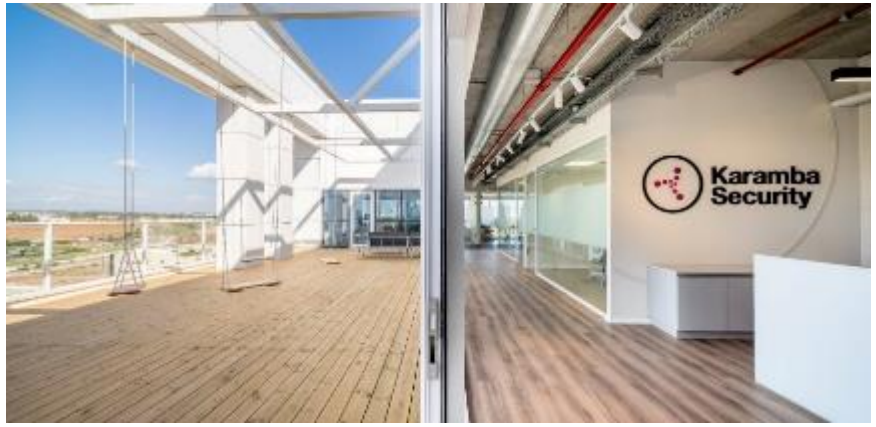
1. Prevent the Attack (Fail-Safe)
2. Collect valuable forensics (stack dump, memory map, registers)
3. Prepare the remedy with no rush- The safety wasn’t compromised

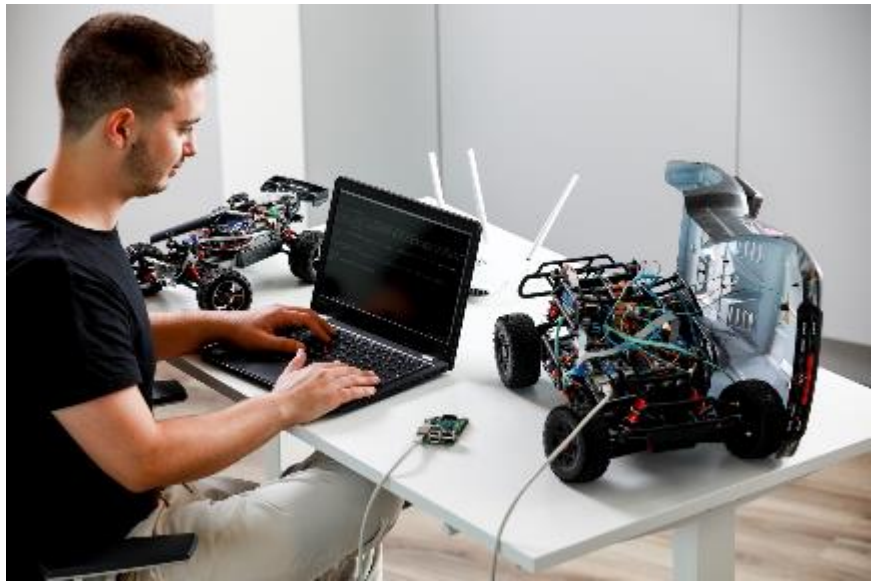
Summing-up

- ✓Safety critical systems can and shall be protected from cyber attacks
- ✓A desirable protection layer would be deterministic, require minimum resources, and prevent known and unknown security threats, providing valuable forensic data.
- ✓To make things harder for hackers: SW development best practices and secure coding are recommended

Meet Karamba Security

- Established in 2016
- The Mission: Prevent hackers from compromising vehicles' safety
- Active engagements with 17 automotive OEMs and tier-1s
- 12 patents granted, 21 pending
- Consistently recognized for market leadership





Forbes Top 25 IoT Startups 2019

Automotive AWARDS | 3 TIME WINNER 2017+2018+2019

WINNER Tech CARS Awards auto connected car news

Questions?

Thank you & keep in touch!

helenb@karambasecurity.com

https://www.linkedin.com/in/helenb