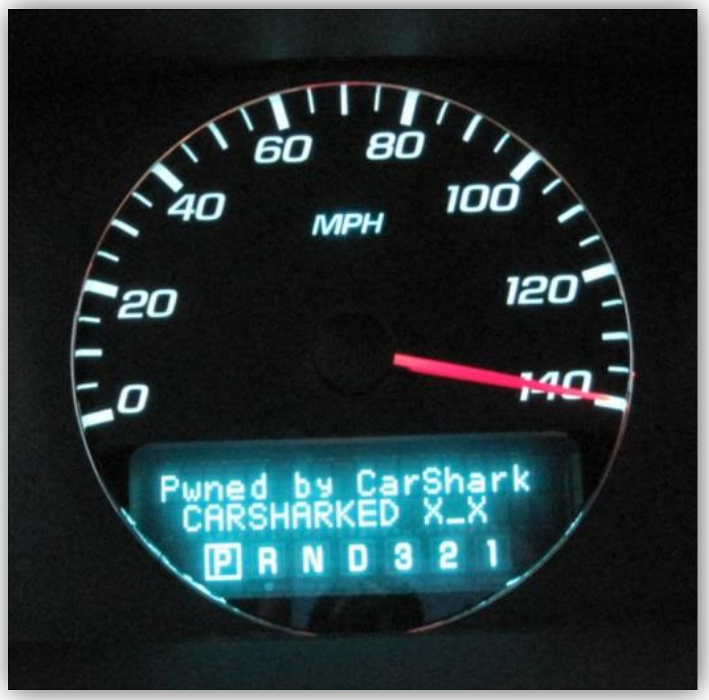
Security Analysis of Automotive Architectures using Probabilistic Model Checking

Philipp Mundhenk, Sebastian Steinhorst,
Martin Lukasiewycz, Suhaib A. Fahmy,
Samarjit Chakraborty
philipp.mundhenk@tum-create.edu.sg

Examples for Automotive Security

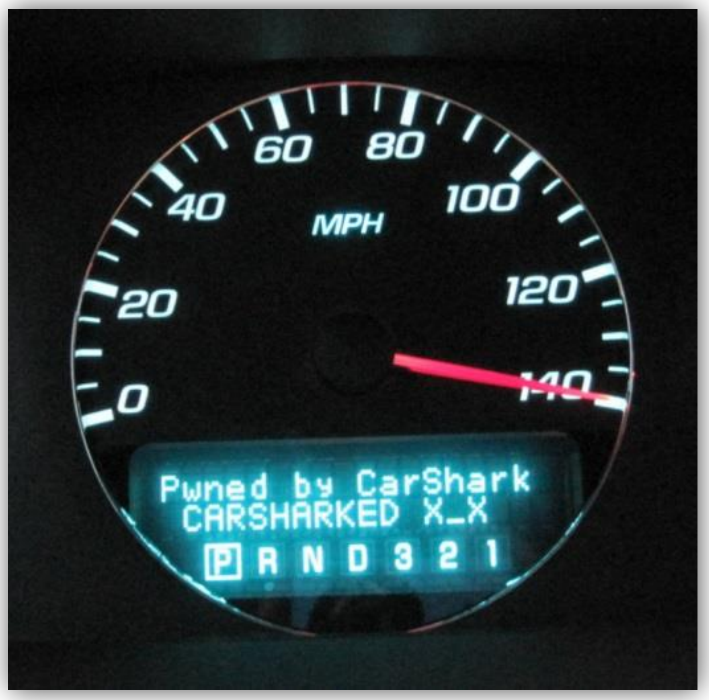
Examples for Automotive Security



[1]

[1] K. Koscher, et.al. Experimental security analysis of a modern automobile. In Proc. of the 31st IEEE Symposium on Security and Privacy (SP), 2010.
[2] https://www.progressive.com/auto/snapshot/

Examples for Automotive Security



[1]

[2]

[1] K. Koscher, et.al. Experimental security analysis of a modern automobile. In Proc. of the 31st IEEE Symposium on Security and Privacy (SP), 2010.
[2] https://www.progressive.com/auto/snapshot/

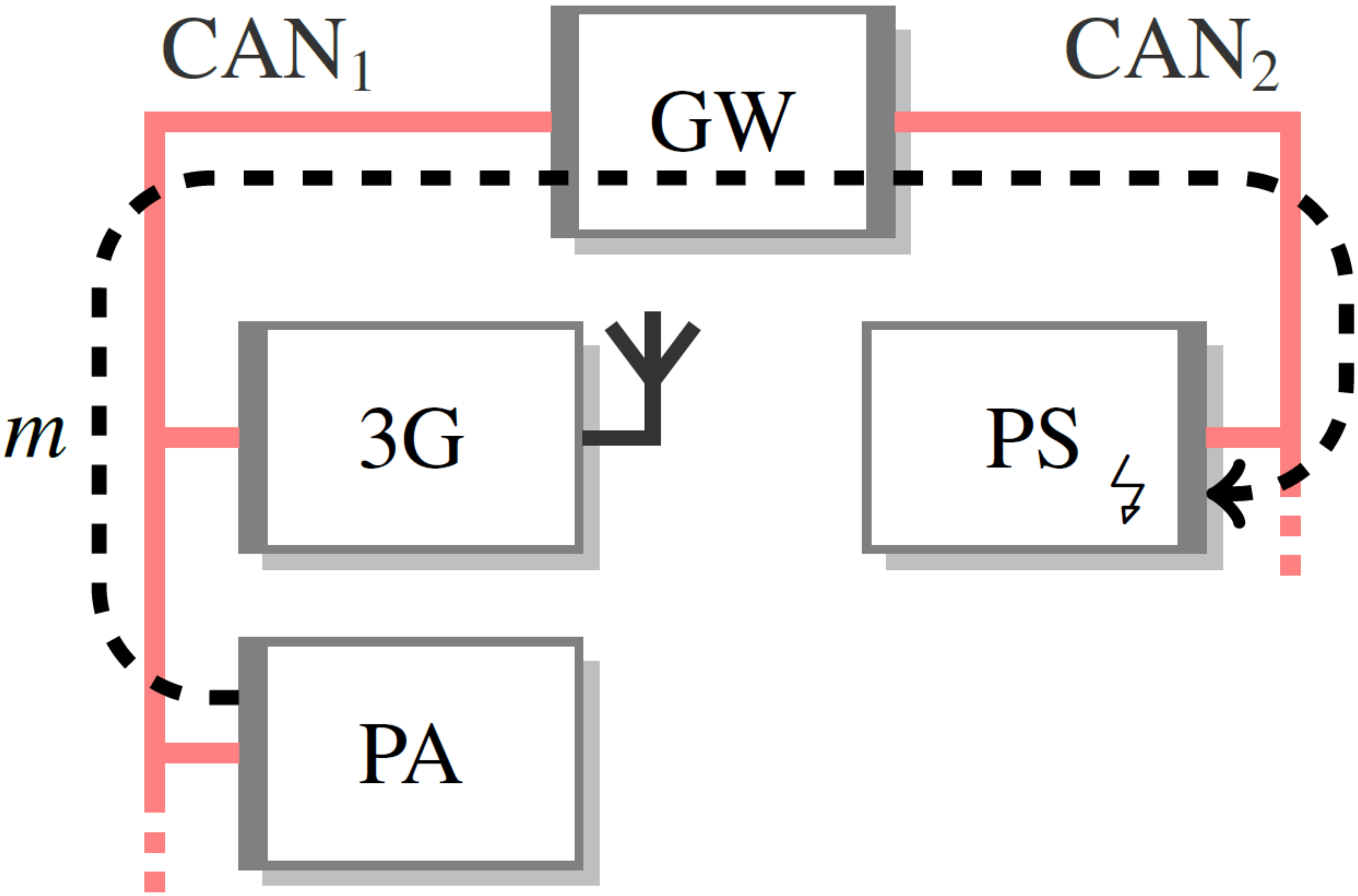
Motivation

- **What** influence do component vulnerabilities have on the security of a specific function?

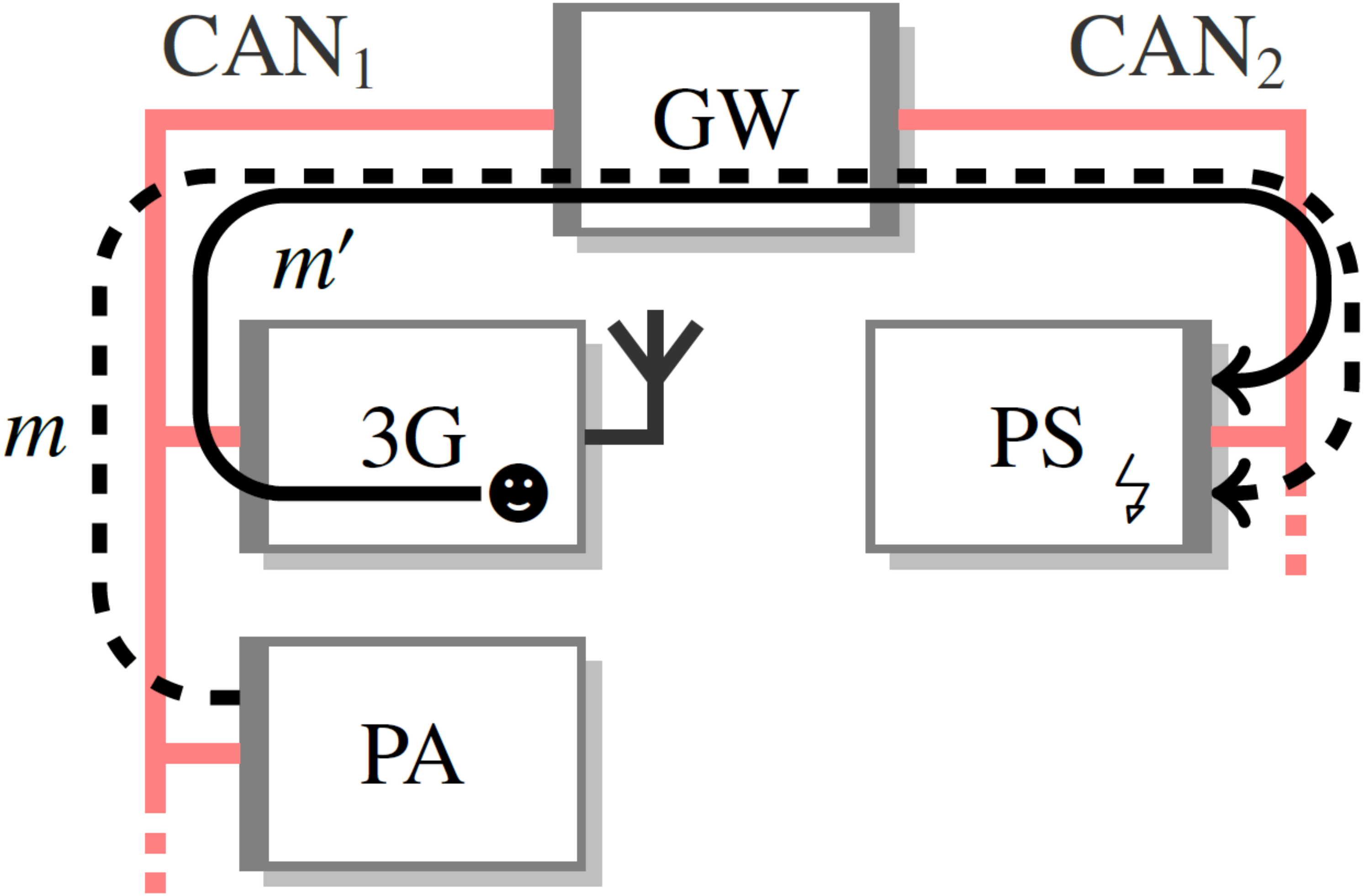
- Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?

- **How much** effort should be invested in the consideration of security during implementation of specific components?

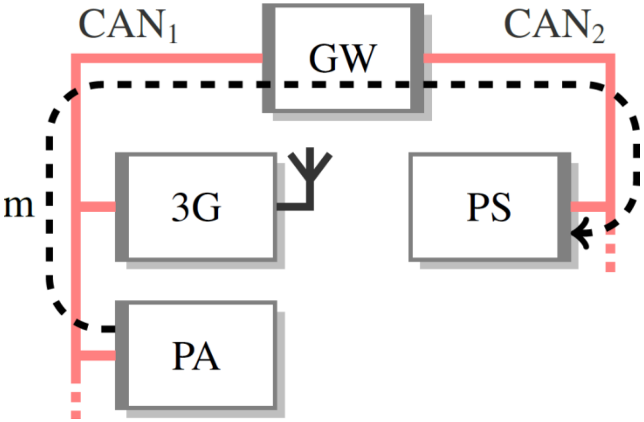
Motivating Example



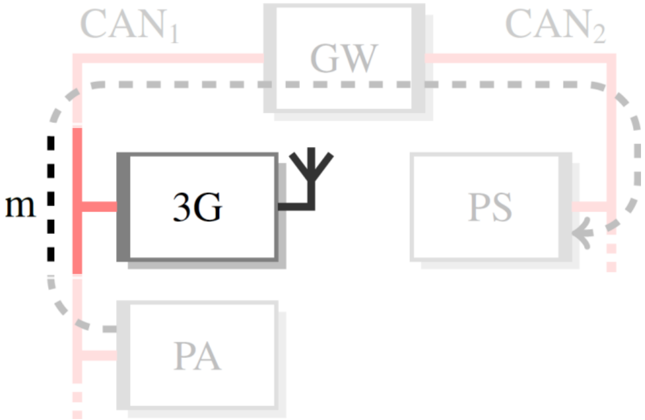
Motivating Example



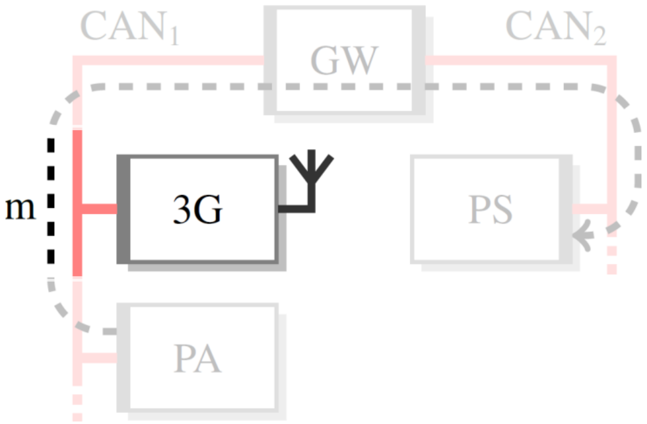
Motivating Example



Motivating Example

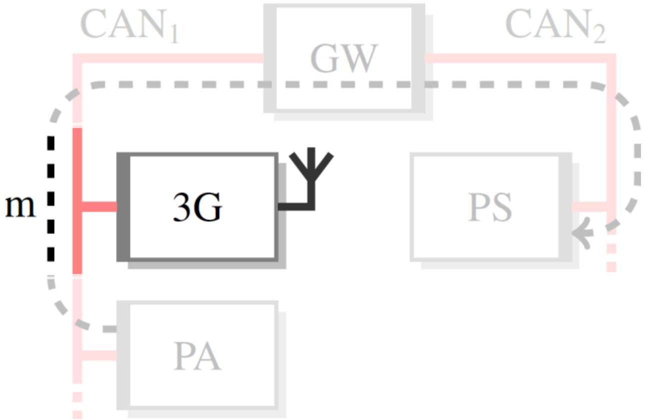


Motivating Example



$$s = (s_{3G}, s_{\mathrm{CAN}_1}, s_{m_{\mathrm{conf}}})$$

Motivating Example



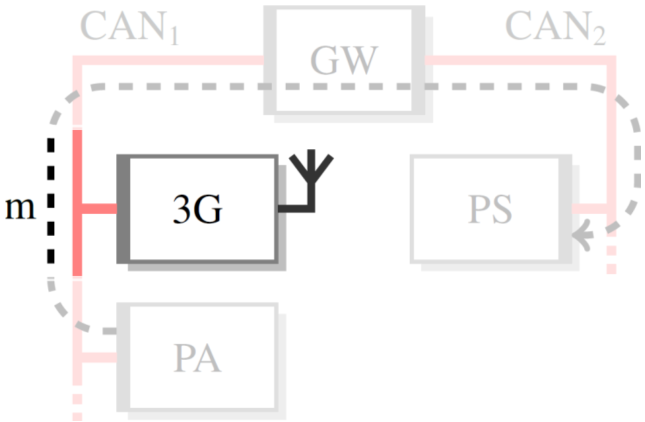
$$s = (s_{3G}, s_{CAN_1}, s_{m_{conf}})$$

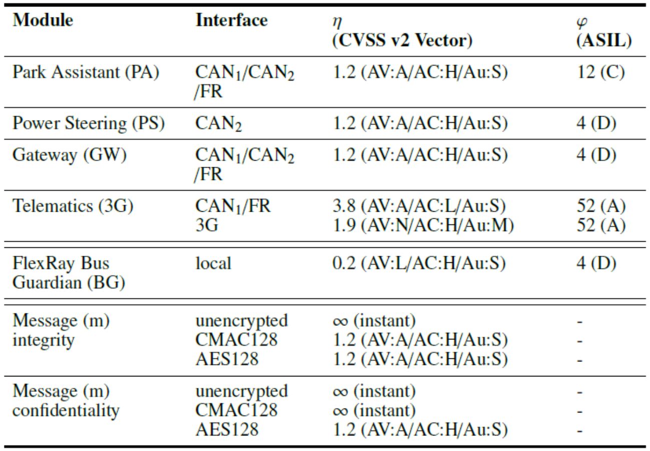
secure

3G exploitable

3G & m exploitable

Motivating Example





Module	Interface	η (CVSS v2 Vector)	φ (ASIL)
Park Assistant (PA)	CAN$_1$/CAN$_2$ /FR	1.2 (AV:A/AC:H/Au:S)	12 (C)
Power Steering (PS)	CAN$_2$	1.2 (AV:A/AC:H/Au:S)	4 (D)
Gateway (GW)	CAN$_1$/CAN$_2$ /FR	1.2 (AV:A/AC:H/Au:S)	4 (D)
Telematics (3G)	CAN$_1$/FR 3G	3.8 (AV:A/AC:L/Au:S) 1.9 (AV:N/AC:H/Au:M)	52 (A) 52 (A)
FlexRay Bus Guardian (BG)	local	0.2 (AV:L/AC:H/Au:S)	4 (D)
Message (m) integrity	unencrypted CMAC128 AES128	∞ (instant) 1.2 (AV:A/AC:H/Au:S) 1.2 (AV:A/AC:H/Au:S)	- - -
Message (m) confidentiality	unencrypted CMAC128 AES128	∞ (instant) ∞ (instant) 1.2 (AV:A/AC:H/Au:S)	- - -

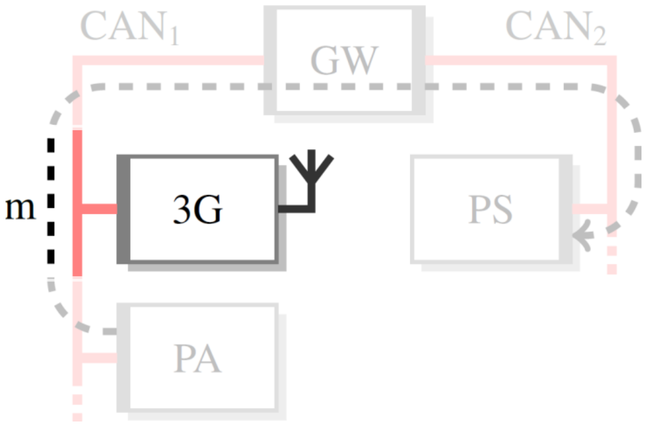
$$s = (s_{3G}, s_{\mathrm{CAN}_1}, s_{m_{\mathrm{conf}}})$$

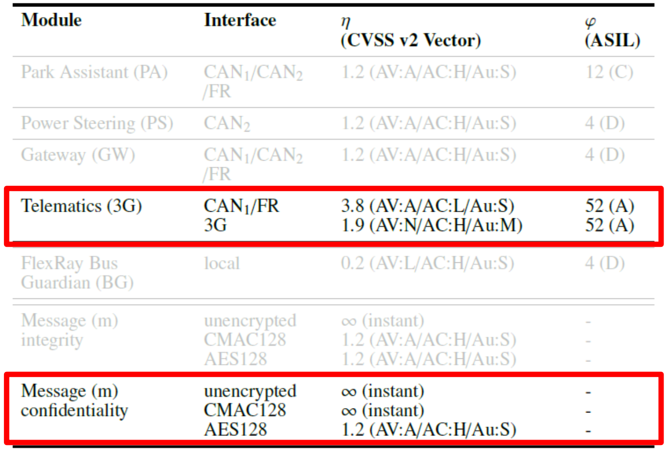
secure

3G exploitable

3G & m exploitable

Motivating Example





Module	Interface	η (CVSS v2 Vector)	φ (ASIL)
Park Assistant (PA)	CAN$_1$/CAN$_2$ /FR	1.2 (AV:A/AC:H/Au:S)	12 (C)
Power Steering (PS)	CAN$_2$	1.2 (AV:A/AC:H/Au:S)	4 (D)
Gateway (GW)	CAN$_1$/CAN$_2$ /FR	1.2 (AV:A/AC:H/Au:S)	4 (D)
Telematics (3G)	CAN$_1$/FR 3G	3.8 (AV:A/AC:L/Au:S) 1.9 (AV:N/AC:H/Au:M)	52 (A) 52 (A)
FlexRay Bus Guardian (BG)	local	0.2 (AV:L/AC:H/Au:S)	4 (D)
Message (m) integrity	unencrypted CMAC128 AES128	∞ (instant) 1.2 (AV:A/AC:H/Au:S) 1.2 (AV:A/AC:H/Au:S)	- - -
Message (m) confidentiality	unencrypted CMAC128 AES128	∞ (instant) ∞ (instant) 1.2 (AV:A/AC:H/Au:S)	- - -

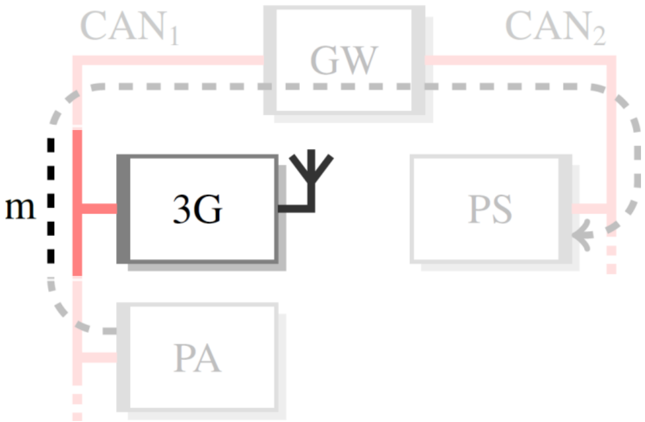
$$s = (s_{3G}, s_{\mathrm{CAN}_1}, s_{m_{\mathrm{conf}}})$$

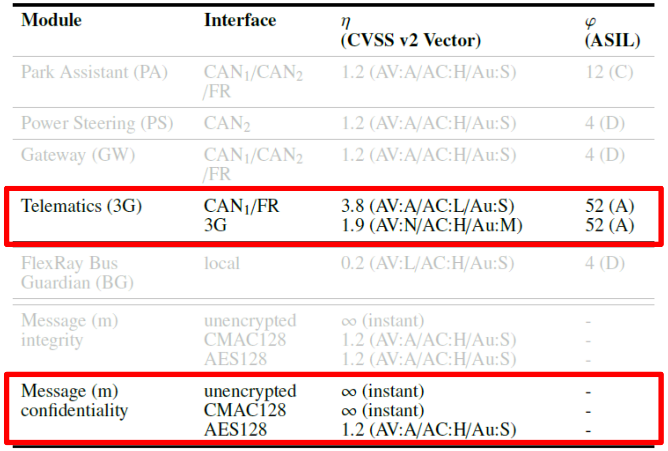
secure

3G exploitable

3G & m exploitable

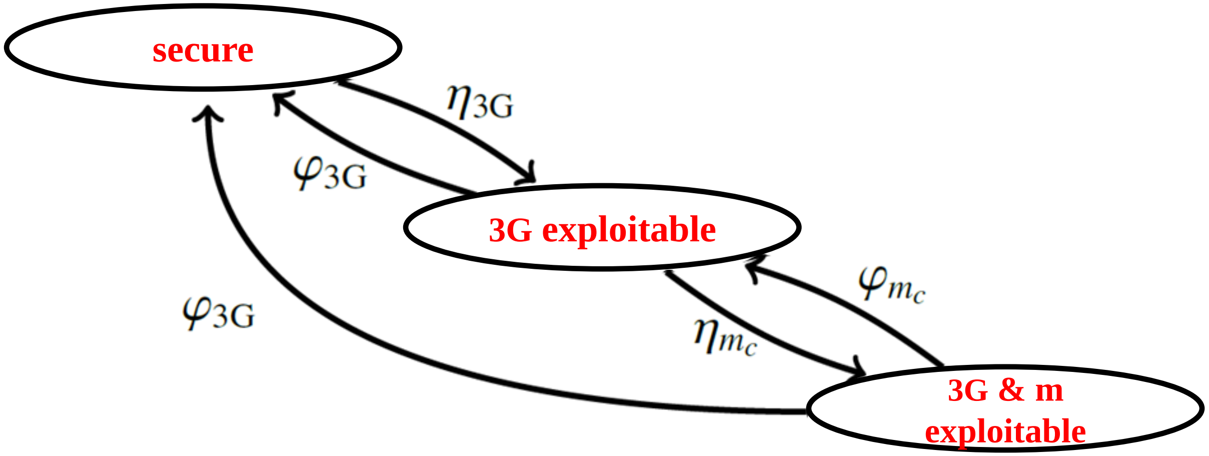
Motivating Example



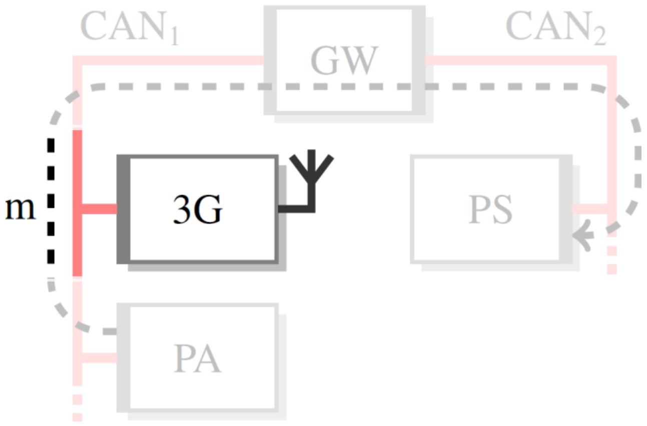


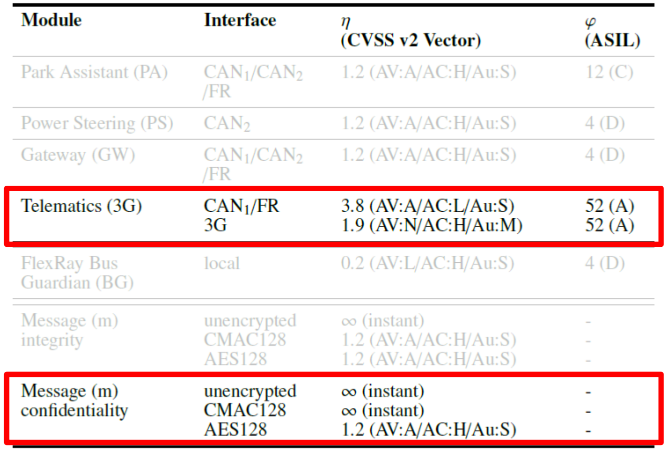
Module	Interface	η (CVSS v2 Vector)	φ (ASIL)
Park Assistant (PA)	CAN$_1$/CAN$_2$ /FR	1.2 (AV:A/AC:H/Au:S)	12 (C)
Power Steering (PS)	CAN$_2$	1.2 (AV:A/AC:H/Au:S)	4 (D)
Gateway (GW)	CAN$_1$/CAN$_2$ /FR	1.2 (AV:A/AC:H/Au:S)	4 (D)
Telematics (3G)	CAN$_1$/FR 3G	3.8 (AV:A/AC:L/Au:S) 1.9 (AV:N/AC:H/Au:M)	52 (A) 52 (A)
FlexRay Bus Guardian (BG)	local	0.2 (AV:L/AC:H/Au:S)	4 (D)
Message (m) integrity	unencrypted CMAC128 AES128	∞ (instant) 1.2 (AV:A/AC:H/Au:S) 1.2 (AV:A/AC:H/Au:S)	- - -
Message (m) confidentiality	unencrypted CMAC128 AES128	∞ (instant) ∞ (instant) 1.2 (AV:A/AC:H/Au:S)	- - -

$$s = (s_{3\mathrm{G}}, s_{\mathrm{CAN}_1}, s_{m_{\mathrm{conf}}})$$



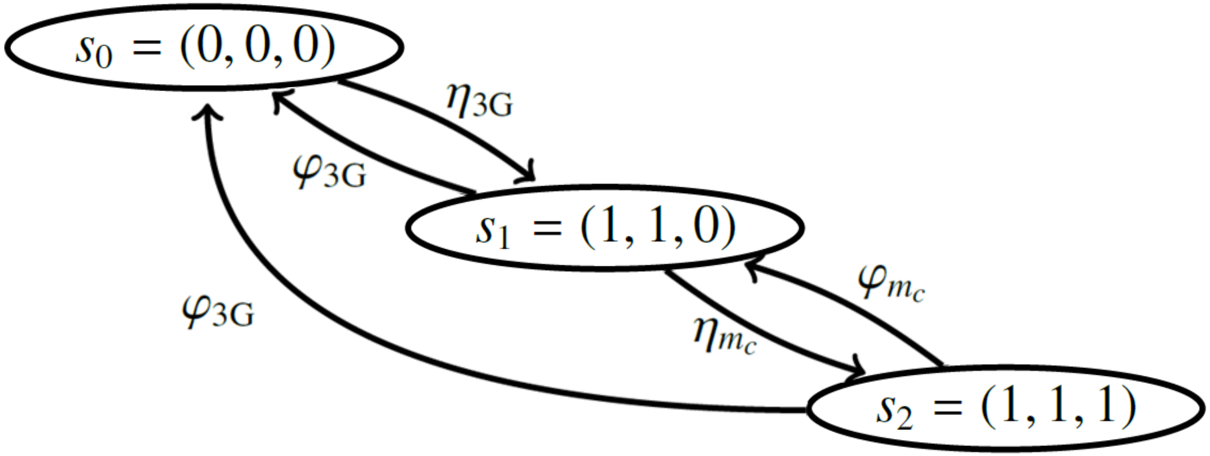
Motivating Example



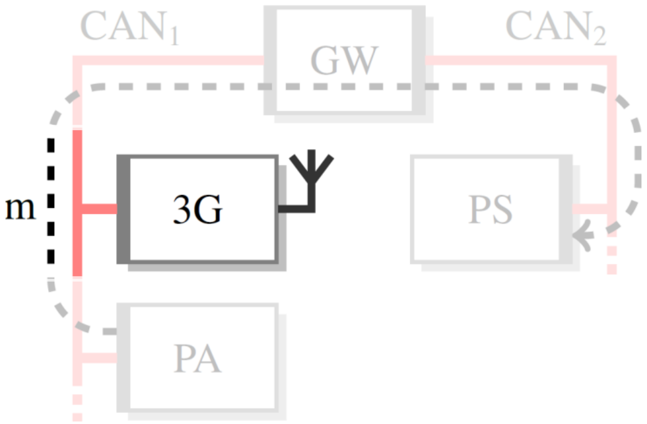


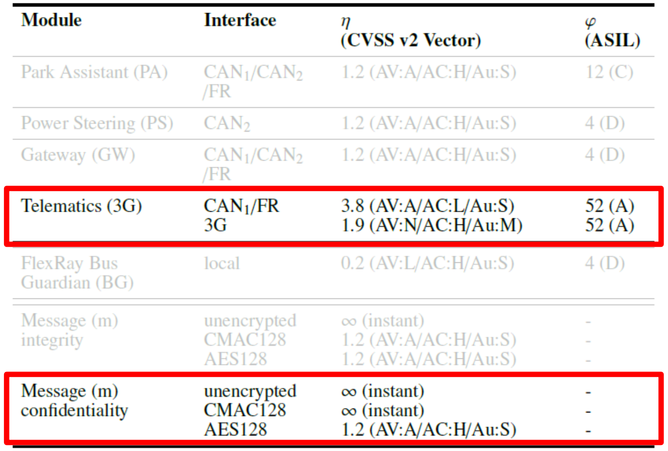
Module	Interface	η (CVSS v2 Vector)	φ (ASIL)
Park Assistant (PA)	CAN$_1$/CAN$_2$ /FR	1.2 (AV:A/AC:H/Au:S)	12 (C)
Power Steering (PS)	CAN$_2$	1.2 (AV:A/AC:H/Au:S)	4 (D)
Gateway (GW)	CAN$_1$/CAN$_2$ /FR	1.2 (AV:A/AC:H/Au:S)	4 (D)
Telematics (3G)	CAN$_1$/FR 3G	3.8 (AV:A/AC:L/Au:S) 1.9 (AV:N/AC:H/Au:M)	52 (A) 52 (A)
FlexRay Bus Guardian (BG)	local	0.2 (AV:L/AC:H/Au:S)	4 (D)
Message (m) integrity	unencrypted CMAC128 AES128	∞ (instant) 1.2 (AV:A/AC:H/Au:S) 1.2 (AV:A/AC:H/Au:S)	- - -
Message (m) confidentiality	unencrypted CMAC128 AES128	∞ (instant) ∞ (instant) 1.2 (AV:A/AC:H/Au:S)	- - -

$$s = (s_{3\mathrm{G}}, s_{\mathrm{CAN}_1}, s_{m_{\mathrm{conf}}})$$



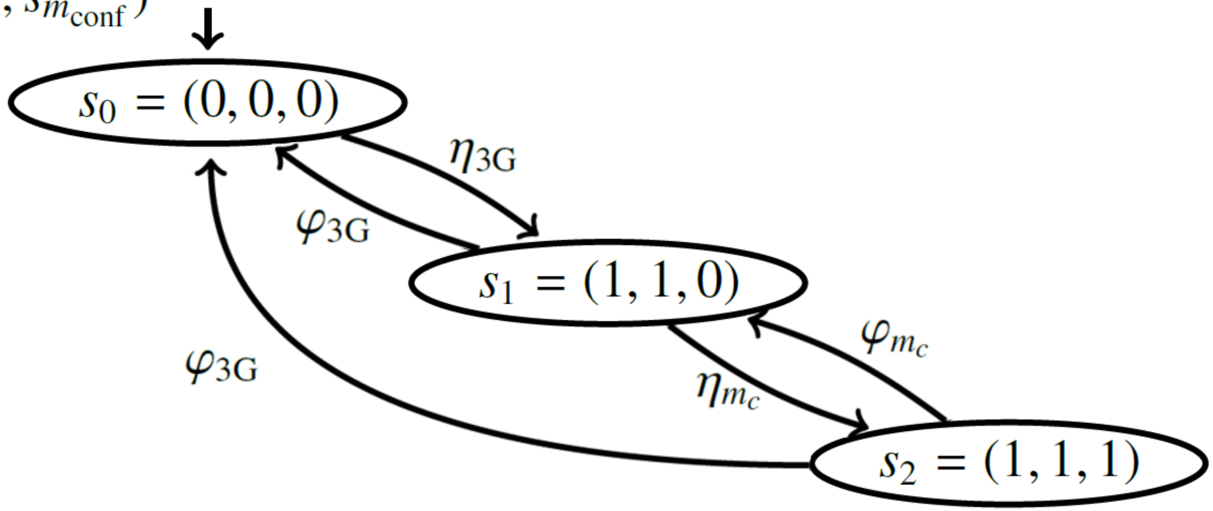
Motivating Example



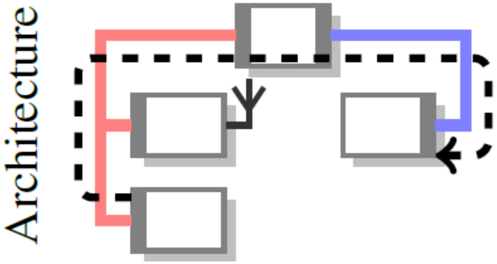


Module	Interface	η (CVSS v2 Vector)	φ (ASIL)
Park Assistant (PA)	CAN$_1$/CAN$_2$ /FR	1.2 (AV:A/AC:H/Au:S)	12 (C)
Power Steering (PS)	CAN$_2$	1.2 (AV:A/AC:H/Au:S)	4 (D)
Gateway (GW)	CAN$_1$/CAN$_2$ /FR	1.2 (AV:A/AC:H/Au:S)	4 (D)
Telematics (3G)	CAN$_1$/FR 3G	3.8 (AV:A/AC:L/Au:S) 1.9 (AV:N/AC:H/Au:M)	52 (A) 52 (A)
FlexRay Bus Guardian (BG)	local	0.2 (AV:L/AC:H/Au:S)	4 (D)
Message (m) integrity	unencrypted CMAC128 AES128	∞ (instant) 1.2 (AV:A/AC:H/Au:S) 1.2 (AV:A/AC:H/Au:S)	- - -
Message (m) confidentiality	unencrypted CMAC128 AES128	∞ (instant) ∞ (instant) 1.2 (AV:A/AC:H/Au:S)	- - -

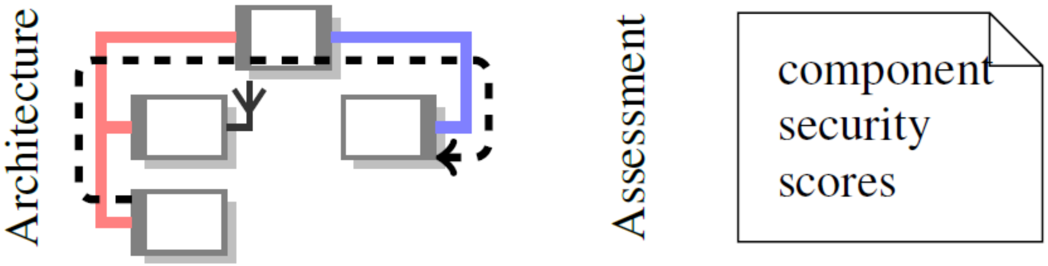
$$s = (s_{3\text{G}}, s_{\text{CAN}_1}, s_{m_{\text{conf}}})$$



Process



Process

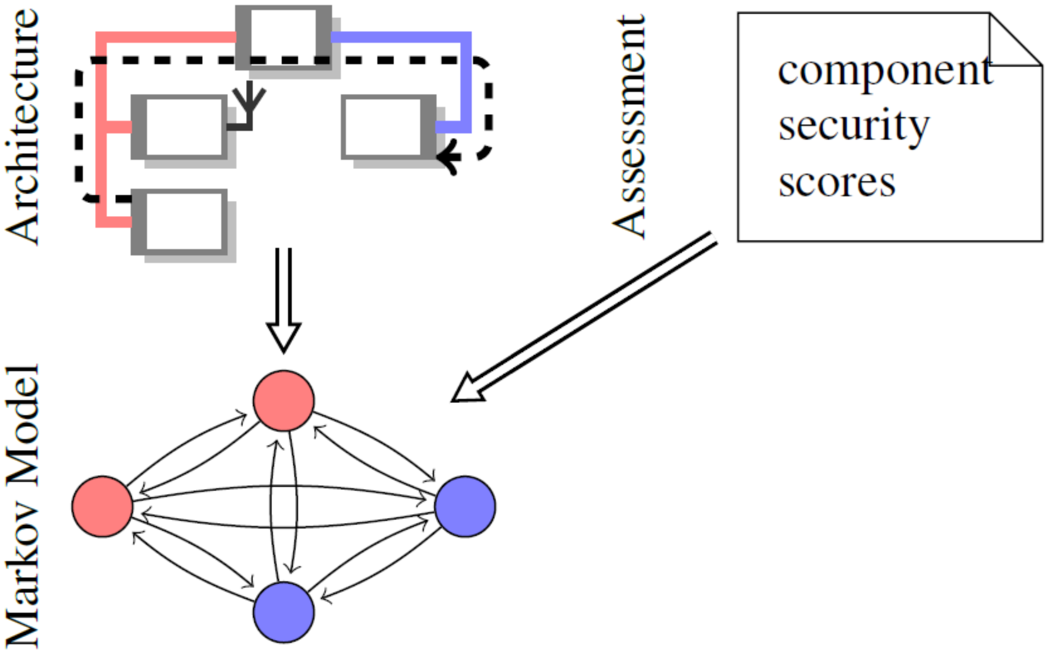


Architecture

Assessment

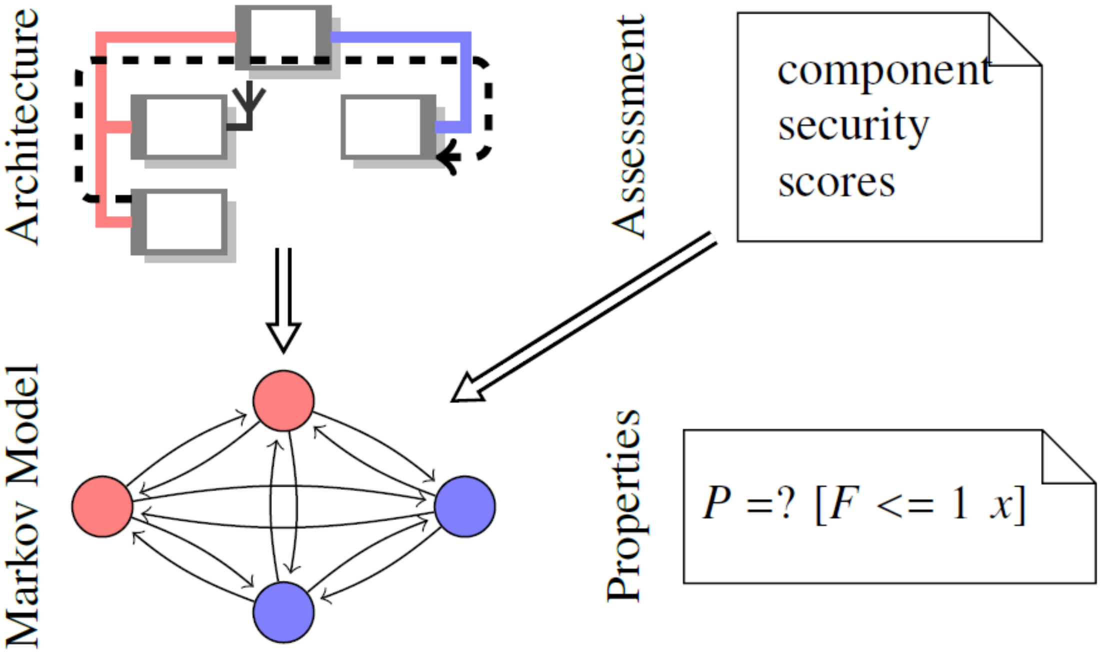
component
security
scores

Process



Architecture
Assessment
component security scores
Markov Model

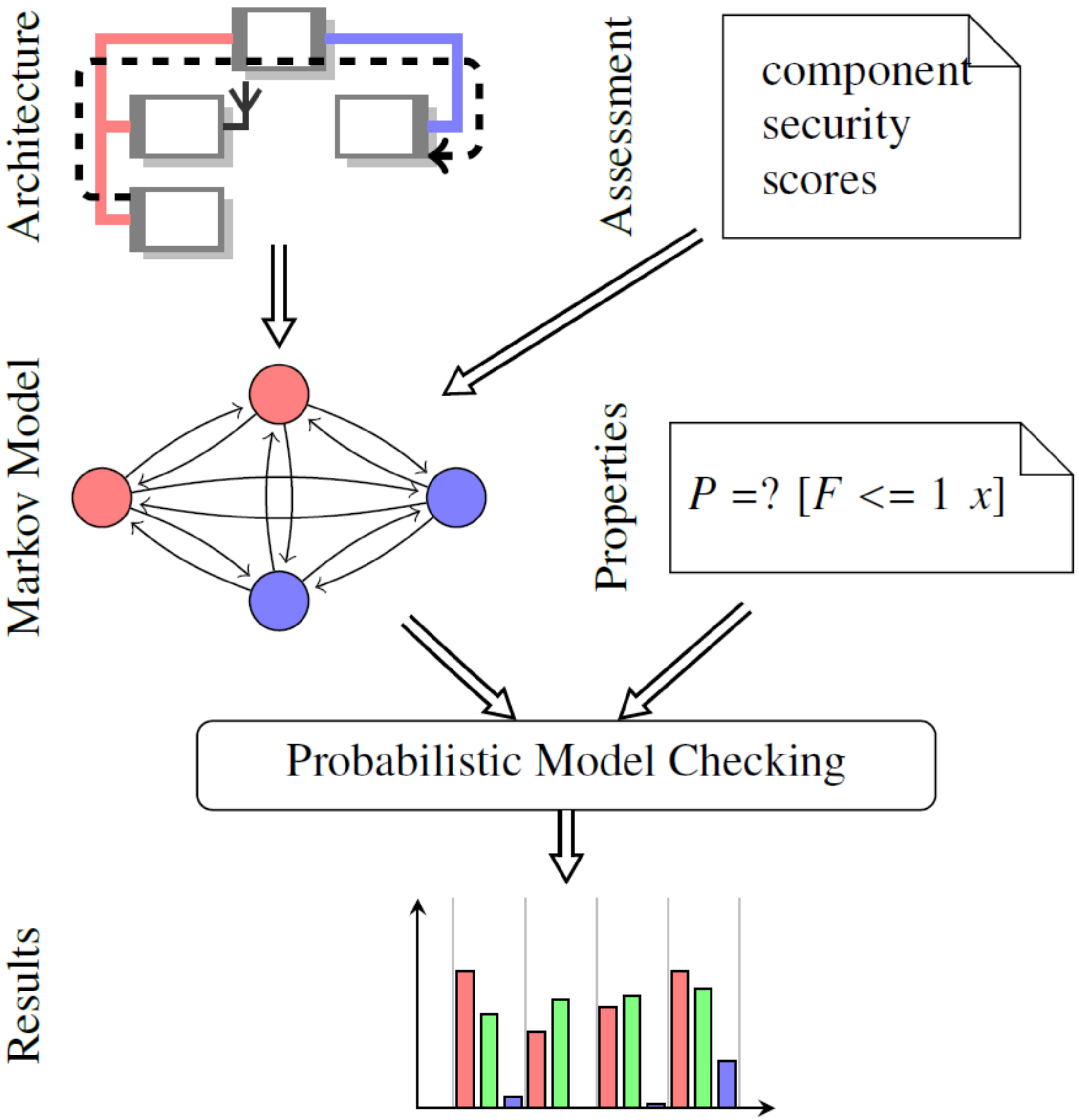
Process



component security scores

$P =? [F <= 1 \; x]$

Process



Architecture

Assessment

component security scores

Markov Model

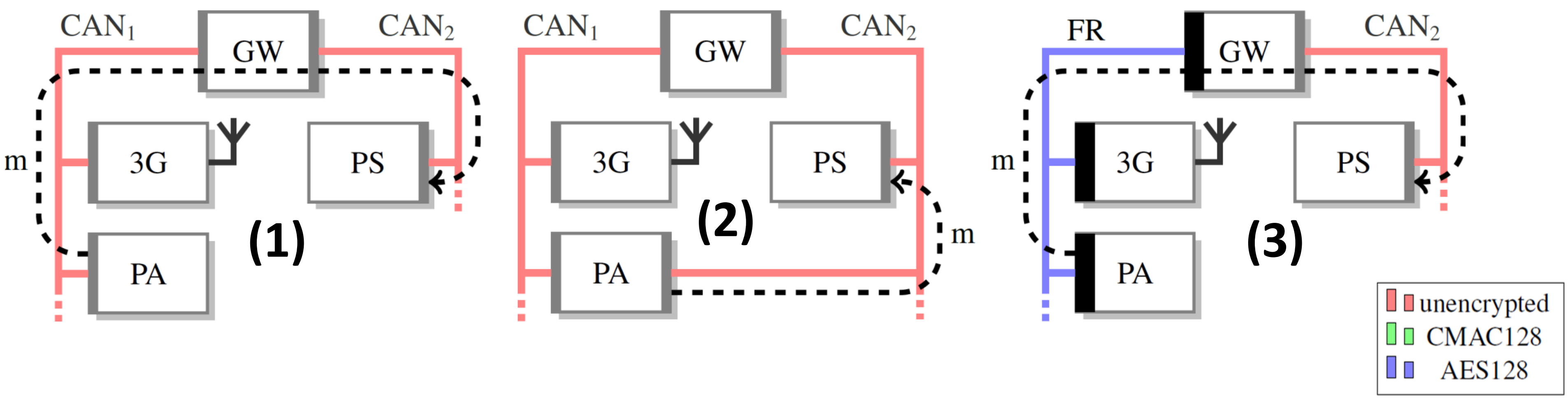
Properties

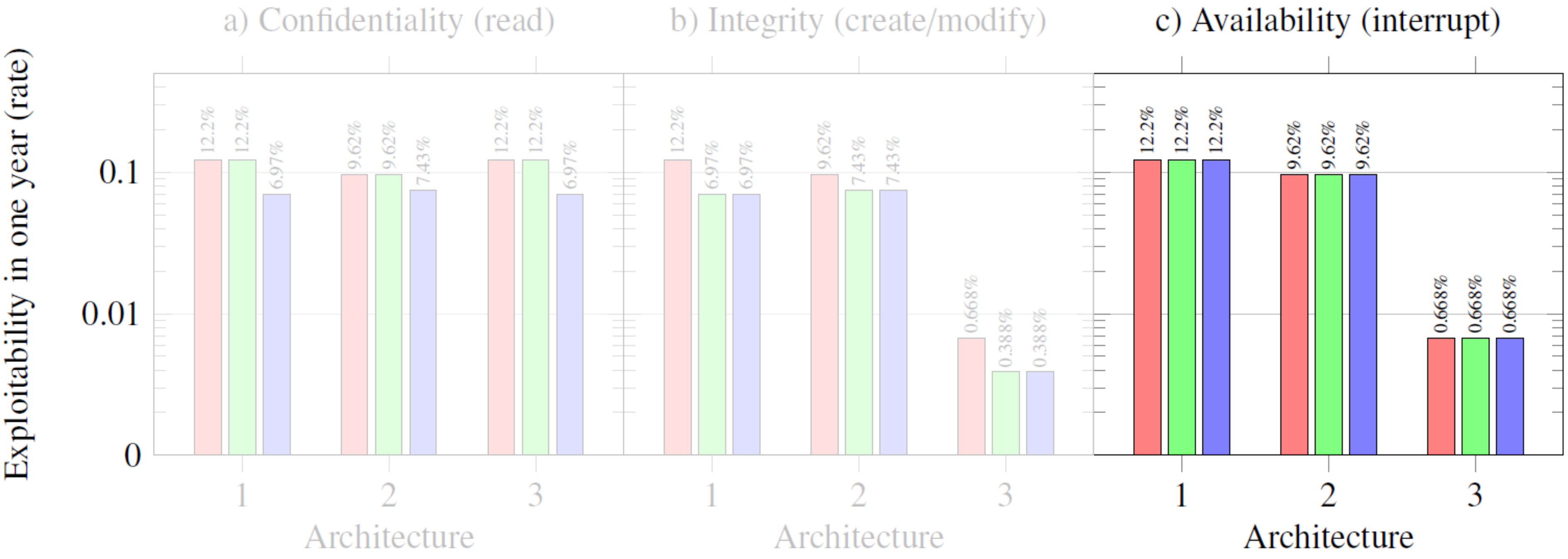
$P =? \; [F <= 1 \;\; x]$

Probabilistic Model Checking

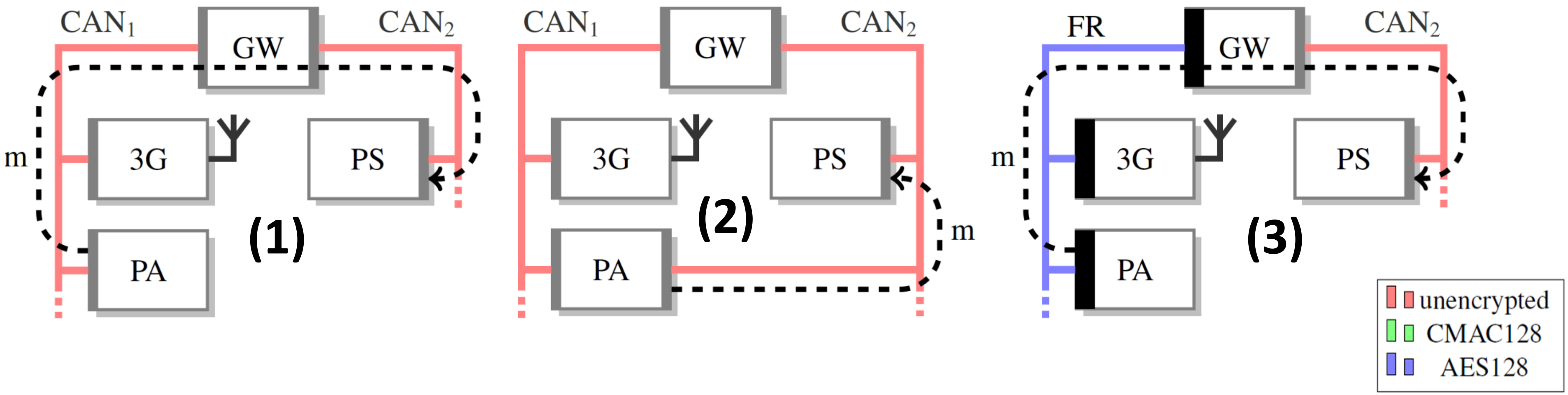
Results

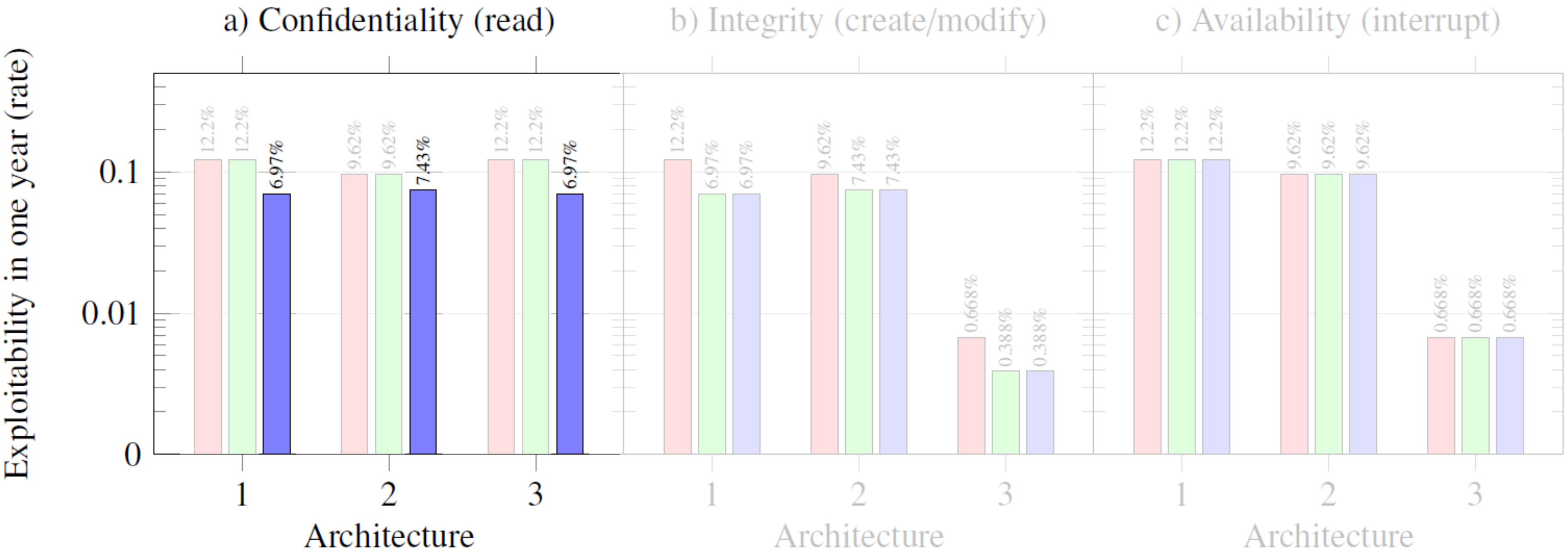
Architecture Security Analysis





Architecture Security Analysis





Summary

Summary

- **What** influence do component vulnerabilities have on the security of a specific function?

Summary

- **What** influence do component vulnerabilities have on the security of a specific function?

➔ Component influence on system can be quantified

Summary

- **What** influence do component vulnerabilities have on the security of a specific function?

➔ Component influence on system can be quantified

- Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?

Summary

- **What** influence do component vulnerabilities have on the security of a specific function?

→ Component influence on system can be quantified

- Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?

→ Comparison of architectures is enabled

Summary

- **What** influence do component vulnerabilities have on the security of a specific function?

➔ Component influence on system can be quantified

- Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?

➔ Comparison of architectures is enabled

- **How much** effort should be invested in the consideration of security during implementation of specific components?

Summary

- **What** influence do component vulnerabilities have on the security of a specific function?

➔ Component influence on system can be quantified

- Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?

➔ Comparison of architectures is enabled

- **How much** effort should be invested in the consideration of security during implementation of specific components?

➔ A quantifiable measure for security impact is given

Summary

- **What** influence do component vulnerabilities have on the security of a specific function?

➔ Component influence on system can be quantified

- Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?

➔ Comparison of architectures is enabled

- **How much** effort should be invested in the consideration of security during implementation of specific components?

➔ A quantifiable measure for security impact is given

Future work:

- increase scalability to full vehicle network

Summary

- **What** influence do component vulnerabilities have on the security of a specific function?

➔ Component influence on system can be quantified

- Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?

➔ Comparison of architectures is enabled

- **How much** effort should be invested in the consideration of security during implementation of specific components?

➔ A quantifiable measure for security impact is given

Future work:

- increase scalability to full vehicle network
- optimize security of architectures

Summary

- **What** influence do component vulnerabilities have on the security of a specific function?

➔ Component influence on system can be quantified

- Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?

➔ Comparison of architectures is enabled

- **How much** effort should be invested in the consideration of security during implementation of specific components?

➔ A quantifiable measure for security impact is given

Future work:

- increase scalability to full vehicle network
- optimize security of architectures
- synthesize new secure architectures

For more Information:

www.mundhenk.org