ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 5, No.17 , September 2015
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

On end-to-end safety for mobile COTS devices

Markus Kucera
[1] OTH Regensburg Technical University of Applied Sciences
Regensburg, Germany
Markus.kucera@oth-regensburg.de

Abstract

Today, ubiquitous mobile devices have not only arrived but entered the safety critical domain. There, systems are about to be controlled where human health or even human life is put at risk. For example, in automation systems first ideas surface to control parts of the system via a COTS smartphone. Another example is the idea to control the autonomous parking function of a car via a COTS smartphone too. As beneficial and convenient these ideas are on the first thought, on the second thought, dangers of these approaches become obvious. Especially in case of failures the system's safety has to be maintained. The open question is how to achieve this mandatory requirement with COTS components, e.g. smartphones that are not developed following the development process necessary for safetycritical systems.
This paper presents a concept to reliably detect human interaction while activating safety critical functions via COTS mobile devices. Thus a means is provided to detect erroneous activation requests for the safetycritical function.

Keywords: *Safety, Smartphone, Automotive, Control.*

1. Introduction

The basic idea when combining safetycritical systems with COTS systems is to make use of the advantages of the COTS domain. These are mainly reduced cost and standardization, which is expected to contribute in a great way to reduce the problem of complexity e.g. in the automotive domain [1,2].
The major problem using COTS devices for safetycritical systems origins from the fundamentally different approach these systems are designed and developed. Mobile COTS systems being designed for the mass market are easy to adapt and change – safetycritical systems are typically designed for one specific application with exactly specified safetyfunctions (functions that achieve or maintain the equipment under control in a safe state). Therefore, safetycritical systems are typically closed systems, whereas mobile COTS systems are typically open systems where changes and adaptions can easily be carried out.
To open safetycritical systems leads to problems, prominent examples are in the security area. Security issues and especially security violations that might lead to dangerous behavior of a safetycritical system are being published more and more [3,4,5].
This paper presents a concept to reliably detect human interaction while activating safetycritical functions via COTS mobile devices. Thus a means is provided to detect erroneous activation requests for the safetycritical function.

Dependable control and data transmission is the foundation in today's safety critical systems. End-to-End protection is one state of the art measure [6] to ensure the required safety for a given application. This is usually done by means of a special protocol implemented on all communication parties involved. However, this approach requires correct and controlled access on all communication endpoints. For that purpose these endpoints are often specially developed dedicated controllers.
As stated above, there is a trend to benefit from COTS mobile devices also in safety related systems. One example from the automotive domain is the autonomous parking function. This function parks the car autonomously with the driver outside of the car merely as a supervisor to start and stop the procedure. If this function was activated and deactivated via a COTS smartphone this phone became part of the safety critical system. To implement this functionality in an open system like a smartphone - following the mandatory safety standards is currently being worked on, e.g. Bosch proposes a solution as follows "You'll simply get out of the car in front of the parking spot, open the Bosch app on your cell phone, and press and hold a button to start the parking maneuver. The vehicle will then drive itself into – and back out of – the spot without anyone at the wheel. To abort the parking maneuver, you simply take your finger off the button." [7].
Other functions from the automotive domain are e.g. [8-13].
Also in the automation and control domain ideas surface and first solutions are proposed [14].

In Figure 1 the initial scenario is depicted. An end-to-end protocol (triangle) is implemented on the mobile device and the safety critical system.

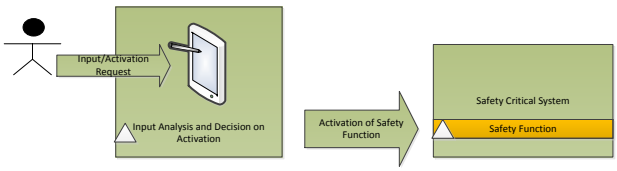

Fig. 1 Initial Situation and Control Flow

2. Critical Scenario

The critical scenario arises in case of an unwanted activation of the safetycritical function (e.g. because of a software fault). It is assumed that this function's safe state is the "not activated" state. As a consequence of this unwanted activation, danger for health and/or life manifests. Since the cause of the unwanted activation is assumed to be above the end-to-end protocol protection this type of failure cannot be controlled by this mechanism in the traditional way. Figure 2 shows the described situation where the failure gets through the end-to-end protection. It becomes apparent that end-to-end protection has to be extended to the front end, i.e. the system's user.

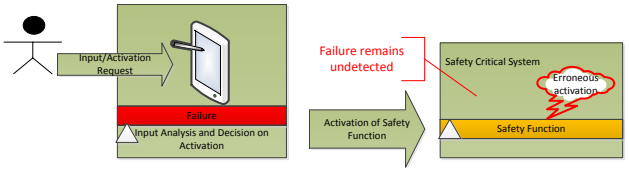

Fig. 2 Failure overcomes end-to-end protection

3. Concept

The proposed concept is consequently placed on the system's top layer thus extending the end-to-end protection to the user. In order to keep the safetycritical function activated the user's activation request is checked dynamically for plausibility by ensuring the continued human interaction with the device. For this purpose the user has to follow predefined screenpatterns while the safetycritical function is being carried out. These patterns are generated by the safetycritical system or offline calculated and stored within the safetycritical system. The user's movements are transmitted to the safetycritical system, which accepts or rejects these. Since the system's safe state is "not activated", it is therefore easy to maintain the safety as soon as the user's movements are outside a window of tolerance.

The suggested concept extends the concept of a dead man's switch or a watchdog timer with a further dynamic aspect. It is not sufficient to periodically activate the function via a pushbutton. The dynamic activation has to prove with sufficient probability for the mobile device that there is a human being behind it.

By having the user to follow predefined patterns originating from the safetycritical system it can be ensured that

- the user's activation request and it's continuation is a conscious one
- the unwanted activation (e.g. because of a software fault) can be prevented, provided that the system's reaction time is sufficient

In Figure 3 the proposed solution is given.

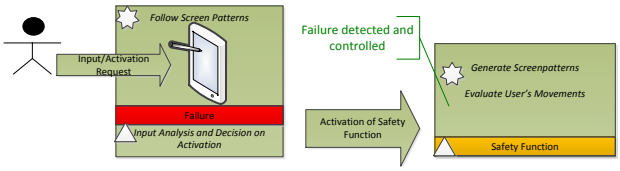

Fig. 3 Proposed solution

4. Conclusions and Future Work

This paper presents a concept to reliably detect human interaction while activating safetycritical functions via COTS mobile devices. The gap between the COTS domain and the domain of safety critical systems is closed by extending the classical end-to-end approach to the system's user.

Future work will concentrate on other biometric information that could be used in order to reliably detect a human being. Experiments will demonstrate how easy such biometric information can be obtained in today's most common mobile operating systems i.e. Android and IOS. For example the fingerprint sensor API of both operating systems unfortunately does not provide information on finger movement or micro movement yet. Such information could be already enough to reliably detect a human being without the need for further pattern generations. However, metrics have to be developed to quantify the value of reliable detection in order to decide on the method for the respective application under development.

References

[1] Di Natale, M.; Sangiovanni-Vincentelli, A.L., "Moving From Federated to Integrated Architectures in Automotive: The Role of Standards, Methods and Tools," in Proceedings of the IEEE , vol.98, no.4, pp.603-620, April 2010.

[2] Reinhardt, D; Kucera, M.; "Domain Controlled Architecture - A New Approach for Large Scale Software Integrated Automotive Systems", in International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS 2013), pages 221 – 226, February 2013.

[3] Jones, R.A.; Nguyen, T.V.; Horowitz, B.M., "System-aware security for nuclear power systems," in Technologies for Homeland Security (HST), 2011 IEEE International Conference on , vol., no., pp.224-229, 15-17 Nov. 2011.
[4] Shin, S., "Activities for Control System Security in Japan," in SICE Annual Conference (SICE), 2012 Proceedings of , vol., no., pp.667-669, 20-23 Aug. 2012.
[5] Chen, T.M.; Abu-Nimeh, S., "Lessons from Stuxnet," in Computer , vol.44, no.4, pp.91-93, April 2011.
[6] ISO 26262:2011(en) "Road vehicles — Functional safety", International Standardization Organization, 2011.
[7] Bosch Global (2015). "Fully automated parking", available at http://www.bosch.com/en/com/boschglobal/automated_driving/technology_for_greater_safety/pagination_1.html.
[8] Wong Hwee Ling; Woo Chaw Seng, "Traffic sign recognition model on mobile device," in Computers & Informatics (ISCI), 2011 IEEE Symposium on , vol., no., pp.267-272, 20-23 March 2011.
[9] Chiung-Yao Fang; Wei-Hong Hsu; Chung-Wen Ma; Sei-Wang Chen, "A vision-based safety driver assistance system for motorcycles on a smartphone," in Intelligent Transportation Systems (ITSC), 2014 IEEE 17th International Conference on , vol., no., pp.328-333, 8-11 Oct. 2014.
[10]Pritt, C., "Road sign detection on a smartphone for traffic safety," in Applied Imagery Pattern Recognition Workshop (AIPR), 2014 IEEE , vol., no., pp.1-6, 14-16 Oct. 2014.
[11]Akhtar, N.; Pandey, K.; Gupta, S., "Mobile Application for Safe Driving," in Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on , vol., no., pp.212-216, 7-9 April 2014.
[12]Kyungwon Chang; Byung-Hun Oh; Kwang-Seok Hong, "An implementation of smartphone-based driver assistance system using front and rear camera," in Consumer Electronics (ICCE), 2014 IEEE International Conference on , vol., no., pp.280-281, 10-13 Jan. 2014.
[13]Yu-Hua Yen; Chih-Li Huo; Tsung-Ying Sun, "Adaptive lane departure warning system on Android smartphone," in Consumer Electronics - Taiwan (ICCE-TW), 2014 IEEE International Conference on , vol., no., pp.67-68, 26-28 May 2014.
[14]Achkar, R.; Haidar, C.A.; Makhoul, N.; Osseili, H., "Gas ascertainment via smartphone," in GCC Conference and Exhibition (GCC), 2013 7th IEEE , vol., no., pp.220-224, 17-20 Nov. 2013.

Markus Kucera received his PhD degree in 1999 from Vienna Technical University. After several years in the automotive industry he became professor at the OTH Regensburg Technical University of Applied Sciences in 2004. His research interests include real-time systems, dependable systems and automotive systems.