Number 106 July 2016

ERCIM NEWS

www.ercim.eu

Special theme:

Cyber-Security

Also in this issue:

Cyber-Physical Systems: Closing the Gap between Hardware and Software

by Marcel Caria, TU Braunschweig

SHARCS (Secure Hardware-Software Architecture for Robust Computing Systems) is defining new ways to create more secure and trustworthy ICT systems.

We are currently witnessing a tremendous expansion of computerisation – of 'smart' entities and devices – in multiple new areas, such as health care (smart medical implants), automotive (smart cars), urban development (smart cities), power supply (smart grids), and others. This development is inevitably leading society as a whole, and the individuals within it, to increasingly rely on critical applications that sense and control systems in our physical environment. These 'cyber-physical' systems (CPS) use a blend of embedded devices and traditional computing systems, and a variety of communication channels. Our increasing reliance on these systems necessitates improved security [1].

The SHARCS project [L1] aims to establish new and secure-by-design CPS strategies. The intended solutions are supposed to be platform-agnostic, and may also be applied to virtualised environments, such as clouds and other (more traditional) ICT systems. The project started last year with four academic and three industrial partners: Foundation for Research and Technology – Hellas (Greece), Vrije Universiteit Amsterdam (Netherlands), Chalmers University of Technology (Sweden), Technische Universität Braunschweig (Germany), Neurasmus BV (Netherlands), OnApp Limited (UK), IBM – Science and Technology LTD (Israel), and Elektrobit Automotive GmbH (Germany). The project started in January 2015 and has a duration of three years with final outcomes being available in early 2018.

The current approach in security research (as well as in existing security solutions) is largely top-down and demand driven. Security-critical applications, software components, services or protocols (whether known to be vulnerable or not) are protected with piecemeal security tools and patched on demand. Attackers often try to bypass strong protection by redirecting their attacks to software layers below the seemingly strong defensive mechanisms.

Regarding these layers as a chain of software components makes it evident that a system is as secure as its weakest link. Thus, for a system to really be secure, all layers of the software stack must provide the same level of security. In other words: applications, compilers, libraries, drivers, hypervisors, and the operating system, must all be hardened, which may still be insufficient, considering the hardware layer below. We propose that the hardware itself must be secured and enabled to provide the appropriate primitives and capabilities for all the software layers built on top.

SHARCS aims to address the above problems by pushing security mechanisms down the system stack, from software to hardware, which is not only known to be much harder to bypass, but also improves performance, simplicity, and power usage. The three planned operational models (see Figure 1) are: New security functions are ideally pushed to the hardware level (left hand side). However, modifying all levels is not always possible, therefore we provide two more relaxed models. The one shown in the middle requires no hardware changes and all features are communicated to a commodity processor (x86 or ARM) using a hypervisor. The other one (on the right hand side) implements no features at the CPU, and there

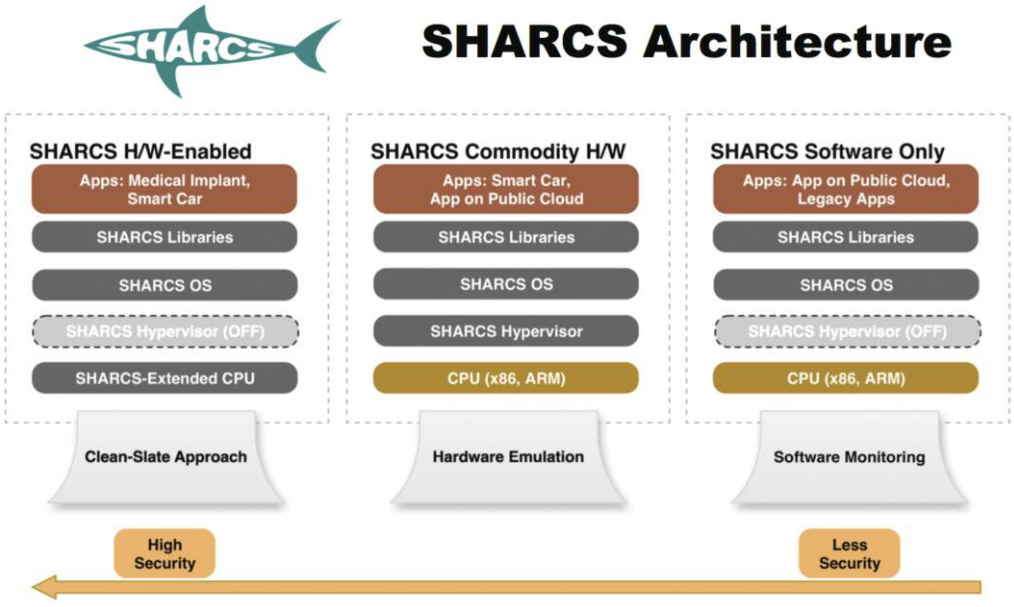

Figure 1: The three planned operational models in SHARCS.

is also no hypervisor available. To realise this last model, we link the application with SHARCS libraries and add kernel modules to the OS, which embed code for reliable and secure monitoring of applications at run-time.

The implementation of core security functions in hardware is one of the central project goals. Techniques like Instruction Set Randomization, Control-Flow Integrity (CFI) [2], and Dynamic Information Flow Tracking will be combined and implemented in hardware, and then supported by the higher (software) layers of the framework. However, security for legacy applications must be provided through security extensions (such as CFI enforcement), which we plan to develop as an integral part of our framework. These extensions should be usable in a transparent fashion, even with proprietary binaries, which will, however, require network requests and assistance from the application's vendor. We thus expect that not all legacy applications will benefit from our framework.

We expect the technologies designed and built in SHARCS to be finally deployed on a very diverse set of security-critical applications. We, therefore, plan to develop an evaluation methodology to assess all security benefits of our framework that have direct security gains in each application domain. This benchmark will also take into account the resource requirements of the examined security features, as well as their typical performance and energy overheads. We consider a security framework's platform independence as vital for its broad employment, which is why we aim to demonstrate SHARCS' universal applicability through the deployment in three real-world use cases: i) a secure, implantable neuromodulator for automatic seizure prevention, ii) secure application execution in an untrusted public cloud environment, and iii) a secure Electronic Control Unit for automotive applications.

Link: [L1] http://sharcs-project.eu

References:

[1] B. Schneier: "The Internet of Things Is Wildly Insecure-And Often Unpatchable", Wired Magazine, January 6, 2014

[2] V. van der Veen, et al.: "Practical Context-sensitive CFI", in Proc. of the ACM Conference on Computer and Communications Security (CCS), Denver, Colorado, US, 2015.

Please contact:

Sotiris Ioannidis, FORTH-ICS, Greece
+30 2810391945
sotiris@ics.forth.gr

ERCIM
European Research Consortium for Informatics and Mathematics

ERCIM – the European Research Consortium for Informatics and Mathematics is an organisation dedicated to the advancement of European research and development, in information technology and applied mathematics. Its member institutions aim to foster collaborative work within the European research community and to increase co-operation with European industry.

ERCIM is the European Host of the World Wide Web Consortium.

Consiglio Nazionale delle Ricerche
Area della Ricerca CNR di Pisa
Via G. Moruzzi 1, 56124 Pisa, Italy
http://www.iit.cnr.it/

Norwegian University of Science and Technology
Faculty of Information Technology, Mathematics and Electrical Engineering, N 7491 Trondheim, Norway
http://www.ntnu.no/

Centrum Wiskunde & Informatica
Science Park 123,
NL-1098 XG Amsterdam, The Netherlands
http://www.cwi.nl/

SBA Research gGmbH
Favoritenstraße 16, 1040 Wien
http://www.sba-research.org/

Fonds National de la Recherche
6, rue Antoine de Saint-Exupéry, B.P. 1777
L-1017 Luxembourg-Kirchberg
http://www.fnr.lu/

SICS Swedish ICT
Box 1263,
SE-164 29 Kista, Sweden
http://www.sics.se/

FWO
Egmontstraat 5
B-1000 Brussels, Belgium
http://www.fwo.be/

F.R.S.-FNRS
rue d'Egmont 5
B-1000 Brussels, Belgium
http://www.fnrs.be/

Spanish Research Consortium for Informatics and Mathematics
D3301, Facultad de Informática, Universidad Politécnica de Madrid
28660 Boadilla del Monte, Madrid, Spain,
http://www.sparcim.es/

Magyar Tudományos Akadémia
Számítástechnikai és Automatizálási Kutató Intézet
P.O. Box 63, H-1518 Budapest, Hungary
http://www.sztaki.hu/

Foundation for Research and Technology – Hellas
Institute of Computer Science
P.O. Box 1385, GR-71110 Heraklion, Crete, Greece
http://www.ics.forth.gr/

University of Cyprus
P.O. Box 20537
1678 Nicosia, Cyprus
http://www.cs.ucy.ac.cy/

Fraunhofer ICT Group
Anna-Louisa-Karsch-Str. 2
10178 Berlin, Germany
http://www.iuk.fraunhofer.de/

University of Southampton
University Road
Southampton SO17 1BJ, United Kingdom
http://www.southampton.ac.uk/

INESC
c/o INESC Porto, Campus da FEUP,
Rua Dr. Roberto Frias, nº 378,
4200-465 Porto, Portugal

Universty of Warsaw
Faculty of Mathematics, Informatics and Mechanics
Banacha 2, 02-097 Warsaw, Poland
http://www.mimuw.edu.pl/

Institut National de Recherche en Informatique et en Automatique
B.P. 105, F-78153 Le Chesnay, France
http://www.inria.fr/

Universty of Wroclaw
Institute of Computer Science
Joliot-Curie 15, 50–383 Wroclaw, Poland
http://www.ii.uni.wroc.pl/

I.S.I. – Industrial Systems Institute
Patras Science Park building
Platani, Patras, Greece, GR-26504
http://www.isi.gr/

VTT Technical Research Centre of Finland Ltd
PO Box 1000
FIN-02044 VTT, Finland
http://www.vttresearch.com