UNIVERSITÉ DU LUXEMBOURG

2nd Workshop on Security and Dependability of Critical Embedded Real-Time Systems

In conjunction with IEEE Real-Time System Symposium 2017, Paris, France

Important Dates

- Workshop submission deadline:
  1st October 2017 (aoe) extended and firm !!!
- Notification of acceptance:
  17th October 2017
- Final versions:
  20th October 2017
- Workshop:
  5th December 2017
- Main conference:
  6th - 8th December 2017

Proceedings

The full CERTS 2017 proceedings are available for download here.

Keynote

Dr. Matthias Schunter, Intel Labs

Principal Engineer, Intel Research Institute for Collaborative Autonomous and Resilient Systems

Vehicle to Cloud - Research Pillars for Secure Intelligent Vehicles

Abstract: Autonomous vehicles are datacenters on wheels, connected wirelessly to the Internet and to backend cloud services. This vastly increases the attack surface and the threat vectors we must face and mitigate. Our research focuses on three pillars to contribute: Secure platforms use hardware capability to protect the vehicle itself. 5G and V2X security pushes the limits on secure communication, and adversarial machine learning aims at increasing the robustness of today's machine learning algorithms.

Accepted Papers

Facing the Safety-Security Gap in RTES: the Challenge of Timeliness

Marcus Völp, David Kozhaya and Paulo Esteves-Verissimo

Safety-critical real-time systems, including real-time cyber-physical and industrial control systems, need not be solely correct but also timely. Untimely (stale) results may have severe consequences that could render the control system's behaviour hazardous to the physical world. To ensure predictability and timeliness, developers follow a rigorous process, which essentially ensures real-time properties a priori, in all but the most unlikely combinations of circumstances. However, we have seen the complexity of both real-time applications, and the environments they run on, increase. If this is matched with the also increasing sophistication of attacks mounted to RTES systems, the case for ensuring both safety and security through aprioristic predictabil-ity loses traction, and presents an opportunity, which we take in this paper, for discussing current practices of critical real-time system design. To this end, with a slant on low-level task scheduling, we first investigate the challenges and opportunities for anticipating successful attacks on real-time systems. Then, we propose ways for adapting traditional fault- and intrusion-tolerant mechanisms to tolerate such hazards. We found that tasks which typically execute as analyzed under accidental faults, may exhibit fundamentally different behavior when compromised by malicious attacks, even with interference enforcement in place.

IDHCC: A Security-Enhanced ID Hopping CAN Controller Design to Guarantee Real-Time

Wufei Wu, Ryo Kurachi, Gang Zeng, Yutaka Matsubara, Hiroaki Takada, Renfa Li

Controller Area Network (CAN) is the most widely used protocol for safety critical applications in current vehicle electronic systems. The security enhancement of CAN is a multi-constrained and cost-sensitive optimization problem, our aim is to propose a real-time and security mechanism. First of all, we propose a novel ID (identify) hopping CAN (IDH-CAN) mech-anism to address both security and safety constraints. Second, to improve the security performance of CAN, we design and implement the IDH-CAN controller (IDHCC) on FPGA, which works as a hardware firewall in the data link layer to isolate the applications from the physical layer. Third, our simulation and practical evaluations demonstrate the effectiveness of this approach in defense reverse engineering, targeted DoS and replay attacks without violating design constraints and highlight the importance of considering security together with other metrics during the design stages for automotive real-time applications.

A Byzantine Fault-Tolerant Key-Value Store for Safety-Critical Distributed Real-Time Systems

Malte Appel, Arpan Gujarati, and Björn B. Brandenburg

From modern cars to airplanes to industrial plants, many applications that must execute in a timely manner are deployed on distributed systems. In case of safety-critical applications, like the anti-lock braking system of a car, the underlying sys-tem must tolerate inadvertent environmentally-induced faults to guarantee user safety. Since such systems often operate at high frequencies, fault-induced failures have to be masked through active replication. Furthermore, before such a system is

deployed, it typically has to be analyzed w.r.t. its runtime, safety guarantees, etc. This is required for common safety-certification standards such as the DO-178C standard for aviation or the ISO 26262 standard for automotive systems.

To ease the development of such systems, our goal is to design a fault-tolerant middleware on which real-time control applications can be effortlessly replicated, that respects real-time and low-latency requirements, and whose reliability can be analyzed a priori for the purpose of safety certification.

Lower-Bounding the MTTF for Systems with (m, k) Constraints and IID Iteration Failure Probabilities
Arpan Gujarati, Mitra Nasri, and Björn B. Brandenburg

We derive a sound lower bound on the mean time to failure of periodic systems with (m, k) constraints. We assume that upper bounds on the failure probabilities of each system iteration, e.g., a job or a runtime activation of a periodic task, or a single actuation cycle of a control loop, are known and that they satisfy the IID assumption. Our analysis leverages prior work on the well-studied a-within-consecutive-b-out-of-c:F system model.

SEEDSTRAINER: An Approach to Improve the Hit Ratio of Malicious Candidate URLs
Yasuyuki Tanaka, and Atsuhiro Goto

Currently, increasing Internet use is plagued by malicious activity; drive-by download attacks have become a particularly serious problem. To counter these malicious sites, blacklisting is widely used as a multilayer defense mechanism in modern Internet security techniques. Blacklisting on network side is especially effective for protecting critical embedded systems or Internet of thing devices because it is not necessary to change the configuration or to use system resources for protection. To make an accurate blacklist, it is necessary to check malicious candidate Uniform Resource Locators (URLs), for example, using client honeypots. Because there are numerous malicious candi-date URLs and limited crawling resources, efficient crawling is necessary. In this paper, we propose SEEDSTRAINER, an approach that improves the efficiency of crawling. SEEDSTRAINER creates high-hit-ratio malicious candidate URL lists using open feeds, open intelligence, and machine learning. With SEEDSTRAINER, the hit ratio was improved by 12.5 times. In addition, we reveal the type of information distributed and the update statuses of various open feeds.

Sponsors

Advertisement

This year, Ada Europe 2018 features a special session on Security in Safety-Critical Systems, welcoming papers on Software and System Aspects of Secure and Dependable CPS, Vulnerabilities and Protective Measures for Safety-Critical System Infrastructures, and Fault and Intrusion Tolerance and Long-Term Unattended Operation for Safety-Critical Systems (not neccessarily only those that are related to Ada).

Conference Webpage: Ada Europe 2018

Call for Papers

Themes

At their heart, many critical systems and system infrastructures are composed of real-time and embedded systems (RTES). For example, RTES control our power grids, maintain our smart homes, steer our vehicles or they host the software in road-side units that allow our vehicles to drive more safely and more efficiently. For sure, they will open the way to even more challenging applications, such as in autonomous and cooperating vehicles, terrestrial or aerial.

However, most of these RTES are distributed or networked, which makes them vulnerable both to accidental faults and targeted attacks and advanced and persistent threats. Worse, compromise of a few nodes may bring down the entire system, in particular if attacks persist.

The grand challenges brought in by these scenarios include ensuring continuous unmaintained operation under faults and attacks. Systems may possibly utilize easier to upgrade computation resources in mobile phones or road side units whose trustworthiness needs to be established while the RTES approaches these units. And while attackers may try to compromise the RTES' functionality or timing, we seek to protect the integrity and timeliness of systems and the privacy of their users. Mastering these challenges requires the expertise of several research areas, and so, the goal of this workshop is to bring together researchers and engineers from the security and dependability, distributed systems and real-time communities, in order to discuss and promote new and exciting research ideas and initiatives, and to identify and discuss the challenges that lie ahead for such critical applications.

CERTS' 17 strives for an inclusive and diverse program and solicits short and long technical papers on open problems, experiments, case studies, new ideas, or future challenges.

Scope and Topics of Interest

CERTS' 17 is open to all topics at the intersection of security and dependability of embedded and real-time systems, with an emphasis on criticality and distribution. As such, areas of interest include but are not limited to the following topics:

- Security and dependability of cyber-physical and other real-time and embedded systems,
- Vulnerabilities and protective measures of CPS infrastructure,
- Fault and intrusion tolerant distributed real-time systems,
- Confidentiality and privacy in real-time and embedded systems, and
- System architectures encompassing combinations of distribution, security, dependability and timeliness.

Contribution formats include technical presentations of systems, system models and architectures, methods, tools, protocols and infrastructures to improve the dependability and security of real-time systems but also open problems and future challenges papers and experimental papers including experience reports and negative results.

Call for Papers

Download / View the Call for Papers (text version / pdf)

Submission Formats

- Short Work-in-Progress Paper: up to two pages, standard IEEE format
- Full Paper: up to six pages, standard IEEE format

Adherence to the format is strict, but we tolerate moderately exceeding the page limit (by up to two pages) if the content so justifies.

Paper Submission and Formatting Guidelines

Submitted papers must strictly follow the IEEE conference format (2 columns, 10 pt, single-line spacing, A4 paper) and should be submitted in PDF format.

LaTeX and MS Word templates may be found at: http://www.ieee.org/conferences_events/conferences/publishing/templates.html

All submissions will be peer-reviewed by the program committee.

Submission website: https://easychair.org/conferences/?conf=certs2017

Title Image: Benh Lieu Song (CC-BY-SA 4.0) original available here

Workshop Organizers

Marisol García Valls
Universidad Carlos III de Madrid
mvalls@it.uc3m.es

Sibin Mohan
University of Illinois
sibin@illinois.edu

Steering Commitee

Marcus Voelp
SnT - University of Luxembourg

Paulo Esteves-Verissimo
SnT - University of Luxembourg

Antonio Casimiro
University of Lisboa

Rodolfo Pellizzoni
University of Waterloo

Programm Committee

Lui Sha
University of Illinois

Christian Esposito
University of Naples Federico II

Hans Reiser
Universität Passau

Danny Dolev
The Hebrew University of Jerusalem

Antônio Augusto Fröhlich
Federal University of Santa Catarina

Zbigniew Kalbarczyk
University of Illinois

Miroslav Pajic
Duke University

Ravi Prakash
University of Dallas

Sasikumar Punnekat
Maelardalen University

Guillermo Rodriguez-Navas
Maelardalen University

José Rufino
Faculdade de Ciencias da Universidade de Lisboa