An Information Architecture Platform for Mobile, Secure, and Resilient Distributed Systems

Submitted by gabor on Tue, 04/22/2014 - 12:20pm. Contributors: Abhishek Dubey; William R. Otte; Gabor Karsai; Alessandro Coglio

Abstract:
Networked platforms such as fractionated spacecraft that perform surveillance and swarms of UAVs that monitor the ground represent a new class of cyber-physical systems (CPS). These CPS are formed from distributed cyber and physical resources that provide a dynamic and mobile platform where the required resources, including available network bandwidth and computing nodes of the network can change at any time during the mission. Moreover, these systems host several mission-specific distributed applications, possibly supplied and used by organizations with different credentials, that must operate at different levels of criticality, simultaneously. The benefit of these platforms is their ability to be reconfigured for different missions with distributed applications that are developed, reused, and operated by different stakeholders.

A number of challenges exist. First, the platform must be able to guarantee resource and performance isolation for applications that might be sourced from different suppliers and need to operate at different criticality and security levels concurrently. As an example, consider a cluster of satellites that execute distributed applications. One application is a safety-critical cluster flight application (CFA) that controls the satellite’s flight and responds to emergency commands. Running concurrently with the CFA, image processing applications utilize the satellites’ sensors and consume much of the CPU resource. Neither interference through shared computing and network resources nor information leakage between these applications is permitted due to safety and security concerns.

Additionally, the system must provide strong resilience guarantees that ensure that the application deployment will be effectively managed and rearranged if either critical resources in the system, either physical or cyber, fail or if the performance of shared resources such as the network degrades substantially. Furthermore, the design tools used to develop applications of these systems must be able to produce verified systems with designed-in security such that resource capacity and security violations are detected and addressed early in the development cycle.

This talk describes a distributed Information Architecture Platform (IAP) [1], [2] that was developed and prototyped under the DARPA System F6 Program. It consists of two parts: (1) a design-time toolsuite for modeling, analysis, synthesis, integration, debugging, testing, and maintenance of application software built from reusable components; (2) a run-time software platform for deploying, managing, and operating application software on a network of embedded, mobile nodes connected via an ad-hoc network. The platform reduces the complexity and increases the robustness of software applications by providing reusable technological building blocks in the form of an operating system, middleware, and application management services. The talk will specifically focus on the key security concepts that have been designed into the platform and on how the platform guarantees strict resource isolation between applications.

The IAP implements a complete, end-to-end solution for software development: from modeling tools, which provide a design environment and support early analysis of software applications to identify violations of information flow security and resource usage, to a robust distributed runtime platform. The runtime platform includes layers that implement the high-level communication abstractions: synchronous and asynchronous interactions and an operating system. The operating system, prototyped as a set of extensions to the Linux kernel - implements all the critical low-level services to support resource sharing (including robust spatial and temporal partitioning), distributed process management (including process migration), secure (i.e. labeled and managed) information flows, and fault tolerance. The other key feature of this platform is a novel kernel-level communication mechanism for providing secure information flows between processes called Secure Transport (ST). ST is a managed...
communications infrastructure that provides for datagram oriented exchange of messages between application tasks. ST restricts the transmission of datagrams according to both a communication topology according to a multi-domain multi-level Security (MLS) policy ([3], [4]), both of which are configured for each task by a trusted system administration infrastructure.

Acknowledgments: This work was supported by the DARPA System F6 Program under contract NNA11AC08C. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of DARPA. The authors thank Olin Sibert of Oxford Systems and all the team members of our project for their invaluable input and contributions to this effort.

References:

Speaker Bio:
Abhishek Dubey is a Research Scientist at Institute for Software Integrated Systems and an adjunct Assistant Professor at Vanderbilt University.

His research interests lie in the area of resilient cyber-physical systems. He received his Bachelors from the Institute of Technology, Banaras Hindu University, India in 2001, and received his M.S and PhD from Vanderbilt University in 2005 and 2009 respectively. He has published over 40 research papers and is a member of IEEE.

License: Creative Commons 2.5

Other available formats:

An Information Architecture Platform for Mobile, Secure, and Resilient Distributed Systems

Switch to normal viewer
Switch to experimental viewer

Architectures
Architectures
Critical Infrastructure
Resilient Systems
CPS Technologies
Distributed Applications
Information flow controls
Kestrel
Institute
Vanderbilt University
National HCSS Conference 2014
Academia Research Organization
Presentation
HCSS'14
Mobility (HCSS'14)