International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **2**, February **2010**

 ISSN 1349-4198
pp. **449–460**

A PORTABLE INTEGRATED AUTHENTICATION AND ACCESS CONTROL SCHEME FOR DISTRIBUTED EMBEDDED SYSTEMS

Yen-Cheng Chen[1] and Lo-Yao Yeh[2]

[1]Department of Information Management
National Chi Nan University
Puli, Nantou 545, Taiwan
ycchen@ncnu.edu.tw

[2]Department of Computer Science
National Chiao Tung University
Hsinchu 300, Taiwan
lyyeh@csie.nctu.edu.tw

Received August 2008; revised February 2009

Abstract. *Due to inherent resource constraints of embedded systems, it is a challenge to maintain an access control scheme for authorized users. In this paper, we propose a portable and lightweight authentication and access control scheme for embedded devices located in a distributed environment, where maintaining consistent access control among embedded devices is difficult. A portable list of accessible resources with privileges granted to a user is encrypted in the smart card issued to the user. Without pre-configuring access control information, an embedded system can effectively authenticate a user and determine user privileges. In addition to specific features for distributed embedded systems, the proposed scheme provides many advantages over previous approaches, in terms of implementation cost, access control facility, and security protection.*
Keywords: Access control, Authentication, Embedded systems, Security

1. **Introduction.** As the increased demand for low-cost and compact devices in information and communications technology (ICT), embedded systems thrive up to be one part of our life [3,22]. In addition to traditional ICT applications, examples of embedded systems can be found in information appliance, home electronics, or consumer electronics. As indicated in [11,17,20,24], embedded devices are getting increasingly connected and involved in network communications, and the security of data transfer and access to embedded devices should be protected. For example, a university may install wireless printers in its campus to provide ubiquitous printing services. If no security facility is imposed on these services, these resources may be abused and malicious eavesdropping may also be carried out easily. The situation stems partially from the lack of authentication and access control. User authentication and access control of networked systems has been studied for years. Indeed, a number of authentication and access control schemes have been proposed [5,7-10,14,18,19]. Most of them were developed without taking into consideration the inherent limitation of embedded systems. Embedded systems have strict limitation in storage space and processor capability. Authentication and access control on such resource-limited devices should be implemented with a modest overhead. In addition, embedded systems usually have restriction on user interface and configuration flexibility. It is not easy to perform configurations on embedded systems. In many applications, embedded systems are deployed in a physically and organizationally distributed environment [1,2,9] to provide services to users, e.g. the ubiquitous printing service in a campus. It is a new challenge to conquer the scalability issues in terms of number of embedded