Chapter 7.15
Secure Authentication Process for High Sensitive Data E–Services:
A Roadmap

Claudio Agostino Ardagna
University of Milan, Italy

Ernesto Damiani
University of Milan, Italy

Fulvio Frati
University of Milan, Italy

Salvatore Reale
Siemens Mobile Communication S.p.A., Italy

EXECUTIVE SUMMARY

The widespread diffusion of online services provided by public and private organizations, firstly driven by e-commerce and more recently by e-government applications, has stressed the need of secure ways to authenticate users who need to access online resources. The huge number of resources accessible on the Web leads to different authentication mechanisms implementations that often require multiple log-on actions also in intradomain multiservices scenario. In case of high sensitive services, users' authentication plays a role of paramount importance. In this article is presented a case study that gives a roadmap of authentication mechanisms implemented at different levels of services' software structure. The discussion starts by illustrating different authentication solutions implemented at operating system, application server or components level to conclude with Single Sign-On approach. For each solution, pros and cons are discussed. The SSO system, called CAS++, developed as an extension to Yale University's CAS, is then presented.

ORGANIZATION BACKGROUND

Established in early July 2002, Siemens Mobile Communications S.p.A. (SMC) is involved in mobile networks (for Italy) and fixed and mobile network access systems (for the international market). It works in close collaboration with the Siemens AG Information and Communication Mobile group. The company is among the foremost research and development centers in the telecommunications industry, with a large percentage of its staff employed at the Cassina dè Pecchi and Cinisello Balsamo (Milan) premises. Manufacturing mainly takes place at the Marcianise plant (in the province of Caserta), as well as in Cassina.

Turnover for 2003–2004 came in at 1,171 million euros, with staff levels at 2,562.

Siemens Mobile Communications' business divisions are marked by their aggressively market-oriented approach and a commitment to excellence in partnerships with mobile operators – regardless of whether they are new or existing clients – in every area of telecommunications, fully capitalizing on the synergies offered by the Siemens Information and Communications group in Italy and internationally. The company comprises two business divisions:

- **Mobile Networks**: Siemens Mobile Communication proposes itself as one of the leading companies in the mobile communication market. Its products are made to answer in the better possible way to the requirements of the costumers. The infrastructure range includes technologies for GSM, GPRS e 3G systems. The processes of technological innovation realized by the research centers pose Siemens always at the highest level in the development of new technologies for the Mobile Network.
- **Microwave Networks**: Microwave Networks division has a lead-house role in Siemens with the mission of developing, manufacturing, promoting, selling, and supporting microwave and WiMAX products. Siemens offers innovative radio products and solutions for the transmission and access to the mobile and fixed networks thanks to the proven turn-key capability and world-wide presence.

SETTING THE STAGE

The increasing usage of GSM mobile phones and the upcoming of a new generation of mobile systems (called third-generation or 3G) have led to the development of applications that manage the mobile network and provide new services to users. In this scenario, every network technician, that has to use multiple parallel services, must manage several pairs username/password, raising a great amount of security concerns (Bettini, Jajodia, Sean Wang & Wijesekera, 2002). In particular, when the organization manages very sensitive data, the main problem that has to be addressed is the efficiency and security of the authentication process, the first point of contact between users and systems. Hence, in this scenario, the major challenges were to improve authentication process in order to avoid malicious accesses, privacy violations and data correlation. The importance of security mechanisms, in fact, arose when a solution for remote management had been adopted for simplifying and improving network management performances. In this scenario, the high sensibility of the information and the risks introduced by the adoption of remote services imposed to provide a strong solution to security issues.

The presented case study, named "Pitagora Project", is managed in the context of a joint research project that involved Siemens Mobile Communication S.p.A. and the Software Engineering and Advanced Architectures Group of the Department of Information Technology of Crema (DTI), University of Milan. This project, started in January 2004, is focused on security

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/secure-authentication-process-high-sensitive/9406

Related Content

Building Context-Aware E-Commerce Systems: A Data Mining Approach
Anahit Martirosyan, Thomas Tranand Azzedine Boukerche (2010). *Encyclopedia of E-Business Development and Management in the Global Economy (pp. 1021-1029).*
www.irma-international.org/chapter/building-context-aware-commerce-systems/41265

SMEs Performance: Leveraging Marketing Process Through E-Business
Malliga Marimuthu, Azizah Omar, T. Ramayahand Osman Mohamad (2012). *International Journal of E-Business Research (pp. 49-66).*
www.irma-international.org/article/smes-performance-leveraging-marketing-process/66053

A Netnographic Analysis of Facebook Content Strategy of World's Top 10 Management Institutes
Anandan Pillaiand Kalpana Chauhan (2015). *International Journal of E-Business Research (pp. 1-17).*
www.irma-international.org/article/a-netnographic-analysis-of-facebook-content-strategy-of-worlds-top-10-management-institutes/132695

E-Banking Operational Risk Management using Soft Computing Tools
Rita E. Ochuko, Andrea Cullenand Daniel Neagu (2012). *Strategic and Pragmatic E-Business: Implications for Future Business Practices (pp. 176-202).*
www.irma-international.org/chapter/banking-operational-risk-management-using/66009

RFID Systems: Applications vs. Security and Privacy Implications
Dennis M.L. Wongand Raphael C.W. Phan (2007). *Web Services Security and E-Business (pp. 57-74).*
www.irma-international.org/chapter/rfid-systems-applications-security-privacy/31220