Information and Network System Security

FLORIN HARTESCU
Research and Development
National Institute for R&D in Informatics - ICI
8-10, Maresal Alex. Averescu Ave., Sector 1, Bucharest
ROMANIA
www.ici.ro
STEFAN-VICTOR NICOLAESCU,
INSCC, Bucharest,
ROMANIA
www.inscc.ro

Abstract : Today all the systems that manage the security are characterized by the complexity of their major functions like identification, authentication, access control and data protection. The implementation of these functions is usually and objectively based on a trusted model that uses a trusted architecture, which is the platform of the security architectures. The purpose of a such platform is to work on the trust IT infrastructures in all the steps of their life cycle from the design, as security and resilience, up to the operations when facing attacks and breakdowns. The approach is to automate and have a dynamic trust infrastructure that interacts automatically with the security infrastructure. So the authorisations, exceptions and more generally all the security management are done by the system itself. This is the goal of the trust platform we propose. The purpose is to go with and reinforce the security and resilience of the networks, IT infrastructure, systems and services. The trust models components :

- Definition of the trust itself: total, partial, delegated;
- Design of the various trust models (based on reputation, frequenting or surveillance, security or redundancy mechanisms) for systems, networks, services, hardware or software component, architecture,
- Specification of the protocols to install the trust,
- Definition of the parameters to measure the trust in real time in a system,
- Estimation of the trust by a user.

Key words : Information security, wireless, Wi-Fi network, IT infrastructure, SSL

1 Introduction

One of the enterprises problems is the lack of interoperability of software applications to manage and progress in their business. Enterprises are looking for new business relationships, and the exchange of information and documents with new partners often cannot be executed automatically or in and electronic format. This is primarily due to problems of incompatibility with the information representation adopted by the software applications they are working with.

The Open Source movement has developed new concepts of making business based on transparent and co-operative ownership of software. We can propose a system we can develop methods and tools to better match the results from the FLOSS (Free/Libre and Open Source Software) software designers community and potential users in collaborative networks in various businesses in an unprecedented way.

A conceptual model is an abstraction for computational realisation of a world of entities (e.g., physical, concept, relationship, method, constructor, fact, rule).

The proposed system could bring together relevant software and technology demonstration in this field and tackles the following issues:

1. Motivations and sustainable business models for open source software provision
2. Co-operative design models for authentication to various enterprise services
3. Developing and integration of mission critical applications for enterprises
4. Reference implementations for open groupware and multimedia archiving solutions
5. Simplification and visualization of FLOSS legal aspects and licensing

2 The system aims

The interoperability in enterprise can be defined as the ability of enterprise Software and Applications to interact.

The proposed system aims at a series of activities to apply this scheme to different types of business areas, especially for SMEs and NGOs in collaborative networks. The overall goal is to foster the usage of FLOSS backend platforms and services and to generate new business opportunities for the Open Source developer community. The open source-based set of tools is supposed to have a high socio-economic effect for both, the providers and users of FLOSS, with a special focus on SMEs. On the development side, the system could arrange around a few models, bringing experience and moderating integration to various end users.

Scientific and technological objectives and state of the art of the proposed system supports the migration of the business processes in enterprises and public organizations to use FLOSS. A number of FLOSS solutions are available for different purposes, however some elements are missing so that FLOSS can be used for supporting all day-to-day business tasks.

The Open Source movement has to tackle some obstacles, in order to be competitive with commercial closed license solutions. First, a few critical applications in the area of accounting, customer relation management or shared calendaring are not available or need major improvements. Secondly, many mature FLOSS applications, which are already used in offices, such as file sharing, forum, web mail, or web logs, usually have different user management schemes, which enforce the user to remember different user names and passwords.

3 General presentation

By splitting the application across three tiers, we are able to separate out the three logical components of the system : user interface, computational logic and data storage. Each logical unit can then be developed separately from the others, introducing an important degree of flexibility into the design of the application.

The open source-based set of tools provides a mechanism for tight integration of authentication schemes of various enterprise related applications to a commonly managed user base. The experience in ISP hosting business shows, that it is not wise, to give any user his own account to access different kind of services due to security risks. Instead, the product manages user accounts in a database and makes it available through various interfaces (including LDAP) and programming languages. This provides high flexibility for user and group management and minimizes the risk for exploits.

The proposed system will provide enterprises with reliable business applications, which seamlessly work together, and makes any office independent from closed source software.

The long-term impact of Open Source business applications is that it radically simplifies and standardizes servers in any companies big, medium or small data center. Because Linux runs as well on low-cost Intel as it does on high-reliability mainframes, Linux brings consistency and manageability to the data center. This makes Linux a key technology that will transform today's garbled, underutilized data center

into a highly automated resource built on cheap hardware components, an architecture named "Organic IT." Unlike today's data center, in which it can take months to deploy an application, an organic IT data center running Linux can deploy the same application in days.

The proposed system outlines a work programme and vision that leads to the development of:

- a framework platform for service deployment;
- an office server platform;
- tools to help developers build services and applications to be deployed on this integrated platform.

This is highly relevant to the strategic objective by producing open source components, by producing an integrated platform built using these components (to enable further innovation in the applications and services market), and by producing tools for designers to use to develop applications and services targeting this platform. A key feature of the platform is that is not simply an abstract middleware platform but an instantiation of such a platform in a real-world domain where there is a great demand for new innovative services (essentially hybrid Internet and office services potentially sharing resources from these two domains). At the heart of the system vision in this area is the use of IETF and W3C standards. The system sees this as being of relevance to all future business related services, especially those targeted at networking capabilities.

PHP Web applications for secured networks commonly make use of some objects to perform tasks such as connecting to databases or sending email. When moving websites between Web servers, it is critical to know which objects are used on the site, as it may be necessary to install these objects on the new web server or to rewrite the code. The system looks for the instantiation of such an objects through the use of the CreateObject and Server.CreateObject functions. The report produced by the system contains a list of the objects used.

The proposed system will use secure socket connections (SSL) to transmit all sensitive information during confidential process.

The system targets will cover three areas.

- Content engineering: is a cooperative task of experts in the domain of SMEs management and information specialists from the IT and multimedia domain. Their outputs are digital modules, consisting of the combination of the management methods, realized by advanced IT solutions.
- Platform engineering: generate the technical framework, supporting the management process and e-business. The platform engineering is based on available standards and methods and executed by integration of IT specialists and IT solutions.
- Business engineering: is a collaborative work, which integrate all the activities of the management and IT professional partners. The target of the business engineering is to offer new management solutions, via the modern methodology and technology.

The proposed system will use encryption and other security mechanisms to ensure that only authorized users can access the collaborative network and the data cannot be intercepted.

Information and network security can be understood as the ability of the network to resist at a certain level of safety, to accidental events or to malicious actions that may compromise availability, authenticity, integrity and confidentiality of stored or transmitted data and for offered or accessible services through the network.

Local wireless networks, particularly Wi-Fi networks (IEEE 802.11 standard) are very attractive for those who want quickly to develop a local, small access network for SME, SOHO of for premises. Such networks, generally with an ad-hoc configuration or, sometimes configured as small dimension mesh networks, offer a degree of mobility and accept nomadic work of customers. The costs of installation are remarkably cheaper as those for cabled networks. The costs of equipments can be well diminished when the number of equipments produced increases. That offers

wireless access networks many advantages compared with fixed access networks.

Nowadays the wireless networks have some disadvantages in comparison with cabled networks. The main disadvantage is given by the number of security threats which is greater than that for fixed, cabled networks. The fact that the radio transmission can be intercepted by non-authorized people can be a disadvantage for wireless networks. But nowadays the information in wired networks can also be accessed sometimes by non-authorized people.

The radio networks based on Ethernet and on the protocol set IEEE 802.11(Wi-Fi) are more and more becoming the preferred solution when implementing the LAN residential and enterprise infrastructures. This is primarily based on decreasing the Wi-Fi equipment prices (network interface cards, access points, routers, bridges). This tendency is sustained by important advantages brought by the radio technologies compared with those technologies requiring cable installation (mobility, shorter installation time and reestablishing the connection after a failure, easier to use, etc.). Another characteristic of these networks, attractive to both users and producers or providers, is the usage of bands which do not require licenses to use the radio frequencies (e.g. 5.7 GHz for IEEE 802.11a and 2.4 GHz for IEEE 802.11b and IEEE 802.11g).

The security of communication must be considered in the context of informatics security. The security problem in wireless networks can be put in such terms as to be not weaker as the security in wired networks. That means the security must be considered at protocols level and also at physical layer.

The wireless connection must be reliable at physical layer. The reliability may be assured by the possibilities offered by IEEE 802.11 standard to use different modulation types and coding. It is well known that the more robust modulation and coding offer the lower rate of transmission ant that must be considered in connection with offered service.

4 Security Vulnerabilities in Wi-Fi Networks

The solutions for security risks evaluation and minimization must be focused on the network and the organization that has it as a whole, no matter what their detailed structure is. This is a new approach of the security matter in the joint transmission support networks, being in total opposition with the traditional way based on isolated approach of different problems. This approach is mostly necessary in the mixed networks made of Wi-Fi technologies segments and cabled segments.

To implement a telecommunication secure system it is necessary to take into account:

- Security features considered as relevant for the system,
- Security objectives at the moment of the system design,
- Possible threats to the system,
- Methods and resources to implement/impose security in the system.

According ETSI ETR 237, the security characteristics of a wireless system are:

- Authentication,
- Confidentiality,
- Integrity,
- Availability, access control,
- Key administration,
- Non-repudiation,
- Security management.

Security features of the system are implemented through security mechanisms. According to ETSI ETR 232, a security mechanism is defined as an algorithm that implements a particular function of security in a physical equipment or a program. Security mechanism stands for the methods used to accomplish certain security features. Therefore, the security mechanism is a constitutive block in the construction process of a security feature.

The main types of threats on the security of Wi-Fi networks are:

- Passive surveillance;
- Unauthorized access;
- Denial of service, DoS;

- Man in the middle attacks;
- Unauthorized or incorrect configured access points;
- Network trespasses.

Passive surveillance consists in the interception of the data packets transmitted through unprotected wireless networks and the research of obtained information through adequate software instruments. This way, there can be found user identifiers and associate passwords, credit cards numbers, etc.

Unauthorized access consists in integration of a pirate client station through association with one of the access points in the network. This station can access servers or network applications. To counteract unauthorized access a mutual authentication between client station and access point is needed.

Denial of DoS, means that Wi-Fi network or station can be put out of function for an undefined time. A DoS attack can be obtained obstructing the function of equipments, for example by overflowing the network with a great number of packets or by creating strong interferences.

Man in the middle attacks consists in emplacement of a fictive client device between a legitimate client and wireless network. For that, the address conversion protocol, ARP usually used for TCP/IP networks, is used. The pirate station will receive the data packets, instead of the actual destination station.

Unauthorized or incorrect configured access points. In a wireless network, such access points may be easy inserted in the network. Such points may break unconscious or deliberately security politics.

Network trespasses, may be generated even by authorized clients, which may affect the network by an abusive use of the resources.

5 Security Techniques And Algorithms In Wireless Networks

Breaches in the security system of wireless networks can affect other parts of the system that can affect the database, as in any communication system, including Internet. Database's security is referring to the hardware and software elements, persons and data. It must be taken into consideration data security relatively to theft and fraud.

Theft and fraud of databases can be obtained by electronic means, breaking security of computers. The intruders may enter such databases and extract or modify data with consequences as confidentiality loss, privacy loss, integrity loss and availability loss. In the case of wireless networks, intruders may enter the system at air interface, by an access point.

The measures against computer system dangers differ from physic control elements to administrative procedure. Generally, a SGBD system security can be as good as the security of the operation system because of the tide link between them. Security in wireless access networks elements :

- Authorization;
- Safety and recovery copies;
- Integrity;
- Encryption.

Authorization means the permission given to a client to access in a system or to an object in a system, like files or folders.

Safety and recovery copies offer security against involuntarily or deliberate damages of files or data.

Integrity means integrity of transmitted data. In a digital communication network, the integrity may be lost by packet loss or by receiving of damaged packet data. Packets may be lost or damaged on propagation path or in the backhaul network.

Encryption must be sustained by encryption key, encryption algorithm and correspondently decryption key and algorithm. In the present approach, new text and image encryption algorithms must be projected and implemented using irreversible functions defined in Galois fields of different sizes and using programming language as C, C++, Java (to allow the movement of the programs on different application platforms).

In a wireless network, beside authorization authentication must be considered, in order

to prevent intrusion of a false client in the network.

6 Conclusion

Implementation of this system in Romanian firms has the following advantages: obtaining a high efficiency and time saving, limited efforts for developing a new secured application in a short period of time and high performance of the system in solving the demands for SMEs applications.

The system uses secure socket connections (SSL) to transmit all sensitive information during confidential process.

The application has been tested in an integrated system, with several servers running Windows 2000 and Linux, connected in a collaborative network. The system was configured easily, and it has worked very fast because the communication protocol transmits just the information needed.

The system targets cover three areas.

- Content engineering: is a cooperative task of experts in the domain of SMEs management and information specialists from the IT and multimedia domain. Their outputs are digital modules, consisting of the combination of the management methods, realized by advanced IT solutions.
- Platform engineering: generate the technical framework, supporting the management process and e-business. The platform engineering is based on available standards and methods and executed by integration of IT specialists and IT solutions.
- Business engineering: is a collaborative work, which integrate all the activities of the management and IT professional partners. The target of the business engineering is to offer new management solutions, via the modern methodology and technology.

The system uses encryption and other security mechanisms to ensure that only authorized users can access the collaborative network and the data cannot be intercepted.

References:

[1] Stefan-Victor Nicolaescu, Florin Hartescu, Information security in Wi-Fi networks, The 8th International Conference on Informatics In Economy, Informatics In Knowledge Society, Romania Bucharest, May 17-18, 2007

[2] W. Wang – Designing Secure Mechanisms for Online Processes

[3] Hauslein A., Page B., Knowledge-based Approaches to Modelling and Simulation Support. Systems Analysis, Modelling Simulation 8 (1991), 4/5, pp. 257-272.

[4] Nussbaumer H., Computer Communication Systems, John Wiley & Sons, 1990.

[5] Selic B., P.T. Ward: The Challenges of Real Time Software Design, Embedded Systems Programming, Miller Freemans Inc., Oct. 1996

[6] Tanenbaum S. A., Computer Networks, Prentice Hall.

[7] Stefan-Victor Nicolaescu, Catalin Muresan, Mihaela Ciurtin: “Sisteme de acces radio de banda larga, conforme standardelor IEEE 802.xx”, Ed. AGIR, Bucuresti, 2006.

[8] Stefan-Victor Nicolaescu, Catalin Muresan, Mihaela Ciurtin: “Retele radio de acces de banda larga”, Ed. AGIR, Bucuresti, 2005.

[9] Coordinators Ion Ivan, Cristian Toma: “Informatics Security Handbook”, Ed. ASE, Bucuresti, 2006.

[10] *** "Baseline security standards; Features and mechanisms", Security Techniques Advisory Group (STAG), ETSI ETR 237, November 1996.

[11] *** "Glossary of security terminology". Security Techniques Advisory Group; ETSI ETR 232.