Shared Applications in Heterogeneous Network Environments

Mgr. Roman Jasek, Ph.D.
Andras Chernel, DMS; DHA
Tomas Bata University in Zlm
Faculty of Management and Economics
jasek@fame.utb.cz, chernel @fame.utb.cz

Key Words:
Penetration detection, shared applications, systems security, systems interlinkage.

Annotation

This contribution describes the basic measures that are associated with the secure sharing of applications in general heterogeneous network environments (e.g. the Internet

The first section of this contribution explains the basic ways and means of securely connecting information systems (e.g. packet filters, applications gates, etc.)

The second section is devoted to the secure sharing of applications. The solutions discussed within it are based ion the tight integration of three fundamental pillars, or technical components. These are, access portals, address book services, and the so-called "Public (electronic) Key" infrastructure. The mutual inter-combination of these technical elements allows the secure sharing of various applications that support the standard interface on the basis of HTML and XML.

Introduction.

Modern information societies cannot no longer do without the widespread general exploitation of information and communications technologies. The need for increases in operational effectiveness coupled to the rapidly approaching ascension into the European Union require ever-higher degrees of the mutual integration of existing information systems that enable the across-the-board and secure sharing of (software) applications.

An integral requirement for the implementation of the qualitative linkage of new infrastructures is the management of all of their security attributes and implications. This contribution seeks to draw attention to certain basic security measures, which can be exploited in the course of connecting up information systems.

The secure interlinkage of systems

Contemporary information and communication systems are ever more based on the integrated collection, transmission, elaboration (processing), and sharing of information. This leads to greater demands being placed on the connection and integration of systems. With the rising "price" of information and the increasing dependence of organisations on the (correct - read secure) functioning of their information systems, there is a corresponding growth in the prerequisite needs for the complex assurance of their security.

The IDA - European (Electronic) Architecture.

A designated public body is working on an overall concept entitled *The Interchange of Data between Administrations* - **IDA** regarding the integration of information systems within the framework of the whole of the European Union. The basic thrust of this conception is the creation of a complex information environment that will enable the intensive and, at the same time, secure exchange of data (and this is equally the aim of so-called open technologies - which form the backdrop to, and at the same time, enable their exploitation for effective e-learning).

From a technical point of view, four levels of security measures distinguish this „architecture*[1]:

1 **Physical Security** - The basics of all security measures is always the sufficient protection of the physical integrity of all of the technologies used.

2 **Technical Security** - This is concentrated on the implementation of security measures in the individual technical elements of the information and communications systems.

3 Network Security - This is an integral component of the transmission service(s), and the measures used determine and ensure the security of the communications infrastructure(s).

4 Applications Security - This is determined by the enforcement of the security features and qualities of the individual information system's applications.

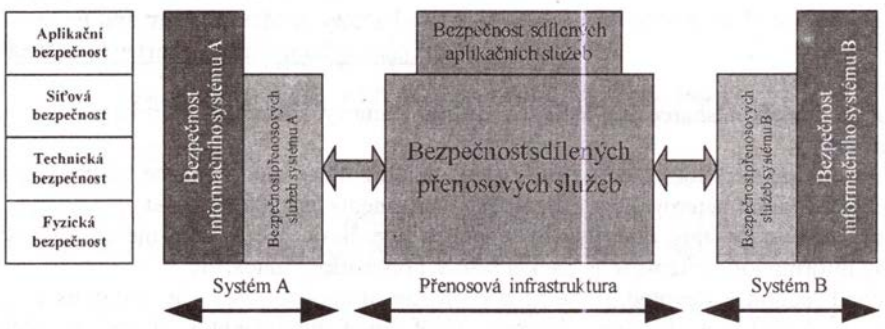


Fig. 1 Basic Conception of Security Architecture

The **IDA** Architecture understands security as being made up of a combination of management practices, a general awareness, and security policies within the context of the technology being used. This enables the creation of highly effective security systems. (In the Czech Republic) The organisational side of security issues are given by the *ČSN 1SO/IEC 17799: 2001 - Information Technology - Set of Approaches for the Management of Information Security* norms.

Network Security.

Secure connection requirements have their roots and origins in the commercial expansion and exploitation of the Internet network into every nook and cranny of the world. The reasons being the need to protect the relatively secure spaces of the internal system from attacks conducted through the medium of the totally unsecured Internet. This useful principle has, with the passage of time, gradually begun to be implemented even m more extensive networks, where above all, they separate the individual information systems with varying degrees of information security.

One of the first instruments to allow the secure connection of two media was the so-called "Firewall". This initially found its applications simply as a defensive interface with public networks; however, over a very short space of time, the firewall has found increasing applications and usage. Today, it is considered as the (most) basic tool for the secure connection of information systems.

The **Firewall** is a security device designed for the protection of one's internal information system against external attack. Firewalls can be divided into two basic types: packet filters and application(s) gates.

1 The Packet Filter is a device, which allows the management of networked operations on the basis of information (contained) in the heading of the packet (i.e. according to protocol type, network port(s) used, source and target addresses, etc.). A higher class of such types of devices are so-called **Transmission Control** Packet Filters, which are also able to analyse the data content and context of the use of the packet. The fundamental advantage of such solutions is their high performance and efficiency level while maintaining a relatively low price level.

2 The Application Gate is a device, which protects one while in direct communication contact between networks. Communication is enabled in that the application(s) gate maintains an individual interface for each and every application, which allows the transmission of data according to (pre-)defined rules. This solution provides a greater measure of security, (but) this is accompanied by a lower performance rate and higher cost of the requisite equipment.

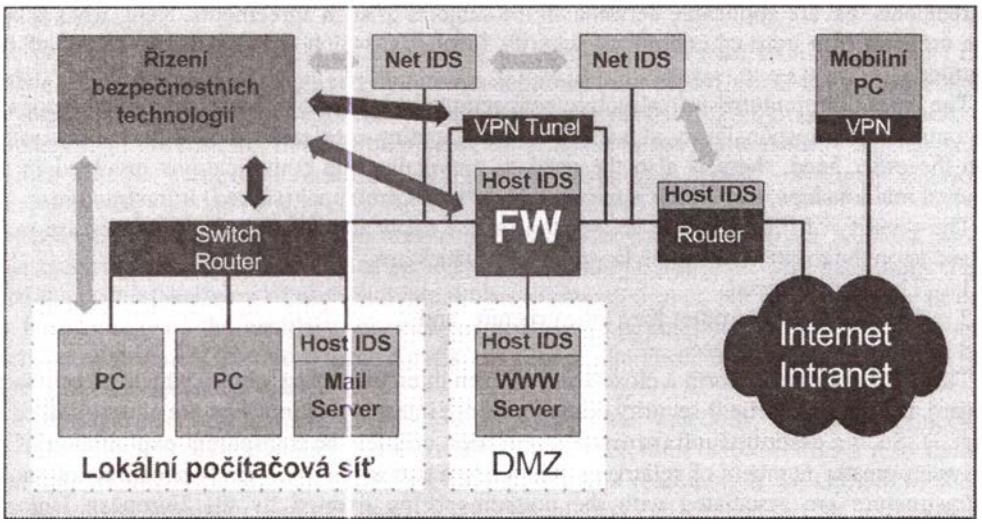


Fig. 2 Security Interface.

When resolving issues involving the secure connection of networks, one cannot forget to consider systems for the detection of penetrations of one's security system (i.e. Intrusion Detection System - IDS). This tool provide a completely new dimension to issues involving the security of network connections, such as the ability to automatise the detection of security attacks or chinks - and the possibilities provided for the correct and timely reaction to problems discovered in these processes.

From the functionality point of view, an important factor for **IDS** is the (suitable) location of the monitoring components of the **IDS** system (i.e. sensors and scanners). The problems and issues associated with IDS may be divided into two categories - dependent upon the location of the installation of the IDS programme.

The aim of Network **Intrusion Detection** is to identify in real time, and if possible to prevent, unauthorised or incorrect usage and misusage of the computer systems network by internal users of the network or from external attackers.

Detection of attacks by such types of IDS system are based on the comparison of the user's relation (to the network), or on user commands with a pre-created database of rules and regulations based on knowledge of the techniques used by attackers when attempting to penetrate (intrude into) one's system.

The aim of **Host Intrusion Dete< tion** is to identify in real time any unauthorised or incorrect usage and misusage of the computer systems network by internal users of the network.

Host **IDS** systems are based on the principle of the significant differences between attacks on the computer system from one's normal activities using that system. Two main detection techniques exist: Statistical Analysis and Expert Systems Analysis.

Both of the above-mentioned methods are concerned with the breakdown of the installation of the monitoring elements of the IDS system. The main component of the **IDS** system is the Centralised Management Centre. Individual packets of data regarding the events being tracked by the monitoring components are sent to this centralised unit for evaluation and analysis.

Securely Shared Applications.

The individual elements of the secure interconnection of networks (usually) serve above all for enabling communication between a limited number of systems. As required, secure sharing of applications will need to be complemented by several other measures, which will reduce the process and organisational complications involved in the realisation of connections at the applications level. This requirement is predominately given by the necessity for the secure integration of a greater quantity of relatively independent information systems.

In such cases, it is practically unreal to base oneself only upon a series of mutual bilateral agreements that are applicable between all the subjects of such agreements. Here, what is key is the creation of a core of communal security functions, which will be shared by all of these entities.

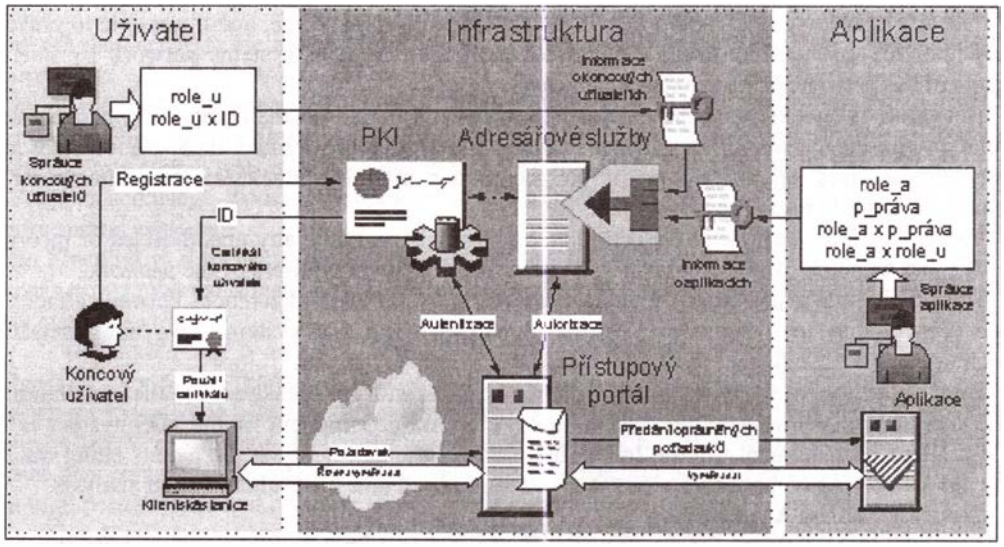
The basis of communal infrastructure connections is, on the one hand, the unambiguous and incontrovertible responsibility of each of the participating entities for their information systems. On the other hand, there is also the need to minirnalise the complications involved in such mutual relationships, and which is impossible wither t communal (shared) infrastructures.

The security of infrastructure connections at the applications level in such cases are mainly based upon the existence of three key elements, which are:

1 The Access Portal.
2 The Public (Electronic) Key Infrastructure, and ...
3 Address book Services.

These three elements form a closely interwoven interconnecting whole, which it necessary to regard as a single (unified) security complex whose internal relationships are closely linked (viz Fig. 3). Such a described infrastructure connection enables the transparent exploitation of data between greater numbers of relatively independent entities. The wider applications of such an infrastructure are associated with the pressures being exerted by the European Union on expanding so-called electronic public sector administration i.e. so-called “e-government”. Generally speaking, it is possible to consider such an infrastructure as a qualitatively higher form of secure linkage of information systems.

In a wider sense, this architecture also penetrates into the internal operational environment of enterprises information systems solutions, where it means the separation of simplified Client server environments from centrally provided applications. In such cases, implementation is often conditional upon the historical developments of the system and the corresponding ways and means of implementing the individual systems elements. An infrastructure, as is herein described, which is designed as a unified functional block, can be of effective service in the planning of future developments of enterprises (as well as e-learning) systems.



rig. 3. Secure Shared Applications Schema.

The Access Portal.

The core of such a complex is the Access Portal, which asserts its rights to managing the access of end users to the individual shared applications. The functional and security capabilities and the degree of standardisation associated with access portals is nowadays highly

perfected, which in turn enables the minimalisation of complications arising from changes to client work stations.

The principle of access portals is based above all upon the consistent standardisation of the interface. Here, the key role is played by Internet solutions (e.g. HTML or XML), which enable the integration of end user and application interfaces. Nevertheless, an important component of the openness of the solution remains their support by means of the latest security mechanisms, of which SAML - Security Assertions Markup Language and SSML - Security Services Markup Language are universally considered to set the standard.

It is possible to divide the basic functions of access portals into two domains. The first, more visible grouping includes the ability to personalise the personal pages of individual users. This part of the portal takes care of each individual visit of each end user, for whom the ease of use (user-friendliness) of the ancillary services is important (e.g. support for the generation and implementation of new (electronic) certificates, the ease of alteration of one's information in the address book service and so on.).

The second area concerns above all those security issues and functions, which are connected to the assertion of access rights in accordance with pre-defined rules. This section is responsible for its own assertion of its own access rights, and for this reason, it is concerned with the authorisation of imminent requirements. A component may be the support of a variety of authentication mechanisms, or the support of complex access rights and regulations (e.g. the combination of the user's role, group, location, and time of access and the context of all of the afore-mentioned).

The Address Book Service.

A further element of the comple.x features address book services, in which are concentrated all data requisite to the authorisation of the requested access. For the service to function correctly, it is necessary on the one hand to collect and collate data about the user and the role(s), in which they are allowed to gain access. On the other hand, it is essential that the address book service be equipped with a set of security rules and the parameters of the shared application(s). The primary role of address book services is to decide about authorisation, and whether or not the received request may be accepted.

Information about users should contain a description of the role(s), which the individual user is entitled to (whether permanent, or temporary). This information is important for the decision-making process when authorising access requests and requirements. Concurrently, they should also contain further contact information (i.e. e-mail, telephone №s, (electronic signature) certification, etc.).

On the other hand, the information about the application(s) must contain definitions of the validation of access rights and all other rules by which decisions may be taken regarding the ways and means of authentication, authorisation, and auditing the access of end users.

The (Electronic Signature) Public Key.

The final element of this complex is the (Electronic Signature) Public Key infrastructure (PKI), whose basic task is the unambiguous identification of the physical and "electronic" identity of the end user. This confidential relationship between the two identities enables the access portal to exploit the benefits of the PKI infrastructure as an effective tool for the identification of users (e-learning technology currently only makes use of user names for identification and passwords for authentication - in more advanced systems, chip cards also have a role to play ... etc.

Here, it is necessary to draw one's attention to the fact that, for communication with the access portal, it is not possible to exploit the Electronic Signature applications. In fact, it is exactly the opposite, since to simplify communication, PKI is especially used as an effective means of verifying the identity of the applicant user, which is in direct contradiction with Law №. 227/2000§ Of Electronic Signatures. Using electronic signatures is always associated with concrete applications, and therefore it is (its source) outside the infrastructure being described.

Apart from differentiating electronic signatures and user authentication, it is highly advisable to take into consideration a whole range of further factors when applying PKI applications (e.g.

the use of date and time stamps, the use of certificates for enciphering data, chip card support, or other technical resources for saving private keys and so on).

Literature Resources:

[BS7799] Information Security Management; BSI2002 & RAC 2002.

[COBIT] COBIT 3rd Edition: Executive Summary, Information Systems Audit and Control Foundation, ISACF 2000.

[IATF31] Information Assurance Technical Framework, Release 3.1, IATF Forum, NS A 2002.

[IDA-AG] Interchange of Data between Administration - Architecture Guidelines for Trans-European Telematics Network for Administration, version 6.1, Enterprise DG, Brussels 2002.

[NIST47] Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems, NIST 2002.