Internet and E-Business Security

Violeta Tomašević
Mihajlo Pupin Institute, Serbia

Goran Pantelić
Network Security Technologies – NetSeT, Serbia

Slobodan Bojanić
Universidad Politécnica de Madrid, Spain

INTRODUCTION

Originally developed for research and education purposes as Arpanet in 1970s, the Internet has become a worldwide network that offers numerous services to the immense community of users. An everyday progress of the network technology brings also new security risks regarding a lot of sensitive data transferred over the network, especially in banking, commercial, and medical applications. Therefore the Internet security could be in general defined as a set of measures that should prevent vulnerabilities and misuse of data transmitted and used through the network.

INTERNET SECURITY THREATS

The computer systems that are connected to the Internet are exposed to various potentially very harmful threats. The damages, like corruption or loss of data, a theft or disclosure of confidential data, or denial of system services are facilitated by the open architecture of Internet (Oppliger, 2002). Computer viruses and worms, eavesdropping and packet sniffing, hacking, illegal intrusions, denial-of-service and other attacks on network resources imperil all participants of the system.

The current and still dominant **Internet protocol** version 4 (IPv4) with end-to-end model assumes that the end nodes provide security. The next generation of Internet protocol, version 6 (IPv6) increases an address space (up to 3 x 10^{38} nodes) and supports auto configuration and mobility of networked devices. It facilitates an introduction of the new technologies like wireless devices, ubiquitous computing, and so forth. It opens the new security issues and requires the built-in smart security services as an integral part of the base protocol suite (Kent & Seo, 2005).

There are numerous other high technology attacks on network infrastructure and resources like domain name system servers and routers that could redirect traffic to other sites, change identity of the attacker, and so forth. Also, some attacks are typical in e-business and online payment systems like SQL injection, price manipulation, cross-site scripting, and so forth. (Mookhey, 2004). Nevertheless all these threats could be prevented if the participants are aware of possible risks and comply with formal security measurements, and if there is a strong cooperation among all those who develop and maintain a system.

BASIC SECURITY REQUIREMENTS

Public Internet services could be considered safe and reliable if the confidentiality, integrity, and availability of data are provided as well as the legitimate use and the nonrepudiation. It means that (a) only authorized users could have access to data and perform appropriate actions, (b) data cannot be read by unauthorized users, (c) data cannot be changed during the transfer and the storage, (d) data and services have to be always available to legitimate users, and (e) a reliable proof of executed actions must exist, especially for **e-business** applications. In the background of the Internet services, safe communication protocols have to exist with multiphase "challenge-response" authentication for reliable identification of participants and data transport.

To fulfill these requirements, different cryptographic methods and technologies are used.

SECURITY POLICY, TECHNOLOGIES, AND METHODS

Organizations that plan to own or use available Internet services have to consider all potential threats, decide which defense measures to undertake and implement them in an effective way. Analysis of system and risk factors (Oteteye, 2003; Schechter, 2005) results in a **security policy** that represents a proposal of measures regarding system administration, authorization and access control, network protocols, and cryptographic methods.

In the environments like wireless network, ubiquitous computing, and Web services, the security should be analyzed in the same way, having in mind their characteristics.

System Administration

System administration is an important security factor whose tasks are to assign passwords and access conditions to the users, maintain and update the system and application software including archives, take antivirus measures, audit and monitor network traffic, check log files, and so forth.

A new extensible access control markup language (XACML) is a language that tries to standardize a policy management and access decisions (OASIS, 2005), and helps the administrators to define the access control requirements for appropriate resources. It includes data types, functions, and rules, and can represent the runtime request for a resource.

Authorization and Access Control

Authorization and access control ensure the legitimate use of the system resources, access to data, and allowed activities. It implies the decision about the type of user identification, for example, additional authentication by digital certification or smart cards with user biometrical data besides user name and password.

The expanded use of public services induced a single sign-on as a form of **authentication** that enables a user to authenticate once to gain access to multiple subsequent Web systems. With obvious convenience for the user it imposes the complex management about authentication and users personal information across the independent sites. The security assertion markup language (SAML) is an example of an open message standard that is used as a good basis for making single sing-on authentication protocols (Groß, 2003).

Network Protocols

Apart from the application level security, there is also a transport layer security where network security protocols and the appropriate devices take part.

The secure sockets layer (SSL) protocol authenticates the entities and encrypts all traffic on the network. It provides a server or client authentication by digital certificate of entity. The Internet protocol security (IPSEC) is based on standards for a safe communication and works on network layers. It neither requires the changes in users' systems nor in applications that is optional in IPv4 but built-in and mandatory in IPv6. IPSEC combines several security technologies, encrypts all IP packets, and ensures data authentication, confidentiality, integrity, and key exchange. The authentication header is a protocol aimed for authentication and data integrity, while the encapsulating security payload provides authentication, data integrity, and confidentiality. The Internet key exchange protocol serves to establish and negotiate security parameters between participants. The virtual private network (VPN) is a private communication network that uses public network infrastructure. Thus, very remote computers can make one logical network and create safe communication tunnels through the public connections.

The firewalls are hardware or software devices that examine network traffic according to the configurable security policy and block it if, for example, inadequate protocols are used, data come from prohibited address, there is attempt to connect to prohibited port, and so forth.

Wireless Networking

Wireless networks and devices add new security issues to standard wired ones. Thus, the new mechanisms like Wi-Fi protected access (WPA) and wired equivalent privacy (WEP) are applied to protect data and wireless signals through the air (Wi-Fi Alliance, 2004). The WEP is a protocol based on the 802.11 Wi-Fi standard that intends to provide the equivalent level of security to wireless network as wired network has. It uses RC4 cipher with a 64-bit key where 24 bits are system generated, but that was shown as insufficient, and thus 128-bit or larger key should be used. The WPA