4- Security Standards

The computer network model also suffers from the standardization التوحيد القياسيproblem. Security protocols, solutions, and best practices that can secure the computer network model come in many different types and use different technologies resulting in incompatibility of interfaces , less interoperability, and uniformity among the many system resources with differing technologies within the system and between systems.
System managers, security chiefs, and experts, therefore, choose or prefer standards, if no de facto standard exists, that are based on service, industry, size, or mission. The type of service offered by an organization determines the types of security standards used. Like service, the nature of the industry an organization is in also determines the types of services offered by the system, which in turn determines the type of standards to adopt.
First the size of an organization also determines what type of standards to adopt. In relatively small establishments, **second** the ease of implementation and running of the system influence the standards to be adopted. **Finally**, the mission of the establishment also determines the types of standards used.
For example, government agencies have a mission that differs from that of a university. These two organizations, therefore, may choose different standards.

We are, therefore, going to discuss security standards along these divisions. Before we do that, however, let us look at the bodies and organizations behind the formulation, development, and maintenance of these standards.
These bodies fall into the following categories:
• International organizations such as the Internet Engineering Task Force (IETF), the Institute of Electronic and Electric Engineers (IEEE), the International Standards Organization (ISO), and the International Telecommunication Union (ITU).
• Multinational organizations like the European Committee for Standardization (CEN), Commission of European Union (CEU), and European Telecommunications Standards Institute (ETSI).
• National governmental organizations like the National Institute of Standards and Technology (NIST), American National Standards Institute (ANSI), and Canadian Standards Council (CSC).
• Sector specific organizations such as the European Committee for Banking Standards (ECBS), European Computer Manufacturers Association (ECMA), and Institute of Electronic and Electric Engineers (IEEE).
• Industry standards such as RSA, the Open Group (OSF + X/Open), Object Management Group (OMG), World Wide Web Consortium (W3C)), and the Organization for the Advancement of Structured Information Standards (OASIS).

• Other sources of standards in security and cryptography. Each one of these organizations has a set of standards. Table 1 shows some of these standards. In the table, x is any digit between 0 and 9.

Table 1 Organizations and their standards

Organization	Standards
IETF	IPSec, XML-Signature XPath Filter2, X.509, Kerberos, S/MIME,
ISO	ISO 7498–2:1989 Information processing systems – Open Systems Interconnection, ISO/IEC 979x, ISO/IEC 997, ISO/IEC 1011x, ISO/IEC 11xx, ISO/IEC DTR 13xxx, ISO/IEC DTR 14xxx
ITU	X.2xx, X.5xx, X.7xx, X.80x,
ECBS	TR-40x
ECMA	ECMA-13x, ECMA-20x
NIST	X3 Information Processing, X9.xx Financial, X12.xx Electronic Data Exchange
IEEE	P1363 Standard Specifications, For Public-Key Cryptography, IEEE 802.xx, IEEE P802.11g, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
RSA	PKCS #x – Public Key Cryptographic Standard
W3C	XML Encryption, XML Signature, exXensible Key Management Specification (XKMS)

4.1 Security Standards Based on Type of Service/Industry

System and security managers and users may choose a security standard to use based on the type of industry they are in and what type of services that industry provides. Table 2 shows some of these services and the corresponding security standards that can be used for these services. Let us now give some details of some of these standards.

Area of Application	Service	Security Standard
Internet security	Network authentication	Kerberos
	Secure TCP/IP communications over the Internet	IPSec
	Privacy-enhanced electronic mail	S/MIME, PGP
	Public-key cryptography standards	3-DES, DSA, RSA, MD-5, SHA-1, PKCS
	Secure hypertext transfer protocol	S-HTTP
	Authentication of directory users	X.509/ISO/IEC 9594–8:2000:
	Security protocol for privacy on Internet/transport security	SSL, TLS, SET
Digital signature and encryption	Advanced encryption standard/PKI/ digital certificates, XML digital signatures	X509, RSA BSAFE SecurXML-C, DES, AES, DSS/DSA, EESSI, ISO 9xxx, ISO, SHA/ SHS, XML Digital Signatures (XMLD-SIG), XML Encryption (XMLENC), XML Key Management Specifica-tion (XKMS)
Login and authentication	Authentication of user's right to use system or network resources.	SAML, Liberty Alliance, FIPS 112
Firewall and system security	Security of local, wide, and metropolitan area networks	Secure Data Exchange (SDE) protocol for IEEE 802, ISO/IEC 10164

4.1.1 Public-Key Cryptography Standards (PKCS)

In order to provide a basis and a substance for interoperable security based on public-key cryptographic techniques, the Public-Key Cryptography Standards (PKCS) were established. These are recent security standards, first published in 1991 following discussions of a small group of early adopters of public-key technology. Since their establishment, they have become the basis for many formal standards and are implemented widely.

In general, PKCS are security specifications produced **by RSA Laboratories in cooperation** with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography. In fact, worldwide contributions from the PKCS series have become part of many formal and genuine standards, including ANSI X9 documents, PKIX, SET, S/MIME, and SSL.

4.1.2 The Standards For Interoperable Secure MIME (S/MIME)

S/MIME (*Secure Multipurpose Internet Mail Extensions*) is a specification for secure electronic messaging. It came to address a growing problem of e-mail interception and falsification at the time of increasing digital communication. So, in 1995, Login and authentication of user's right to use several software vendors got together and created the S/MIME specification with the goal of making it easy to secure messages from nosy eyes. It works by building a security layer on top of the industry standard MIME protocol based on PKCS. The use of PKCS purposes the user of S/MIME with immediate privacy, data integrity, and authentication of an e-mail package. This has given the standard a wide appeal, leading to S/MIME moving beyond just e-mail. Already vendor software warehouses, including Microsoft, Lotus, Banyan, and other on-line electronic commerce services are using S/MIME.

4.1.3 Federal Information Processing Standards (FIPS)

Federal Information Processing Standards (FIPS) are National Institute of Standards and Technology (NIST)-approved standards for advanced encryption. These are U.S. federal government standards and guidelines in a variety of areas in data processing. They are recommended by NIST to be used by U.S. government organizations and others in the private sector to protect sensitive information. They range from FIPS 31 issued in 1974 to current FIPS 198.

4.1.4 Secure Sockets Layer (SSL)

SSL is an encryption standard for most Web transactions. In fact, it is becoming the most popular type of e-commerce encryption. Most conventional intranet and extranet applications would typically require a combination of security mechanisms that include

- Encryption
- Authentication
- Access control

SSL provides the encryption component implemented within the TCP/IP protocol. Developed by Netscape Communications, SSL provides secure web client and server

communications, including encryption, authentication, and integrity checking for a TCP/IP connection.

4.1.5 Web Services Security Standards

In order for Web transactions such as e-commerce to really take off, customers will need to see an open architectural model backed up by a standards-based security framework. Security players, including standards organizations, must provide that open model and a framework that is interoperable, that is, as vendor-neutral as possible, and able to resolve critical, often sensitive, issues related to security.

The security framework must also include Web interoperability standards for access control, provisioning, biometrics, and digital rights.

To meet the challenges of Web security, two industry rivalمنافس standards companies are developing new standards for XML digital signatures that include XML Encryption, XML Signature, and exXensible Key Management Specification (XKMS) by the World Wide Web Consortium التحالف(W3C), and BSAFE SecurXML-C software development kit (SDK) for implementing XML digital signatures by rival RSA Security.

In addition, RSA also offers a SAML Specification (Security Assertion Markup Language), an XML framework for exchanging authentication, and authorization information. It is designed to enable secure single sign-on across portals within and across organizations.

4.2 Security Standards Based on Size/Implementation

If the network is small or it is a small organization such as a university, for example, security standards can be spelled out كما موضحas best practices on the security of the system, including the physical security of equipment, system software, and application software.

• **Physical security** – this emphasizes التاكيد على the need for security of computers running the Web servers and how these machines should be kept physically secured in a locked area. Standards are also needed for backup storage media like tapes and removable disks.

• **Operating systems**. The emphasis here is on privileges and number of accounts, and security standards are set based on these. For example, the number of users with most privileged access like *root* in UNIX or *Administrator* in NT should be kept to a minimum. Set standards for privileged users. Keep to a minimum the number of user accounts on the system. State the number of services offered to clients computers by the server, keeping them to a minimum. Set a standard for authentication such as user passwords and for applying security patches.

• **System logs**. Logs(records) always contain sensitive information such as dates and times of user access. Logs containing sensitive information should be accessible only to authorized staff and should not be publicly accessible. Set a standard on who and when logs should be viewed and analyzed.

• **Data security**. Set a standard for dealing with files that contain sensitive data. For example, files containing sensitive data should be encrypted wherever possible using strong encryption or should be transferred as soon as possible and practical to a secured system not providing public services.
As an example, Table 3 shows how such standards may be set.

Table 3 Best security practices for a small organization

Application area	Security standards
Operating systems	Unix, Linux, Windows, etc.
Virus protection	Norton
Email	PGP, S/MIME
Firewalls	
Telnet and FTP terminal applications	SSH (secure shell)

2.4.3 Security Standards Based on Interests

In many cases, institutions and government agencies choose to pick a security standard based solely on the interest of the institution or the country. Table 4 below shows some security standards based on interest, and the subsections following the table also show security best practices and security standards based more on national interests.

Table 4 Interest-based security standards

Area of application	Service	Security standard
Banking	Security within banking IT systems	ISO 8730, ISO 8732, ISO/TR 17944
Financial	Security of financial services	ANSI X9.x, ANSI X9.xx

2.4.3.1 British Standard 7799 (BS 7799)

The BS 7799 standard published by BSI Group in 1995.The first part , outlines a code of practice for information security management that further helps to determine how to secure network systems. It puts forward a common framework that enables companies to develop, implement, and measure effective security management practice and provide confidence in inter-company trading. BS 7799 was first written in 1993, but it was not officially published until 1995, and it was published as an international standard BS ISO/IEC 17799:2000 in December 2000.