Web Services Security

Introduction

Developing standards for Web Services security

•XML key management Specification (XKMS)
•XML Signature
•XML Encryption
•How Web Services affect network security and security policies.

Introduction

Effective Web Services Security allows clients to access appropriate services while keeping sensitive information confidential.

Web services require end-to-end security for transactions.

•Authentication (e.g., Login names and passwords) can be compromised because of communications not encrypted.

•Required strong interoperability

Because transmissions occurs across multiple platforms and must be secured at all times.

Well-defined and well-documented security policies, as well as implementation, administration and maintenance, are crucial to any security infrastructure.

Companies are responsible to create their own security policies.

-Result in disparate security policies across organizations

-Need to develop security-policy standards for organizations to communicate effectively without compromising their security policies.

Basic Security for Transmission over HTTP

- HTTP enables web servers to authenticate users before allowing access to resources.

-Web server check user's credentials (e.g., username and password)

-HTTP security employs secret-key cryptography, message digests etc.

- However, HTTP do not encrypt the body of a message

-Need other strong security technologies

- E.g., SSL or Kerberos.

Challenge-response authentication

- Users must provide specific authentication information to verify their identities.

  Return 401 Unauthorized response when users are not unauthenticated to view a protected resource
- Users provide username and password setup up by, for example, emails

  Return 403 Forbidden if denied
- Relatively weak security solution

  Username and password are not encrypted.

Basic Security for Transmission over HTTP

Digest authentication

-A protocol

-Part of HTTP 1.1 specification

-A user's credentials are submitted to the server as a checksum

-Checksum, input as message digests in digital signature are generated using username, password, requested URL, the HTTP method and a nonce value (a unique value generated by the server for each transmission)

-created using MD5 algorithm, with 128 bits input.

- Message content not encrypted

  - easy to be intercepted

- Both the client and server must support digest authentication

  - use public-key or Kerberos for security help for HTTP1.1

- Server can restrict access on the basis of an IP address, password, or public-key.

- Server can disallow access to all or part portions of a site for users with a certain IP address or from a specific IP subnet.

- Also, use **Public-key cryptography** or other **security methods** in password.

Web Service and Secure Socket Layer

- **SSL protocols secures** the channel through which data flows between a client and server and enables authentication of both parties.
- Still have problems using SSL to secure Web services

  -Users credentials and certificates are sometimes **too large** to transmit efficiently between computers.
- Affect success of transactions.

  -SSL encryption uses processor power
- **Slow down transmissions** and significantly **impede web services performance.**
- **Use SSL accelerators** to handle complex SSL encryption calculations to free server resources and improving performance.

For Web services, information going through a third-party device before reaching destination.

-SSL cannot guarantee the security if the messages.

-E.g., credit-card information.

-SSL connects two computers at a time.

•Protect data transmission, but not end-to-end security

HTTPS

-Secure communications by sending HTTP requests and responses over an SSL connection.

•Use port 443, instead of port 80

XML Signature

XML-based applications have security concerns

-XML documents are plain-text

-DTDs and style sheets can be modified

-Alter XML documents (security holes) to allow anyone to access information.

Digital Signature

-Solve the problem above by verifying document integrity.

XML SIGNATURE

W3C's XML Signature Specification

-Define an XML-based standard for representing digital signatures.

-Provide authentication, message integrity and nonrepudiation

-Use Digital Signature Standard (DSS) algorithm and the Secure Hash (SHA-1) authentication algorithm.

XML SIGNATURE

Extended XML signature to support their own algorithm and secure models.

-Sign any type of file, not just XML document.

-Signed data can reside inside or outside the XML document that contains the signature.

-The data object is cryptographically signed and used in generating a message digest.

XML SIGNATURE

using canonical form of an XML document before it is signed

-Avoid XML documents have the same hash value

-Same canonical form -> logically equivalent

-Small differences create different hash values

•E.g., comments or spaces that have no impact on the meaning of an XML document.

-Transform an XML document into a context interpreted by an application

•Logically equivalent documents produce the same message digest.

•Regardless of structures of documents.

XML SIGNATURE

An example

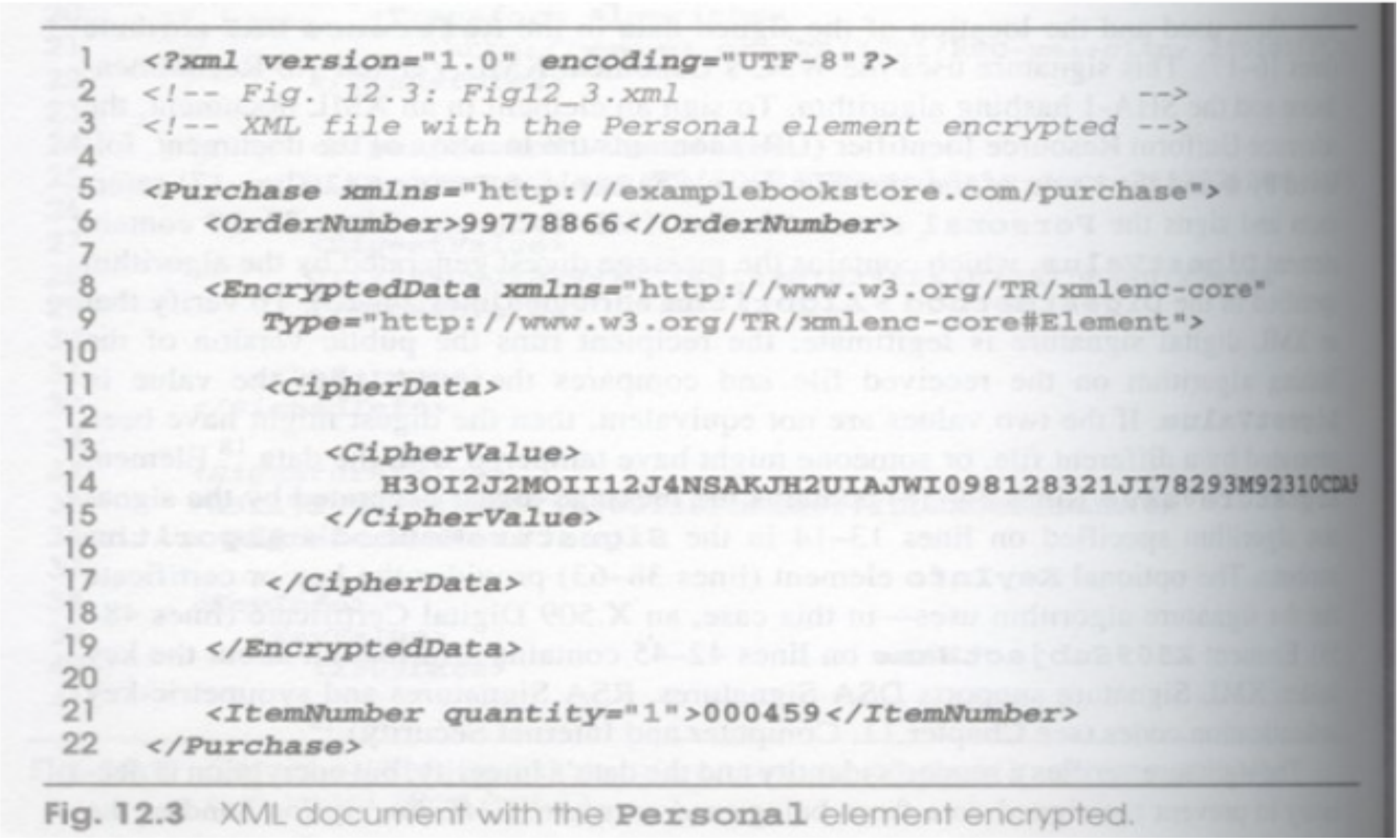
-Online book order using credit card

- Send an XML document contains name, address, credit-card information, and order info.
- Information is protected by the signature and sent to the seller.
- Seller checks the integrity of the customer's signature and sign the document before submitting it to the credit-card company.
- The credit-card company receives signatures that verify the authenticate the customer and the seller
- protects buyers against unauthorized purchases.

XML Encryption

- Handle the encryption and decryption of XML documents that are secured with XML signature.
- Signature verifies a sender's identity and the data's integrity, but encryption is necessary to prevent the signed data from being read en route.
- Protect any form of data.

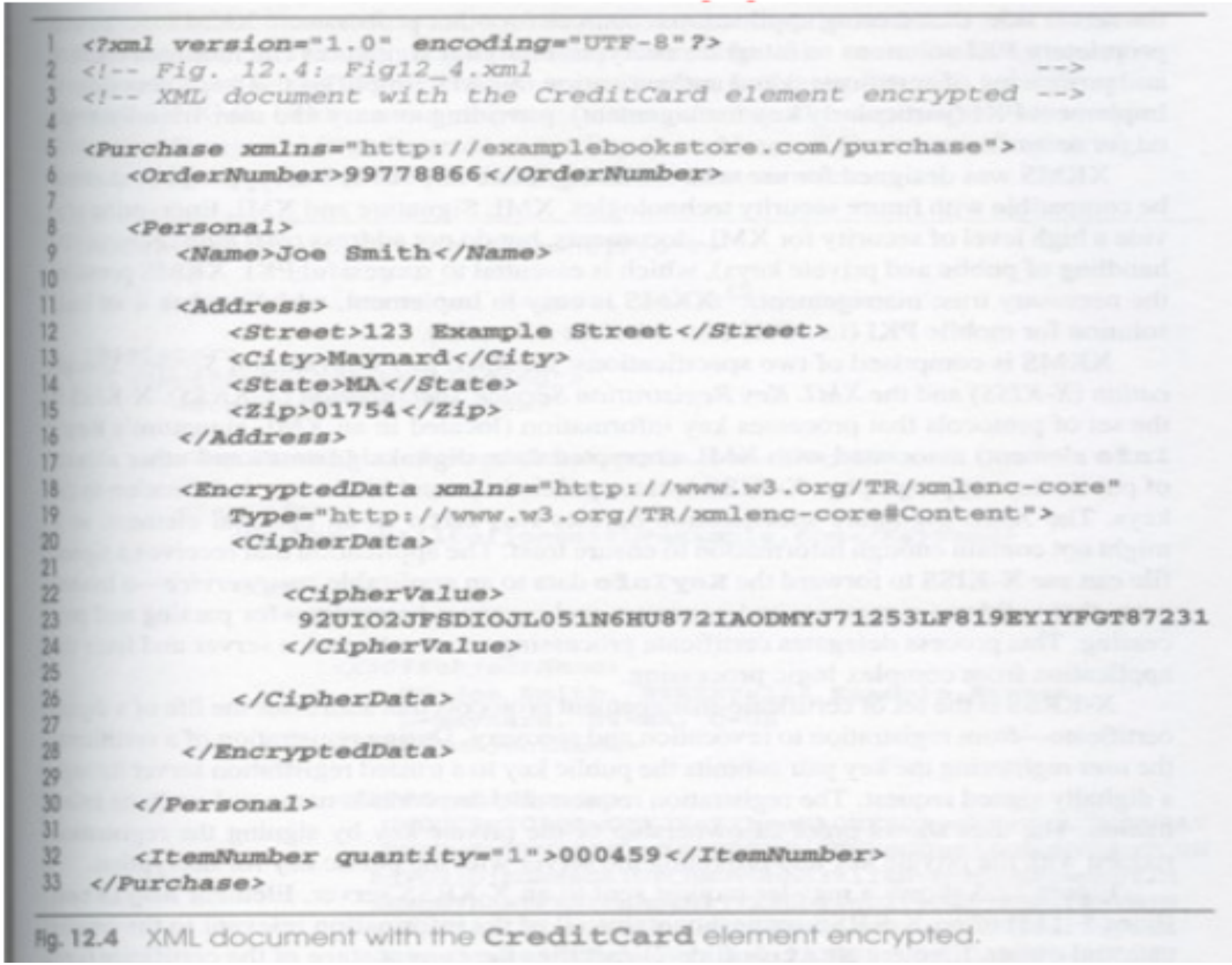
XML ENCRYPTION



```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Fig. 12.3: Fig12_3.xml                               -->
<!-- XML file with the Personal element encrypted -->

<Purchase xmlns="http://examplebookstore.com/purchase">
   <OrderNumber>99778866</OrderNumber>

   <EncryptedData xmlns="http://www.w3.org/TR/xmlenc-core"
      Type="http://www.w3.org/TR/xmlenc-core#Element">

      <CipherData>

         <CipherValue>
            H3OI2J2MOII12J4NSAKJH2UIAJWI09812832IJI78293M92310CDAJ
         </CipherValue>

      </CipherData>

   </EncryptedData>

   <ItemNumber quantity="1">000459</ItemNumber>
</Purchase>
```

Fig. 12.3 XML document with the **Personal** element encrypted.

XML ENCRYPTION



```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Fig. 12.4: Fig12_4.xml                                    -->
<!-- XML document with the CreditCard element encrypted -->

<Purchase xmlns="http://examplebookstore.com/purchase">
   <OrderNumber>99778866</OrderNumber>

   <Personal>
      <Name>Joe Smith</Name>

      <Address>
         <Street>123 Example Street</Street>
         <City>Maynard</City>
         <State>MA</State>
         <Zip>01754</Zip>
      </Address>

      <EncryptedData xmlns="http://www.w3.org/TR/xmlenc-core"
         Type="http://www.w3.org/TR/xmlenc-core#Content">
         <CipherData>

            <CipherValue>
             92UIO2JFSDIOJL051N6HU872IAODMYJ71253LF819EYIYFGT87231
            </CipherValue>

         </CipherData>

      </EncryptedData>

   </Personal>

   <ItemNumber quantity="1">000459</ItemNumber>
</Purchase>
```

Fig. 12.4 XML document with the CreditCard element encrypted.

XML key management specification (XKMS)

•Developed by Microsoft, VeriSign and Web Methods.

•A specification for registering and distributing encryption keys for Public Key Infrastructure (PKI) in web services.

•Problems with PKI

-No Web services PKI standards exist.

-PKI solutions are expensive, difficult to implement

-No interoperable with other businesses' PKI product.

XML key management specification (XKMS)

XKMS solves the problems

- Establishes a platform-independent set of standards.

- Place portions of the PKI workload on the server side

• Free application resources for other processes

- Works with proprietary PKI solutions to **integrate encryption, digital signature and authentication.**

- **Easy the steps** to implement PKI.

- Provide **an easy and user-friendly** method for secure transactions.

Authentication and Authorization for Web Services

web service providers that want to reach the largest number of users should provide authentication and authorization via various popular sign-on services.

Authentication and Authorization for Web Services.

•Microsoft Passport uses .NET Web services for authentications and authorization.

-Provide single sign-on

-Required to access Windows XP applications and Hotmail

-Adopted by many e-business, including eBay, Monster

-200 millions users registered.

Authentication and Authorization for Web Services

Liberty Alliance

-Formed in October 2001 by sun Microsystems.

-Try to establish non-proprietary single sign-on standards for e-business.

-Seek to secure businesses' and users' confidential information and to establish universal single sign-on methods.

-Participants include AOL Time Warner, General Motors, American Express, MasterCard International, and RSA Security

Liberty Alliance

-The specification is designed to support decentralized authentication and interoperability

•users are not required to contact a central server to receive authentication.

•Increase flexibility

•Provide an ideal authentication system for wireless communications.

-Offer an alternative to Microsoft Passport Service.

Web Services and Network Security

Web services create additional network security concerns

-Network authenticate users before allowing access to resource.

-However, Web services are designed to use single sign-on

- Allow access to applications on the basis of another source's authentication credentials.
- Carry transactions beyond firewalls and place resources in risk of attack.

Web Services and Network Security

•The biggest concern

-The immaturity of underlying standards.

-Vulnerabilities are not discovered until attacks.

•Usually, companies operate Web services over internal networks and restrict external access.

-For security reasons.

-Need extra steps to protect applications and network to offer external access to Web Services.

Web Services and Network Security

•Still improving

-Web services create new security challenge, but also can protect computers on a network.

•use Web services to search networks for signs of viruses.

•Use Web services to apply updates to computers.