CS259 – Security Analysis of Network Protocols
The Project

03/11/04

Jun Yoshida (Visiting Scholar)

protocol

XML Security (XML Encryption, XML Signature)

properties which should be preserved

XML elements (ex. credit card number)

kind of attacks

Authentication, Secrecy

tool

Murphi

self or team

myself

papers

XML Encryption Specification

http://www.w3.org/TR/xmlenc-core/

XML Signature Specification

http://www.w3.org/TR/xmldsig-core/

WS-Security Specification

http://www-106.ibm.com/developerworks/webservices/library/ws-secure/

MSDN Online - WS-Security Specification Index (Japanese)

http://www.microsoft.com/japan/msdn/webservices/dnsrvspec/wssecurspecindex.asp

result

XML Encryption and Signature have the flexibility to use. When I modeled one example of XML Encryption without XML Signature, Murphi found one error that intruders can decrypt some messages. So it is important to use XML Encryption and Signature correctly.

normal case

$$A \rightarrow B : \{E_1\}SSK_{X1} / PK_B, \{SSK_A\}PK_B$$
$$B \rightarrow A : \{E_2\}SSK_{X2} / PK_A, \{SSK_B\}PK_A$$
$$A \rightarrow B : \{E_3\}SSK_B$$
$$B \rightarrow A : \{E_4\}SSK_A$$

error case

$$A \rightarrow B : \{E_1\}SSK_{X1} / PK_B, \{SSK_A\}PK_B$$
$$B \rightarrow I : \{E_2\}SSK_{X2} / PK_A, \{SSK_B\}PK_A$$
$$I \rightarrow A : \{E_2\}SSK_{X2} / PK_A, \{SSK_I\}PK_A$$
$$A \rightarrow I : \{E_3\}SSK_I$$