

WEB SERVICES SECURITY: Architectures, patterns, and standards

Dr. Eduardo B. Fernandez

Dept. of Computer Science and Eng.

Florida Atlantic University

www.cse.fau.edu/~ed

About me

- Professor of Computer Science at Florida Atlantic University, Boca Raton, FL., USA
- Worked at IBM for 8 years (L.A. Scientific Center).
- Wrote the first book on database security (Addison-Wesley, 1981).
- Author of many research papers
- Consultant to IBM, Siemens, Lucent,...

Value of information

- We rely on information for our credit, health, professional work, business, education
- Information is very valuable
- Illegal access (reading or modification) to information can produce serious problems

Security objectives

- Confidentiality--no leakage of sensitive or private information
- Integrity-- no unauthorized modification or destruction of information
- Availability (No denial of service) -- annoying , costly
- Lack of accountability (Non-repudiation)-- legally significant

The meaning of security

- Security implies providing these objectives in the presence of attacks
- Security requires technical, managerial, and physical countermeasures (defenses)
- We only consider technical aspects here
- A related aspect is privacy, a legal and ethics concern

Countermeasures

- Identification and Authentication– first step
- Access control/ authorization --provide confidentiality and integrity
- Auditing-- basis for prosecution or improvements to the system
- Cryptography-- a mechanism to hide information and prove identity and rights
- Intrusion detection

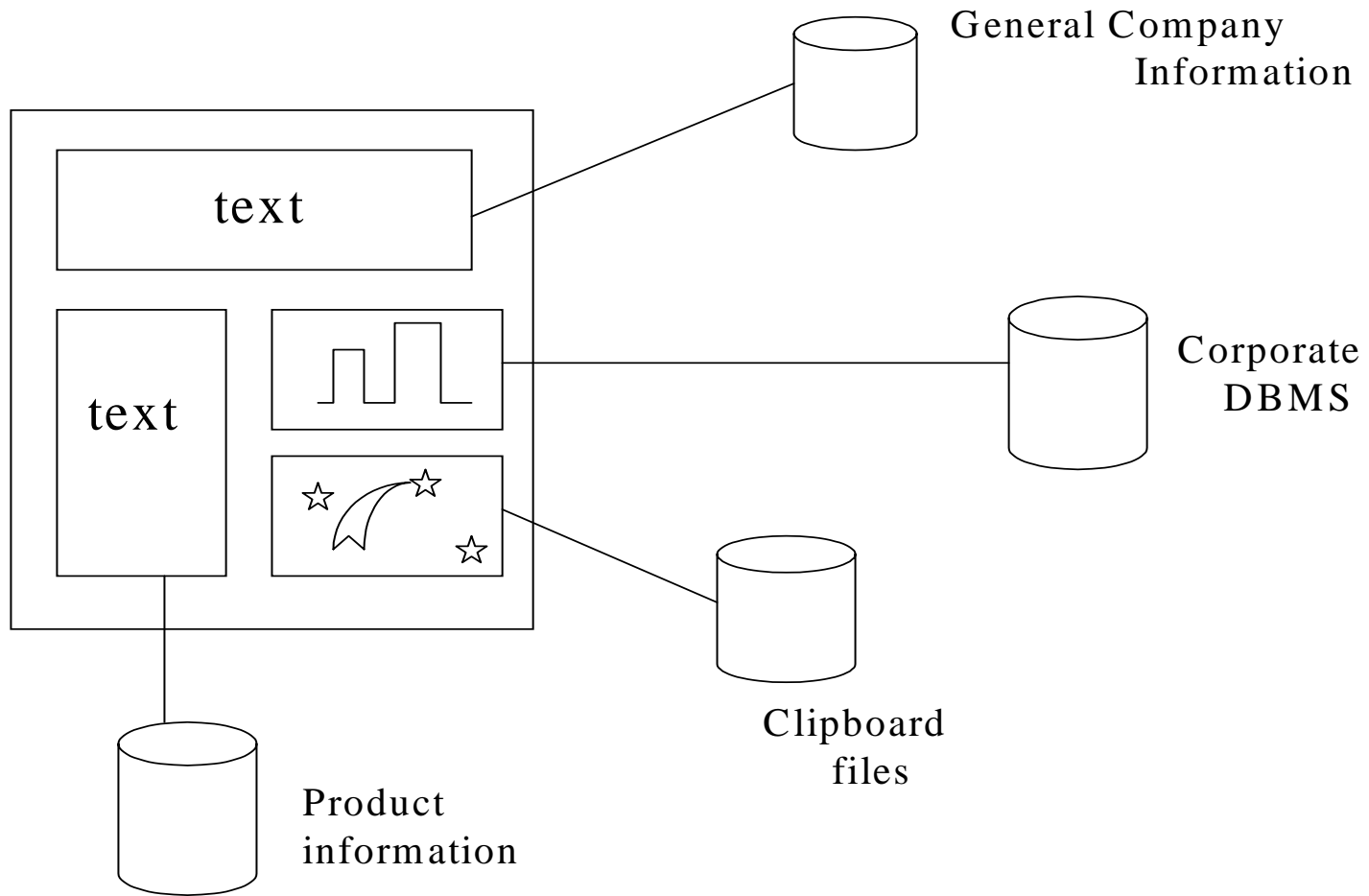
Environment

- The Internet is pervasive, all over the world
- Very large and complex system
- Small variety of architectural components
- Individual and institutional information is accessible through it

Web documents

- Hypertext /multimedia
- Passive or active (contain links to programs)
- Fixed or dynamic (assembled on request)
- Potentially all institution data can be considered documents

Example of a web page



XML

- XML is a metalanguage to define the meaning and structure of documents. A subset of SGML (Standard Generalized Markup Language). Basic ideas: use tags in data items to define their meaning, relate data items through nesting and references.

Effect of XML on security

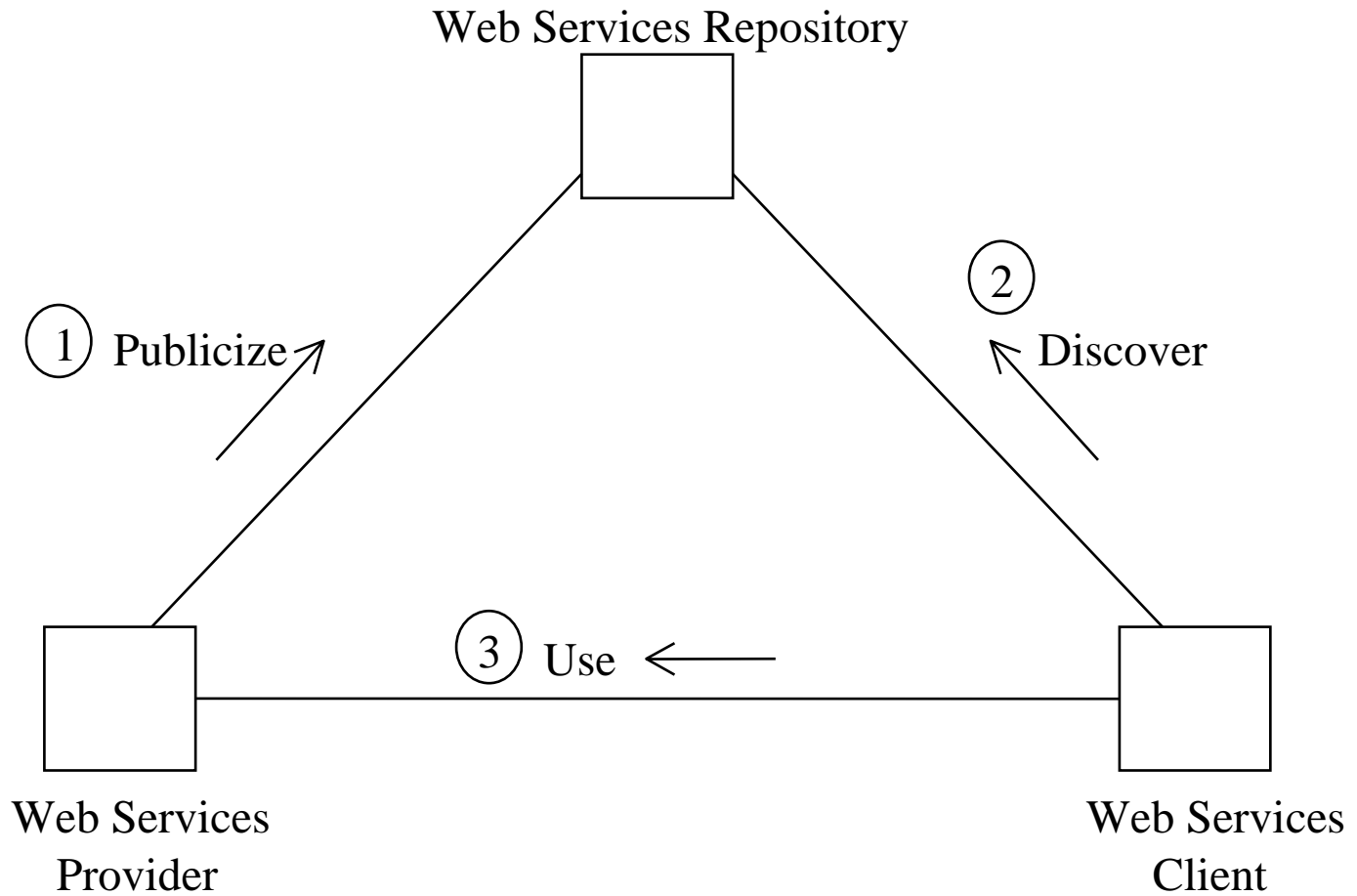
- Every element in a document has a meaning and can be protected in a separate way
- This increases the granularity of protection from one page to an element of a page
- Can be used to increase security and to improve performance (protect only sensitive parts of a document)

Web Services

- A Web Service is a type of component that is available on the web and can be incorporated in applications or used as a standalone service
- Require a standard supporting framework

Related to distributed objects

- Loosely coupled (any language, any platform)
- But they need standards to replace uniform framework (broker, etc.): XML. SOAP, many security standards
- Conceptually simple but standards are complex.



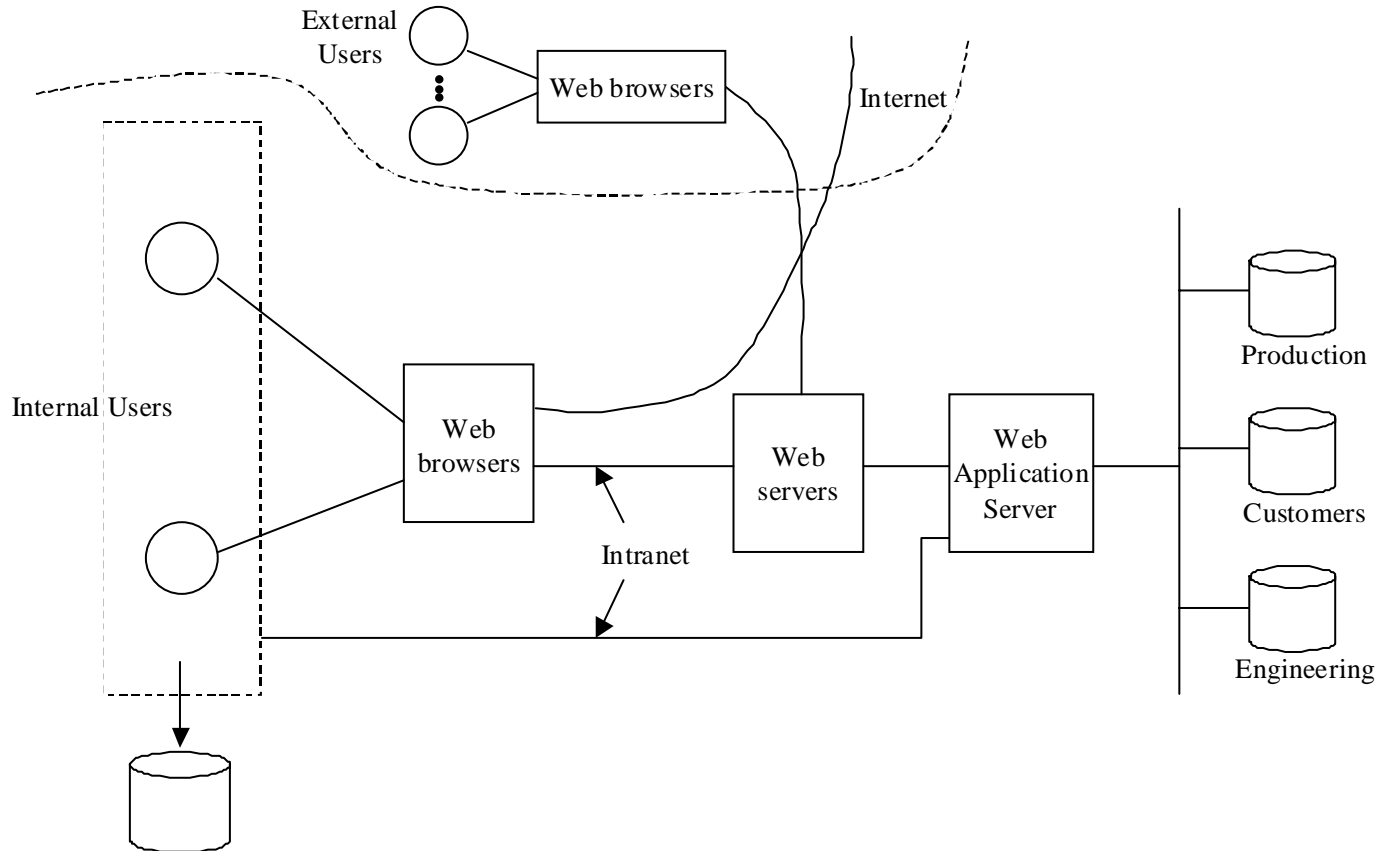
Architectures

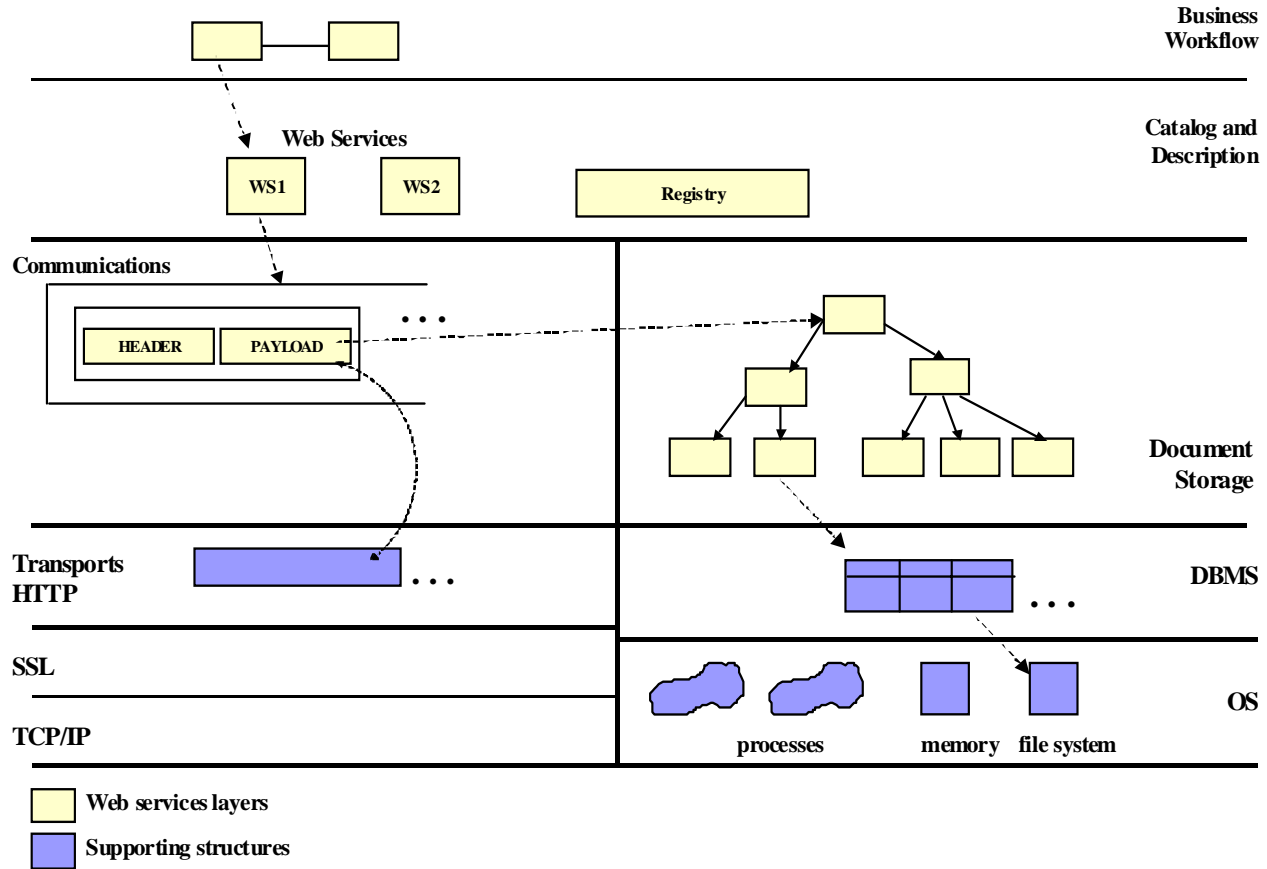
- Web services are a part of the application layer
- Web services are built out of XML, a lower-level data layer
- A SOAP layer is used for XML message transmission
- Internet layers and web server layers provide support for these layers

Deployment

- The application that uses web services typically resides in a web application server (WAS).
- The enterprise model is made up of components, J2EE or .NET.
- Web services complement an application or can be the whole application.

Enterprise architectures





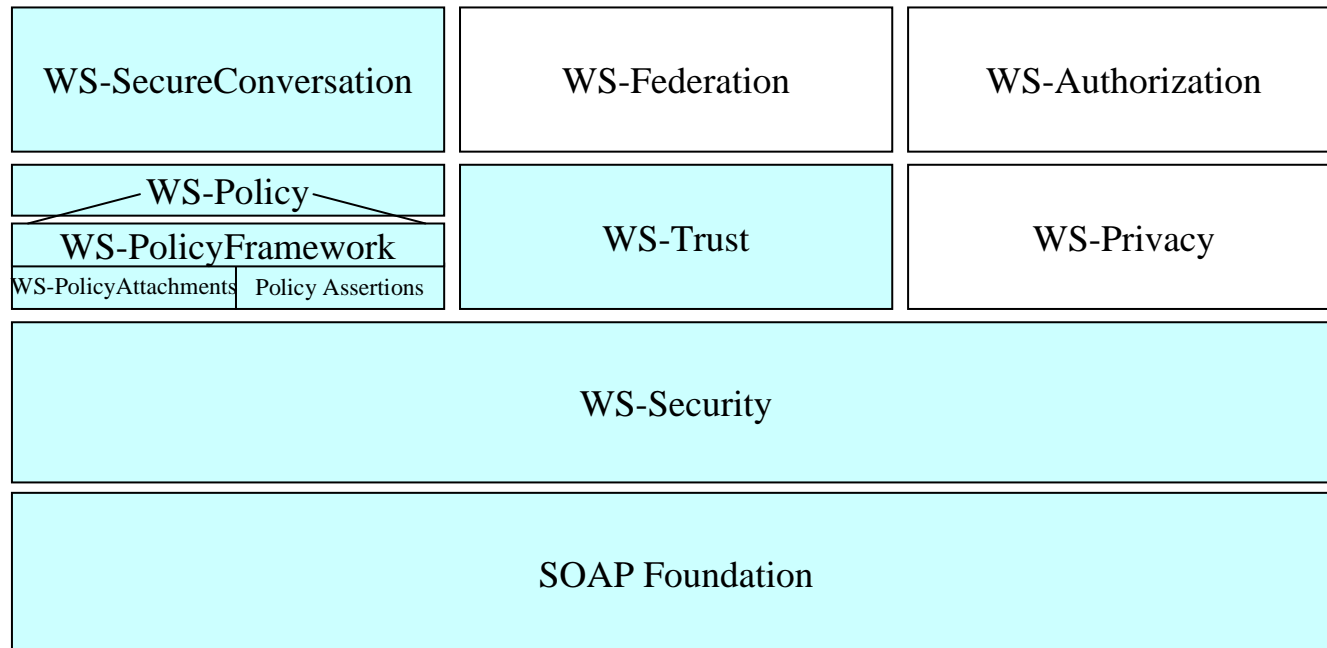
Standards

- Orange Book
- Common Criteria (NIST)
- IEEE
- IETF (Internet Engineering Task Force)
- OASIS (Open Applications...)
- W3C
- Industry ad hoc groups: IBM, Microsoft,...

Standards for web services

- A variety of standards to cover all levels
- May overlap or be in conflict
- XACML, WS-Security, SAML, SOAP security, privacy standards
- Confusing for vendors and users

Industry standards



Secure systems

- Design should be based on institution policies
- Policies define objectives
- Policies are guidelines for design and evaluation

Example of university policies

- An instructor can look at all the information about the course he is teaching.
- An instructor can change the grades of the students in the course he is teaching
- A student may look at her grades in a course she is taking
- The department head can add/delete course offerings
- The registrar can add/delete students from course offerings
- Faculty members can look at information about themselves

Roles in policies

- Originator of a document
- Manager of a group
- Secretaries
- Secretaries in the Engineering Dept.
- Authorizer
- Custodian
- Auditor

Roles in Web services

- *Creator*—this is a person or business that creates a web service and places it in a public repository. He wants only authorized customers to access his services.
- *Keeper of repositories of web services*—these are the institutions that provide public catalogs of services. They must assure authorized access to these catalogs.
- *Provider or keeper of web services*—these store the web services code and data. They may be the same as the keepers of repositories or the creators of web services, but could also be specialized institutions. As providers of web site functions they are concerned about proper access to their services and possible denial of service to their sites.
- *Consumer of web services*—they expect good quality services without malicious software. If they send their data to a web service, this data should be used in the proper way and protected from leakage or corruption.

Classification of security models

- Multilevel --users and data are assigned security levels
- Access matrix -- subject has specific type of access to data objects
- Mandatory --access rules defined only by administrators
- Discretionary -- users own data and can grant access to other users

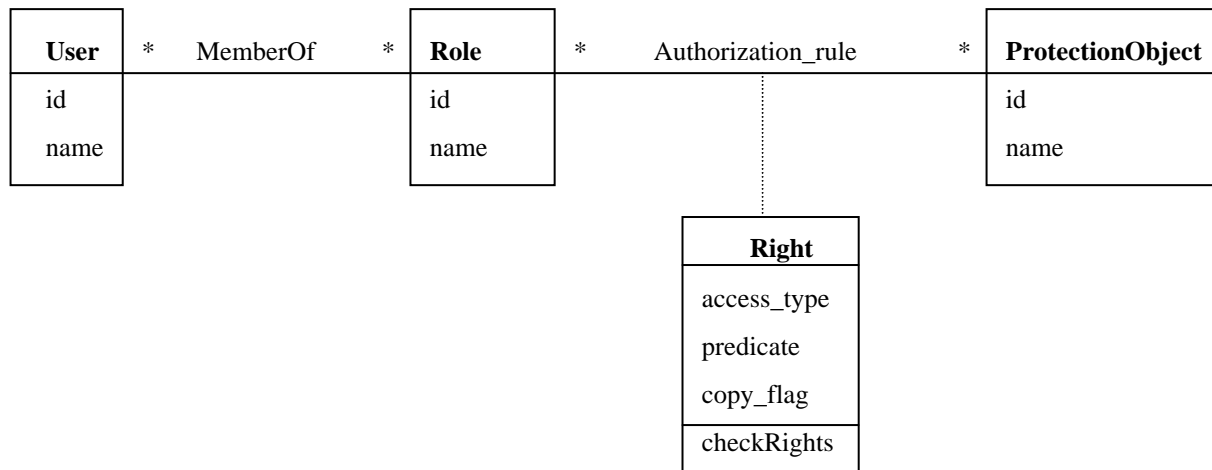
Access matrix authorization rules

- Basic rule (s, o, t), where s is a subject (active entity), t is an access type, and o is an object
- Extended rule (s, o, t, p, f), where p is a predicate (access condition or guard) and f is a copy flag
- This, and the other models, can be described by OO patterns

Role-Based Access Control

- Users are assigned roles according to their functions and given the needed rights (access types for specific objects)
- When users are assigned by administrators, this is a mandatory model
- Can implement least privilege and separation of duty policies

Basic RBAC pattern



Cryptography value

- Authentication—Can authenticate the identity of users, transactions, and systems.
- Protection of messages—Can protect the secrecy of a message and prevent illegal modification. Cannot protect against destruction of the message.
- Protection of software and data—Can protect the confidentiality of them although not avoid their destruction. For example, passwords can be encrypted.

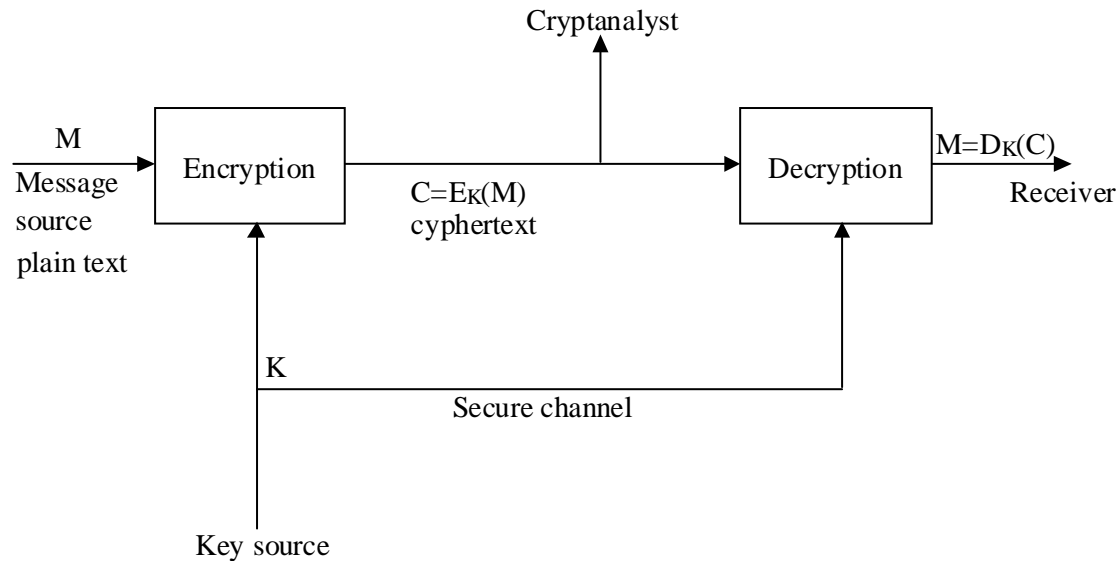
Cryptography value II

- Digital signatures—Can authenticate the origin of a message.
- Nonrepudiation—A user that signed or otherwise authenticated a document using cryptography cannot deny having sent it.

Mechanism

- Encryption is encoding a message to hide its meaning.
- *Plaintext* is converted into *cyphertext*.
Formally, $C=E(P)$ and $P=D(C)$.
- The cryptosystem must produce $P=D(E(P))$ to be useful

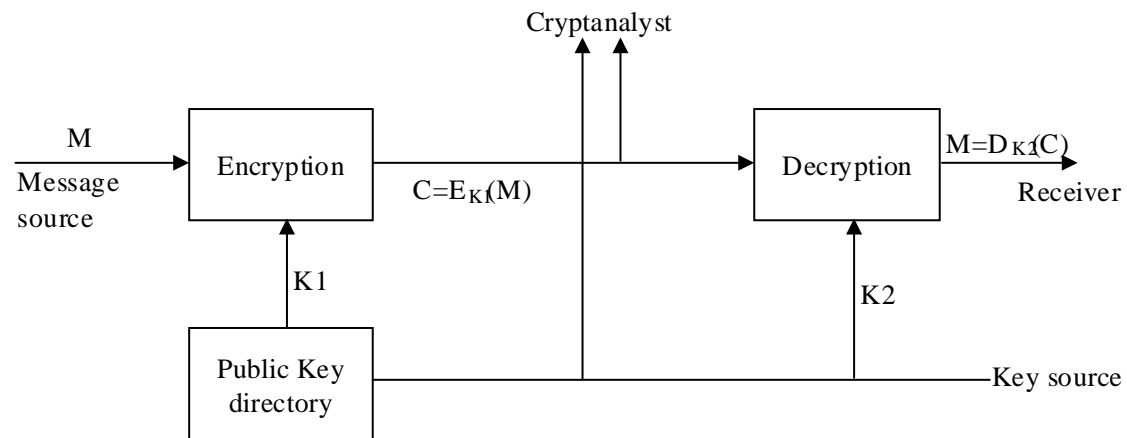
Symmetric cryptosystem



Public Key Systems (PKS)

- These algorithms use two keys, one of which is public and the other secret. The approach is based on the infeasibility of determining the decryption key given the algorithm and the public key.
- Instead of permutations and substitutions these algorithms use properties of mathematical functions. In particular, they use the theory of NP functions, those for which there is no polynomial time algorithm.
- Rivest, Shamir, and Adelman developed the so-called RSA cipher used in most current systems. This takes advantage of the difficulty of factoring a number into primes.

Public key systems



Value of PKI

- Easy key distribution (public and secret keys)
- Convenient digital signatures
- Hash values to detect message modification

Certificates

- The public keys are normally registered with a *certification authority* (CA). This authority distributes *certificates*, which are public keys with the signature of the CA.
- There are authentication and attribute certificates. Attribute certificates assert that certain properties are true of the owner of some authentication certificate. Attribute certificates are used in SSL and other protocols.

WS-Security

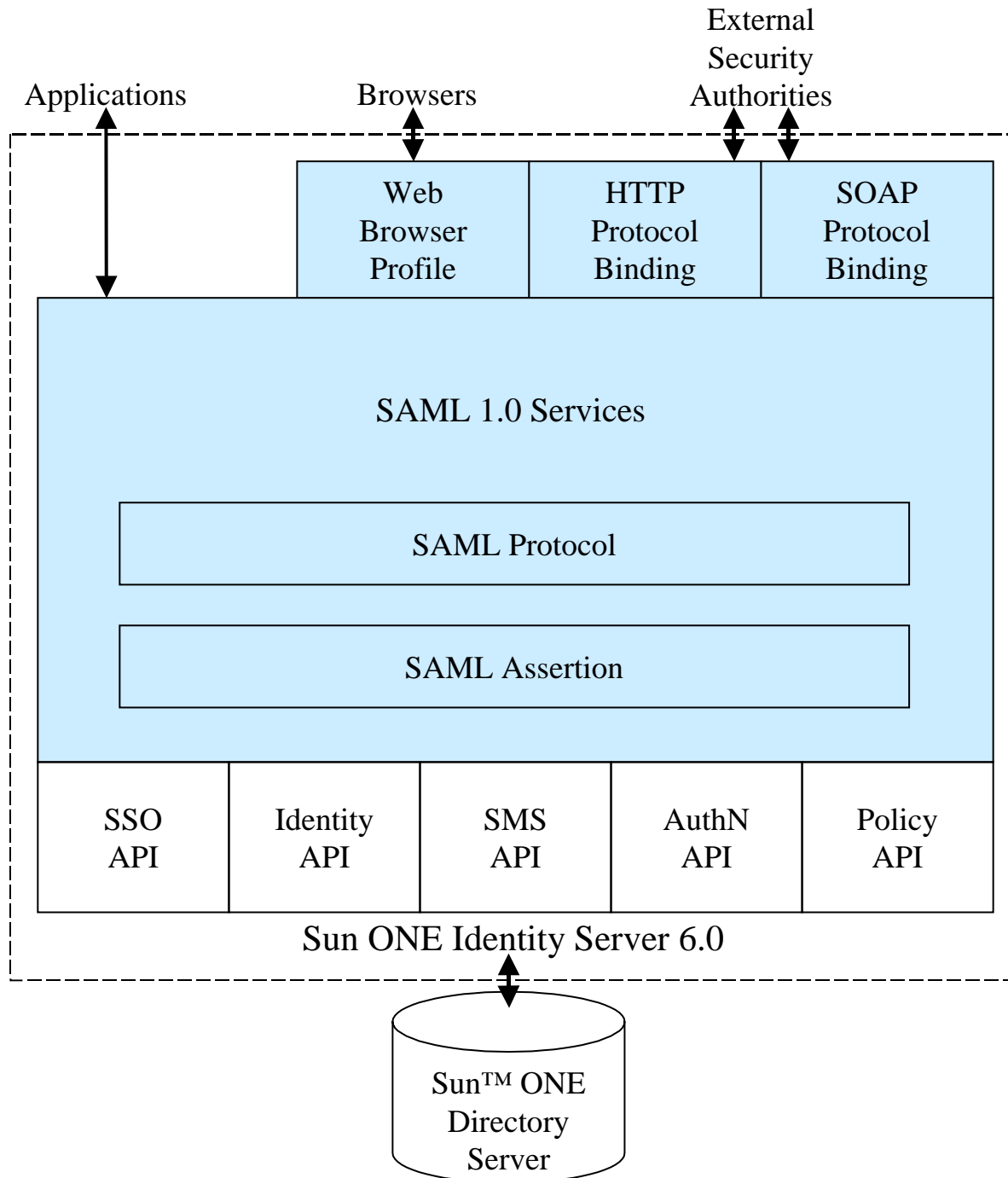
- Standard from IBM, Microsoft, and Verisign
- Defines security tokens
- Tokens may include certificates and Kerberos tickets
- Tokens can be used for claims of authentication or rights
- SAML can be used for headers

Security tokens

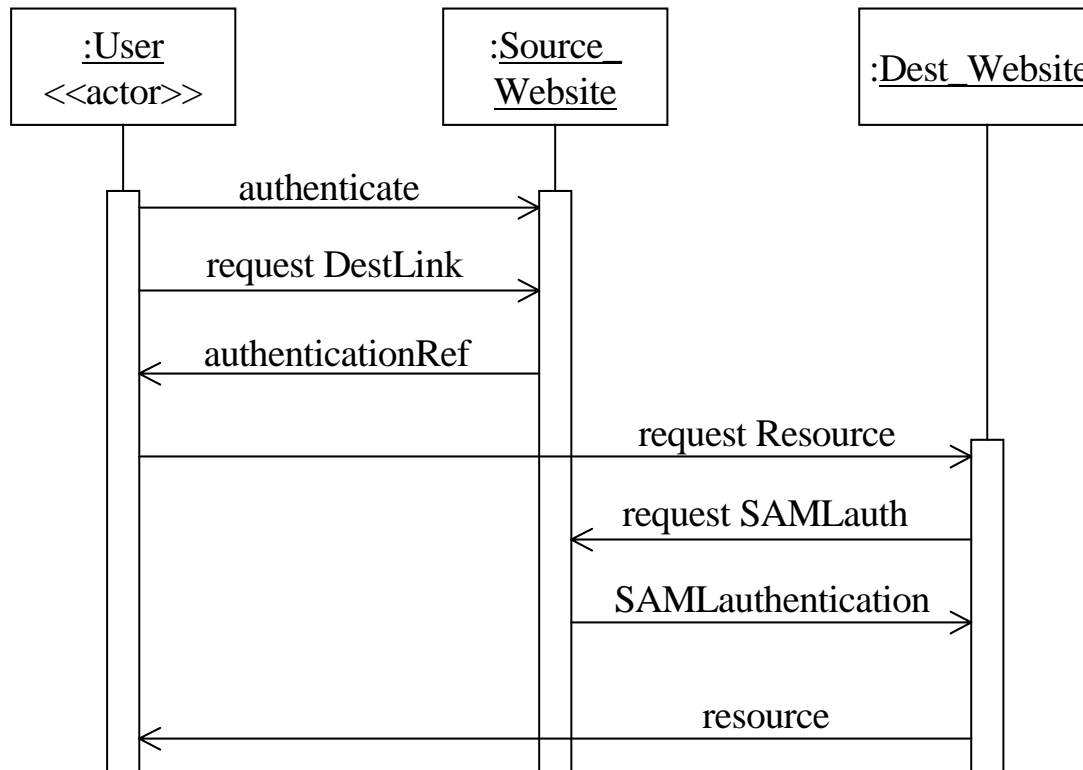
- *Signed Security Token* -- A signed security token is a token that contains a set of related claims (assertions) cryptographically endorsed by an issuer. Examples of signed security tokens include X.509 certificates and Kerberos tickets.
- *Claims* -- A claim is a statement about a subject either by the subject or by an relying party that associates the subject with the claim.

Identity

- Concept of network identity: set of all attributes that define a user
- Liberty Alliance—Sun, Visa, HP...
- Passport--- Microsoft



(Single Sign On) SSO pull model



Simple Object Access Protocol

- `<SOAP-ENV:Envelope`
- `xmlns:SOAP-ENV="`
- `http://schemas.xmlsoap.org/soap/envelope/"`
- `....`
- `<SOAP-ENV:encoding style="..." >`
- `<SOAP-ENV:Header>`
- `</SOAP-ENV:Header>`
- `<SOAP-ENV:Body>`
- `....`
- `</SOAP-ENV:Body>`
- `</SOAP-ENV:Envelope>`

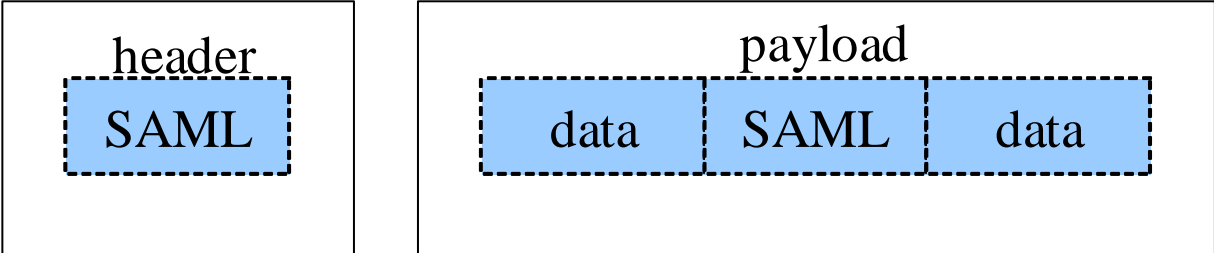
SOAP message security

- Headers can be used for signatures
- Authorization and authentication information in payload
- XML data can be encrypted
- Transport data can be encrypted

XML Message

transport

xp message



<SOAP-ENV:Envelope

xmlns:SOAP-ENV="

http://schemas.xmlsoap.org/soap/envelope/"

xmlns:xsi="

http://www.w3.org/1999/XMLSchema-instance"

xmlns:xsd="http://www.w3.org/1999/XMLSchema">

<SOAP-ENV:Header>

</SOAP-ENV:Header>

<SOAP-ENV:Body>

<ns1:sayHelloTo

xmlns:ns1="Hello"

SOAP-ENV:encodingStyle="

http://schemas.xmlsoap.org/soap/encoding/">

<name xsi:type="xsd:string">John</name>

</ns1:sayHelloTo>

</SOAP-ENV:Body>

</SOAP-ENV:Envelope>

XML encryption requirements

- XML Encryption Working Group (W3C)
- Granularity of encryption to the element (including start/end tags) or element content (between the start/end tags)
- Can reduce overhead by not encrypting all the document
- Can improve security by encrypting with different keys

Public Key Infrastructure

- XML Key Management Specification (XKMS)
- Registration of key pairs (X-KRSS)
- Location of keys for later use
- Validation information associated with a key (X-KISS)
- X-KRSS and X-KISS use SOAP and XML

XML security: Document

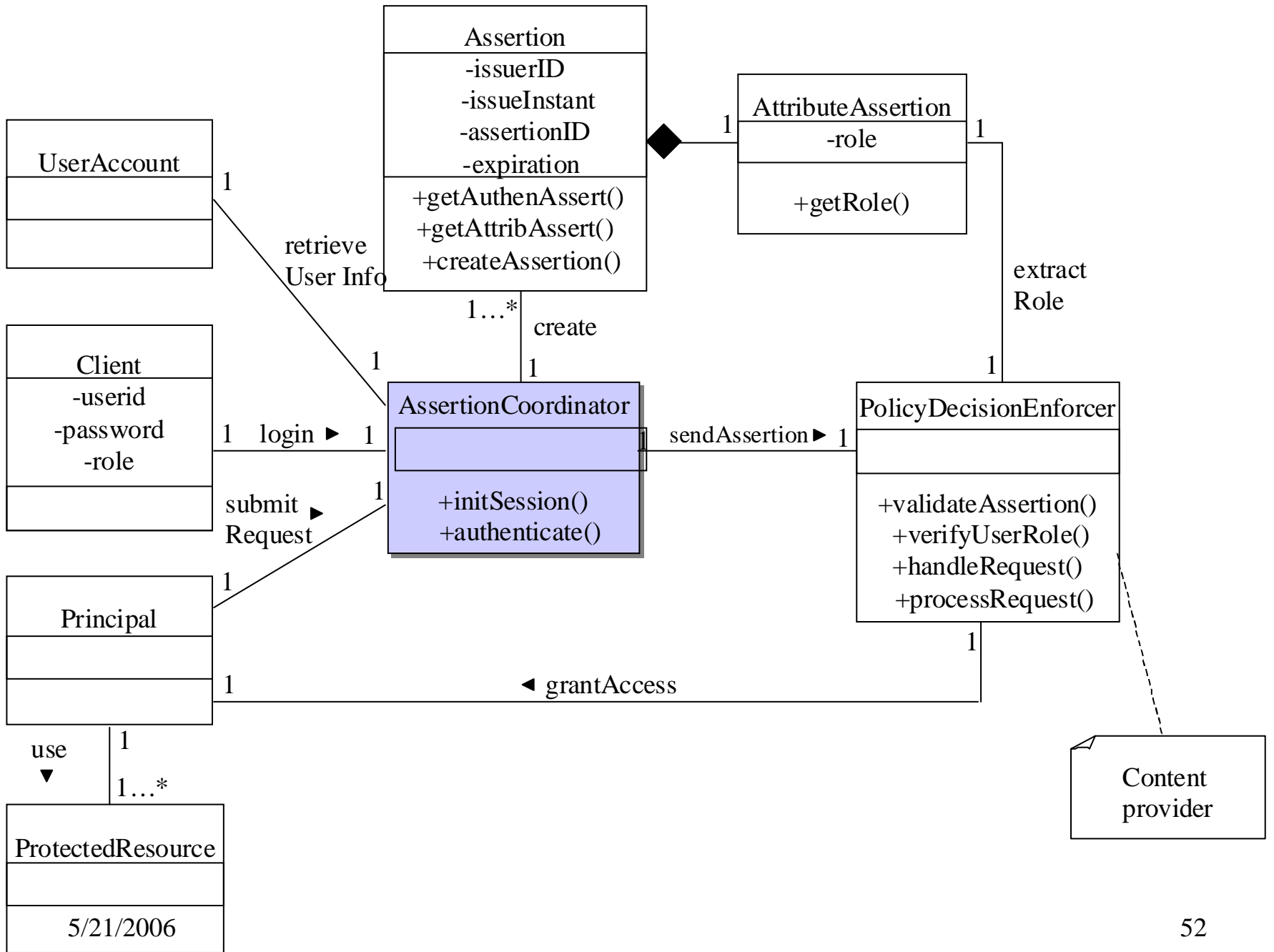
- One can (and should) use domain-based security according to document contents
- Languages to define authorizations on elements (access matrix)
- SAML (Security Assertion Markup Language)
- XACML (XML Access Control Language)
- Encryption of elements
- DTDs, DOMs, and links can also be used for security

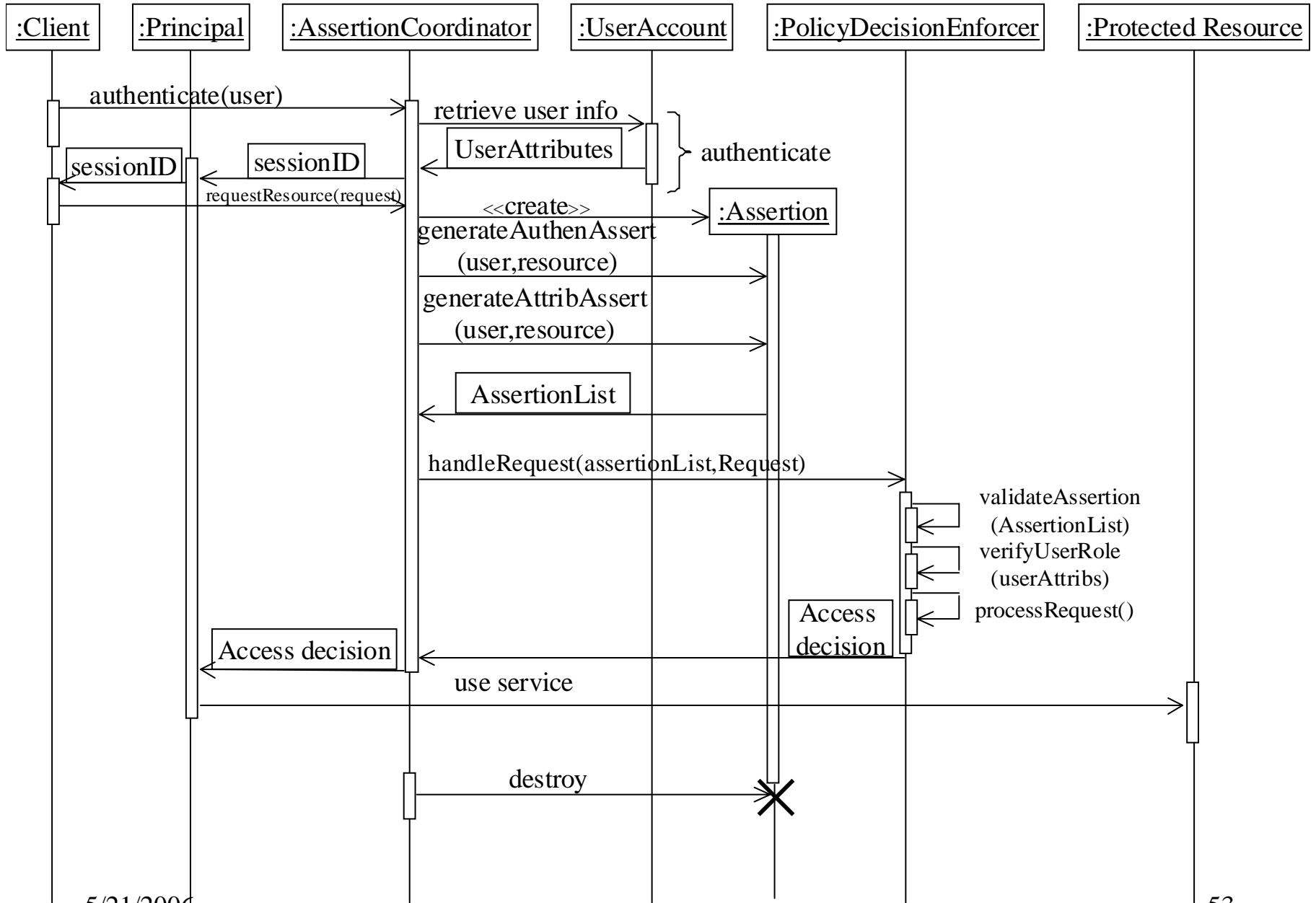
Security Assertion Markup Language (SAML)

- Part of XML-based Security Services
- XML framework for exchanging authentication and authorization information
- SAML information can be added to XML messages

Three types of assertions

- Authentication
- Authorization
- Attributes (groups, roles,...)

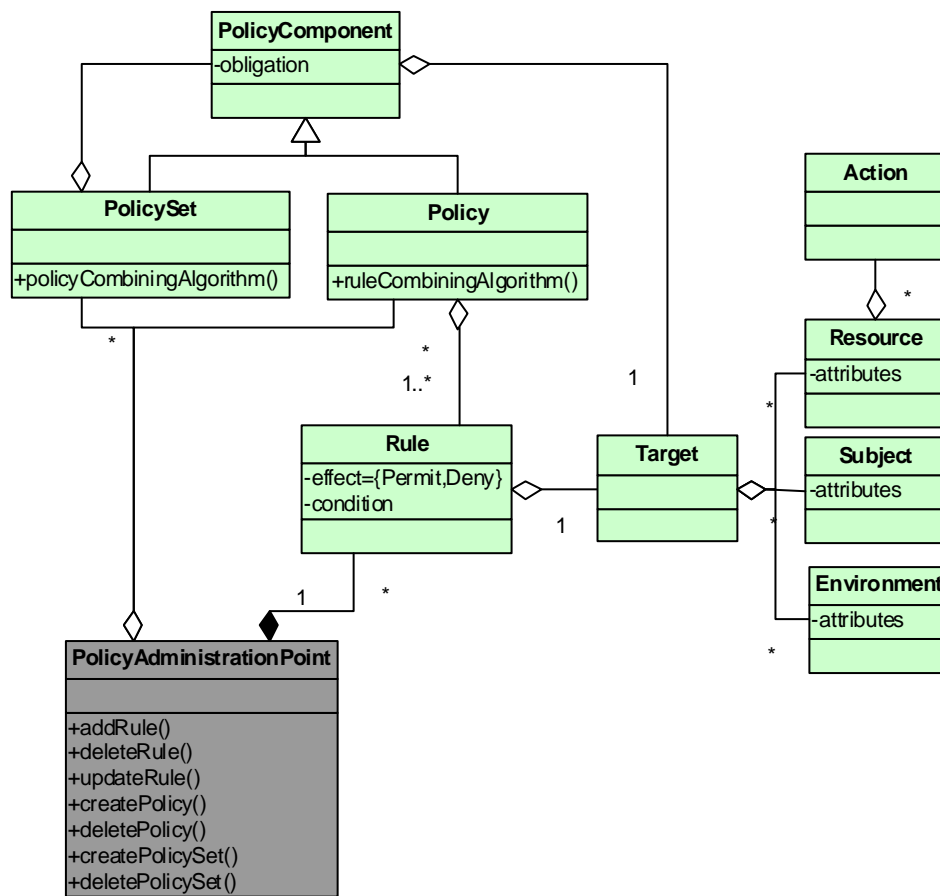




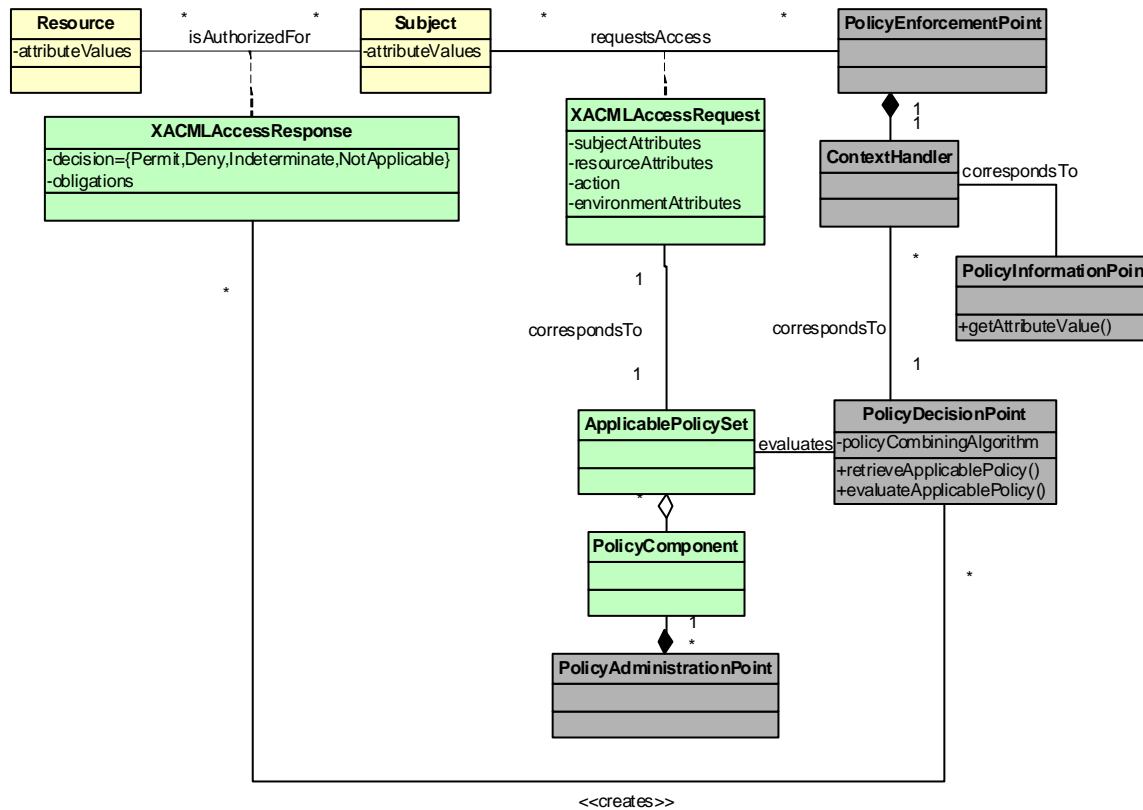
XACML

- Special technical committee of OASIS
- Specification of policies for information access over the Internet
- Combines work of IBM Tokyo and University of Milano, Italy.
- Implemented by Sun in early 2003

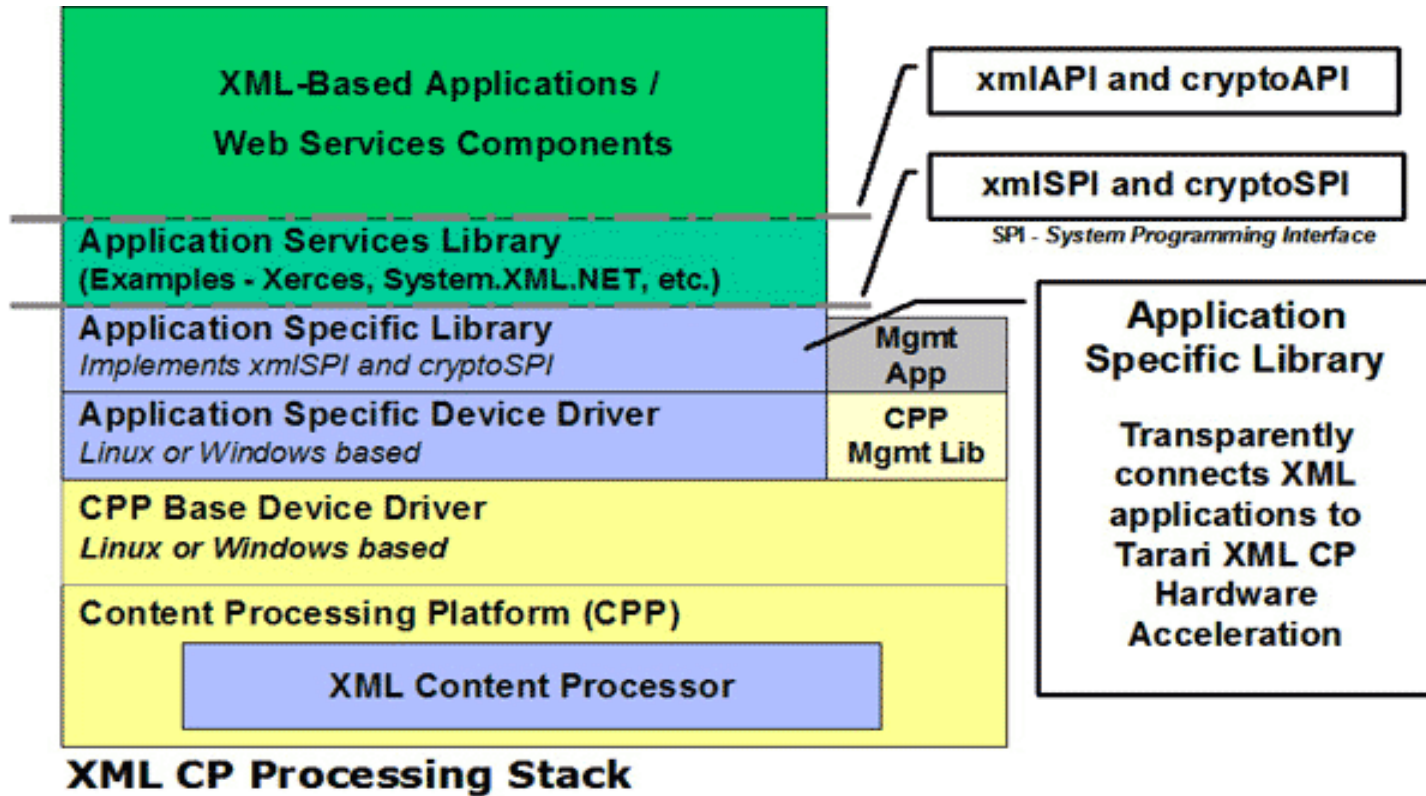
XACML Authorization



Access control evaluation



Tarari XML processor



Application attacks

- Buffer overflow
- Exceeding array bounds
- Misuse of pointers
- Downloaded active contents

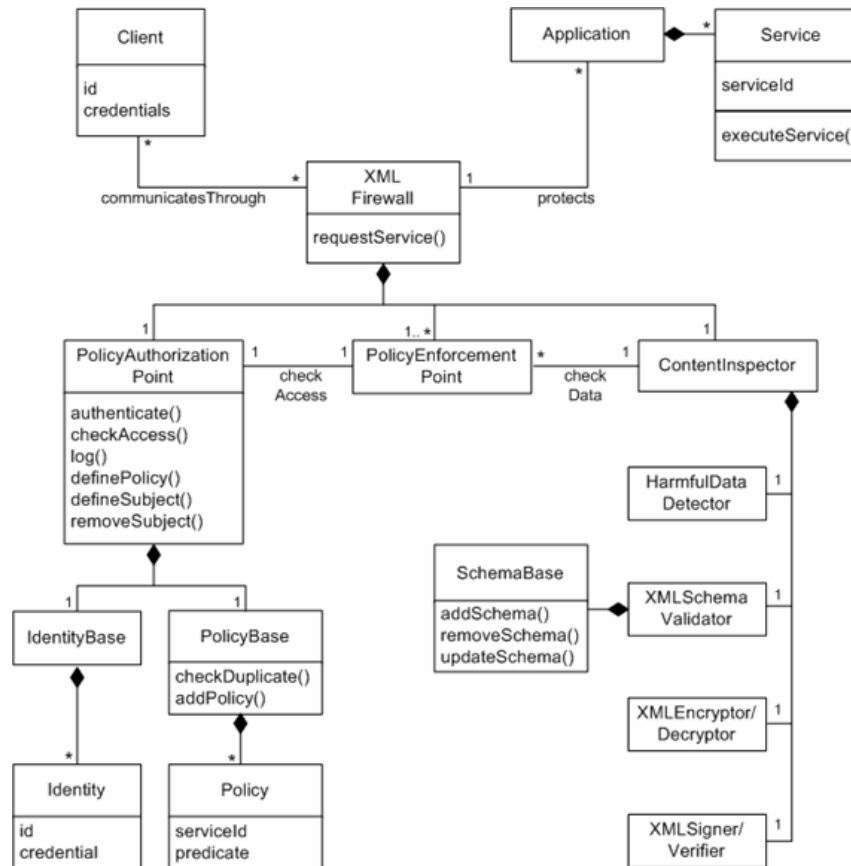
Application controls

- Apply access control to inputs and outputs
- Can check for parameter length, malformed inputs, ...
- Application firewalls
- XML firewalls for Web services

XML firewall

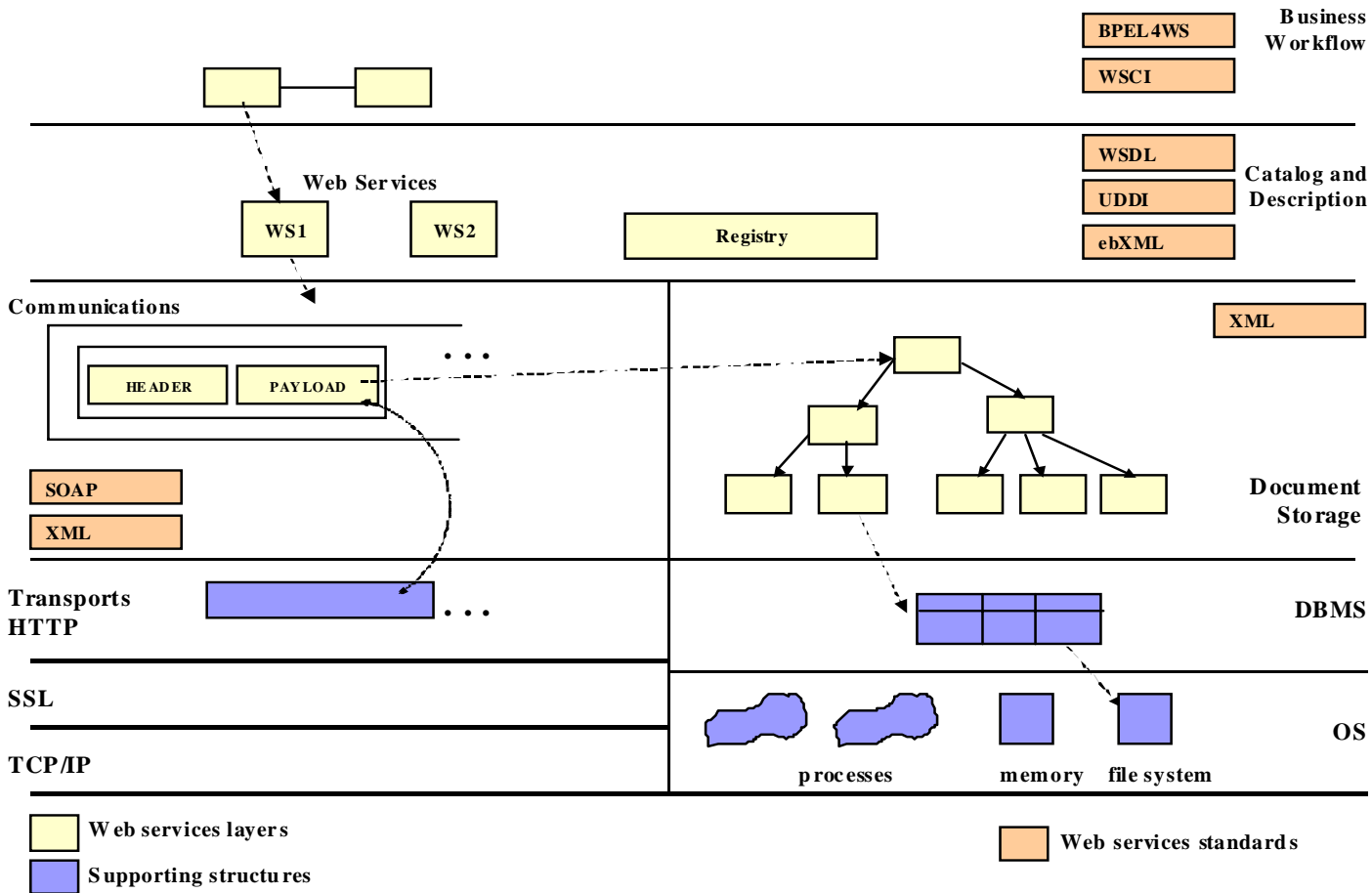
- Controls input/output of XML applications
- Well-formed documents (schema as reference)
- Harmful data (wrong type or length)
- Encryption/decryption
- Signed documents

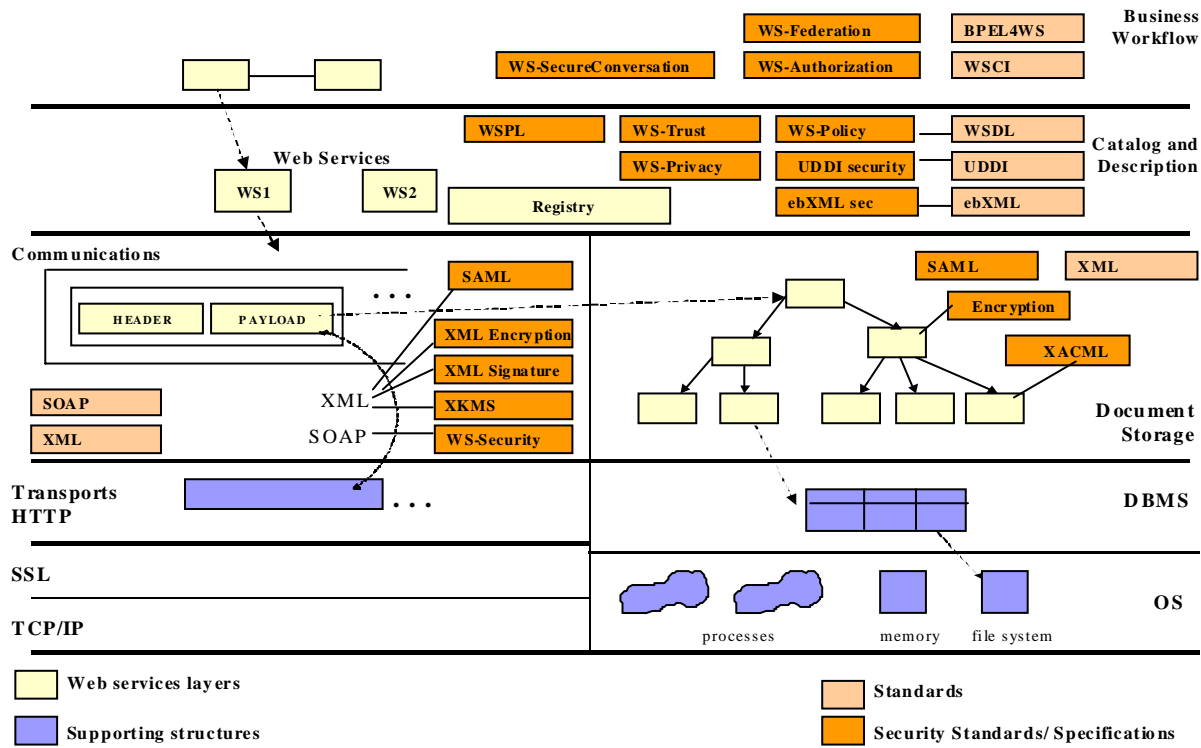
XML firewall pattern



Business workflow level

- New standard: Business Process Execution Language for Web Services (BPEL4)
- A language for the formal specification of business processes and interactions (Coreography)
- Allows WSs to perform business transactions (WS-Transaction)



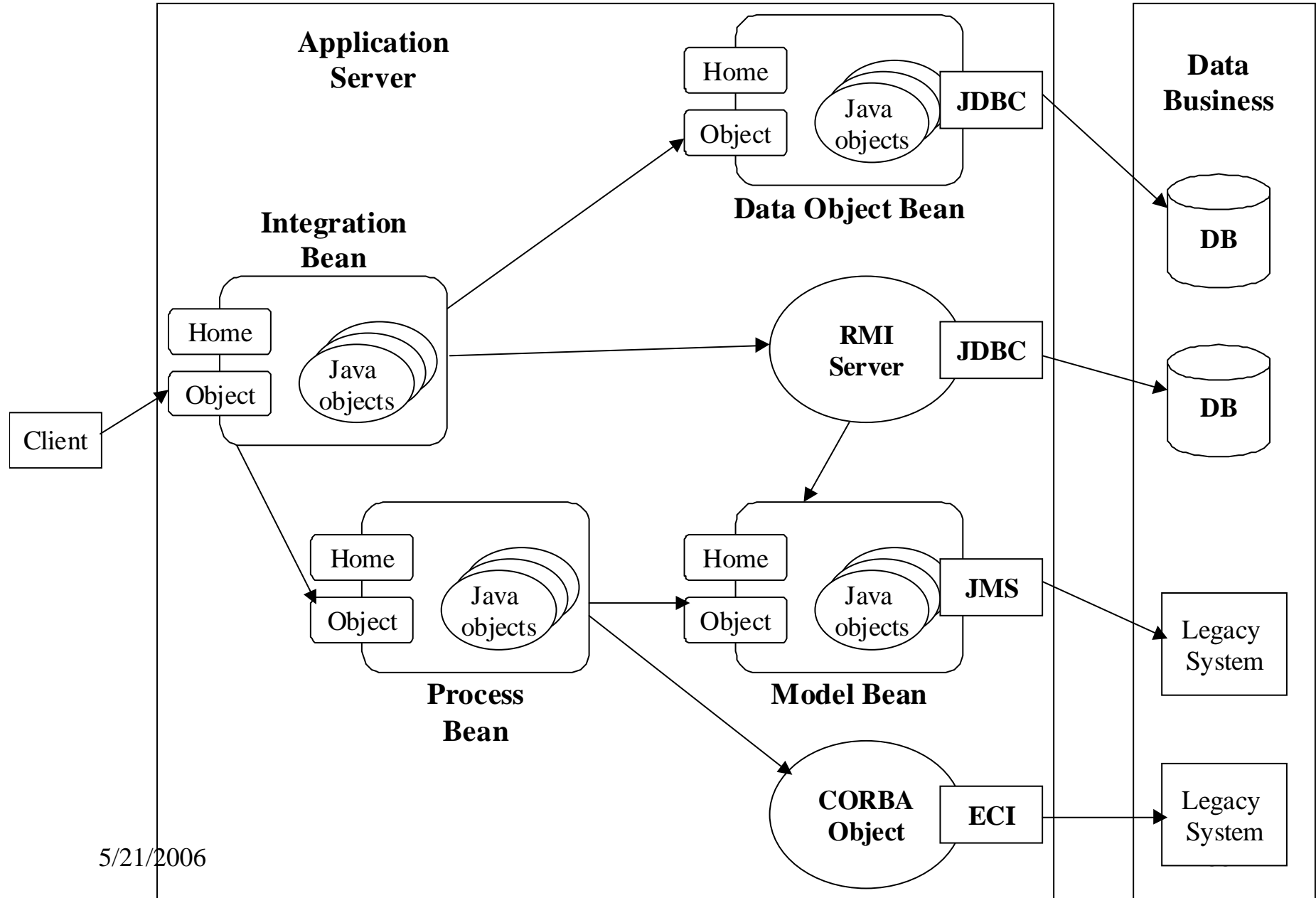


Web Application Servers

- Applications which interact with each other using web standards. Application servers are normally part of a 4-tier architecture including a client (typically a browser), an http server (for content management), an application server (components that implement a business model and access the data), and a data layer (corporate databases). Complementary systems include web portal servers, gateways for wireless devices and mail, and security directors.

Application Server and Integration

Integration via EJBs



Web services research

- Security models, including XACML
- Secure mappings between levels
- Patterns
- Conformance of standards
- Support infrastructure
- Formalization
- Wireless web services

Conclusions

- Internet-based systems are very useful and flexible, but also very complex and changing
- Complexity brings vulnerability
- Security must be defined at the high levels and mapped to low levels
- Use of OO and patterns is a promising way for designing secure systems

Two new books

- The design of secure systems (Addison Wesley)
- Security patterns (Wiley)



Markus Schumacher
Eduardo Fernandez-Buglioni
Duane Hybertson
Frank Buschmann
Peter Sommerlad

SECURITY PATTERNS

**Integrating Security
and Systems Engineering**



WILEY SERIES IN
SOFTWARE DESIGN PATTERNS