17. Security for Open Distributed Geospatial Information Systems

Andreas Matheus

This chapter gives a brief introduction to relevant security requirements and how they can be implemented based on standards. It is not the intention to provide individual solutions, as an adequate solution typically depends on many more factors than can be taken under consideration in this chapter. Instead, we like to see this as a starting point from where the reader can follow references to applicable standards for further reading.

Security for Geographic Information Systems (GIS) has gained in importance since Service-Oriented Architecture (SOA) has enabled the implementation of large distributed networks for the creation, processing, viewing, and maintenance of geographic information. Its main characteristic – as specified in [17.1] – is that SOA is a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains.

As such, SOA causes challenges to implementing effective security functions that take under consideration not only the traditional requirements existing from installing a GIS in one's own local area network with known and trusted users, but also communication with insecure network segments such as the Internet without knowing which computers and users have access to that network. Therefore, the traditional paradigm of *we are secure because we have a firewall* no longer holds, as with (web) services, requests can intrude into an internal system over firewall port 80 or over port 443 for Transport-Layer Security/Secure Sockets Layer (TLS/SSL) over Hypertext Transfer Protocol Secure (HTTPS). However, because there has to be an open port as an essential requirement for participating in a distributed processing system, the question exists of how to properly make one's own system secure and protect it from unauthorized access that might come in via that open firewall port. It is not the intention of this chapter to elaborate a holistic security approach that encompasses all existing requirements and evaluates all possible options to determine the best solution; rather, we will address aspects that provide better understanding of what it means and what needs to be done to make a geosystem secure for participation in a larger system.

When it comes to the decision that *we* intend to participate in a distributed geospatial information system, many questions arise related to security: What do we need to do to prevent unauthorized access to the geospatial information and services that we are going to provide? Which potential attacks are we facing, hence which threat models do we need to consider, and can we mitigate or prevent attacks? Can we build a solution based on standards, and which standards are applicable?

17.1 Security Requirements

Before we begin, it is essential to define what we mean by security in the context of this chapter: what it is and is not concerned with. *Security* is described as the characteristic of a system (whether distributed or not) that prevents unwanted, hence unauthorized, actions to be executed on the system itself with potential side-effects on information that is accessible via the system. The Trusted Computer System Evaluation Criteria, also known as *Orange Book* states [17.2]:

> *In general, secure systems will control, through use of specific security features, access to information such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information.*

Extending this definition for a single system to a distributed system which consists of multiple autonomous computers that communicate through a computer network, the communication shall not have any influence. This means that the capability of the system to prevent unauthorized access to the information needs to include the communication between the distributed systems.

The typical requirements that exist when securing a distributed system are described in ISO 10181 consisting of

- ISO 10181-1 *Overview* [17.3],
- ISO 10181-2 *Authentication* [17.4],
- ISO 10181-3 *Access control* [17.5],
- ISO 10181-4 *Non-repudiation* [17.6],
- ISO 10181-5 *Confidentiality* [17.7],
- ISO 10181-6 *Integrity* [17.8],
- ISO 10181-7 *Security audit and alarms* [17.9].

ISO 10181-1 describes the organization of security frameworks, defines relevant security concepts, and describes relationships of the services of the frameworks. To do this, it uses security architecture definitions from ISO/IEC 7498-2 [17.10], such as access control, availability, denial of service, digital signature, and encryption. It also provides other relevant definitions such as security information, security domain, security policy, trust entities, trust, and trusted third parties, and for the security information it defines security labels, cryptographic check values, security certificates, and security tokens. In addition, it defines denial of service and availability in such a sense that denial of service cannot always be prevented. In these cases, other security services can be used to detect the lack of availability and allow the application of corrective measures. Annex A of 10181-1 provides an example of protection measures for security certificates and defines the key management framework, as its functions are applicable to any information technology environment where digital signatures and encryption are used.

ISO 10181-2 defines all aspects of authentication in open systems and the relationship with other security functions such as access control.

ISO 10181-3 defines all aspects of access control in open systems as it applies to the interactions of user with processes, user with data, process with process, and process with data. It also defines the relationships to other security functionality such as authentication and audit.

ISO 10181-4 refines all aspects of nonrepudiation and extends the concepts defined in ISO/IEC 7498-2.

ISO 10181-5 defines confidentiality as a service *to protect information from unauthorized disclosure* in retrieval, transfer or management.

ISO 10181-6 defines integrity as a property that *data has not been altered or destroyed in an unauthorized manner.* This applies to data in retrieval, transfer or management.

ISO 10181-7 defines the basic concepts of a general model for and identifies relationships between services for security audit and alarms.

When it comes to classified information, and in the geospatial domain you can find examples for classified information quite easily, additional requirements exist that extend the typical access control requirements where rights are associated to users either directly or by role to ensure the confidentiality of the information and its integrity, including security labels.

Information flow control models such as the Bell–La Padula [17.11] and Biba models [17.12] are relevant as outlined in RFC 1457 [17.13].

To guarantee the confidentiality of classified information, *The Orange Book* names the Bell–La Padula (information flow control) model [17.2] that defines secure state, modes of access, and rules that grant/deny access. It ensures that classified information is not flowing from higher classification to lower classification. Therefore, the model is also known for its main purpose: *no read up – no write down*.

The Biba model addresses integrity of information by defining conditions to ensure: *no read down – no write up*.

17.1.1 Thinking About the Threats – Who Is the Enemy?

Before thinking of a particular implementation of security functions, it is essential to think about the relevant, and hence applicable, security requirements. Perhaps it is not always relevant to implement them all. To determine this, the question of which potentially threats exist must be asked. There is a big difference if you consider the *Internet threat model* and/or the *browser threat model* as a relevant cause for any attacks to your system.

With the Internet threat model, it is considered that the communicating end systems can be trusted, but that the communication is unsafe. As defined more precisely in RFC 3552 [17.14], the attacker has control of the communications channel over which the end systems communicate, and the attacker can read any protocol data on the network and undetectably remove, change, or inject forged information.

In addition to the defined Internet threat model, other threats exist that relate to browsing the Internet that are sometimes listed under the umbrella of the browser threat model. This model considers that the client – the browser application running on an end system, for example – and its user are vulnerable to attacks such as phishing, identity theft, etc.

Without elaborating on this in more detail, it is important to understand which of the listed requirements are important and which standards are applicable to build the solution.

17.1.2 Which Requirements Are Geo-Specific?

From the requirements stated in ISO 10181 (all parts), the requirement for access control is geo-specific. This has to do with the characteristic of the information: Attributes of the information objects as well as the user can hold geometry information that represents the location, extent, etc. of the object or user. For geospatial data and services, use cases exist that require the declaration and enforcement of access rights based on the

- location of the subject, or
- geometry of the object (resource), or
- location of the subject and the geometry of the resource, or
- topological relations between geometries, or
- results of complex processing on geometries.

17.2 Standards for Interoperable Implementation of Security Functions

When it comes to implementation of security functions, it is a particularly good idea to review existing standards to determine whether there is not (at least) one that can be used. Why? Because many experts have found a keen and practical solution to a problem, and typically software exists – in the form of either libraries or even larger software packages – that have implemented the standard (Chap. 13).

Figure 17.1 provides a first overview of security-related standards that are applicable to secure a distributed geospatial information system based on web services supporting implementation of the listed requirements. It is worth mentioning that actually one geo-specific specification from the Open Geospatial Consortium (OGC) exists: GeoXACML (geospatial extensible access control markup language). We will elaborate more on GeoXACML in a later section.

Figure 17.1 is structured such that it categorizes the standards and stacks the layers in a similar way as the open systems interconnection (OSI) model [17.15].

The Internet Engineering Task Force (IETF) RFCs (request for comments) IPSec (Internet Protocol Security) [17.16] and TLS/SSL [17.16] are applicable to actual OSI (Open Systems Interconnection) network layers: IPSec falls into the OSI network layer, and TLS/SSL falls into the transport layer.

The IETF HTTP RFC [17.17] falls into the OSI application layer, as does SOAP (simple object access protocol) [17.18].

As SOAP enables communication using extensible markup language (XML) notation, the next layer above are the XML security standards which contain the W3C recommendations XML digital signature [17.19] and XML encryption [17.20].

The next category, message security, is concerned with enabling integrity and confidentiality in XML messages exchanged via SOAP messages. Here the most dominant standard is the OASIS (Organization for the Advancement of Structured Information Standards) WS-security [17.21]. As a supplement, one can see the relevance for expressing the requirements that a web service places on a client to establish communication. WSDL (Web services description language) [17.22], WS-policy [17.23], and WS-SecurityPolicy [17.24] provide these capabilities.

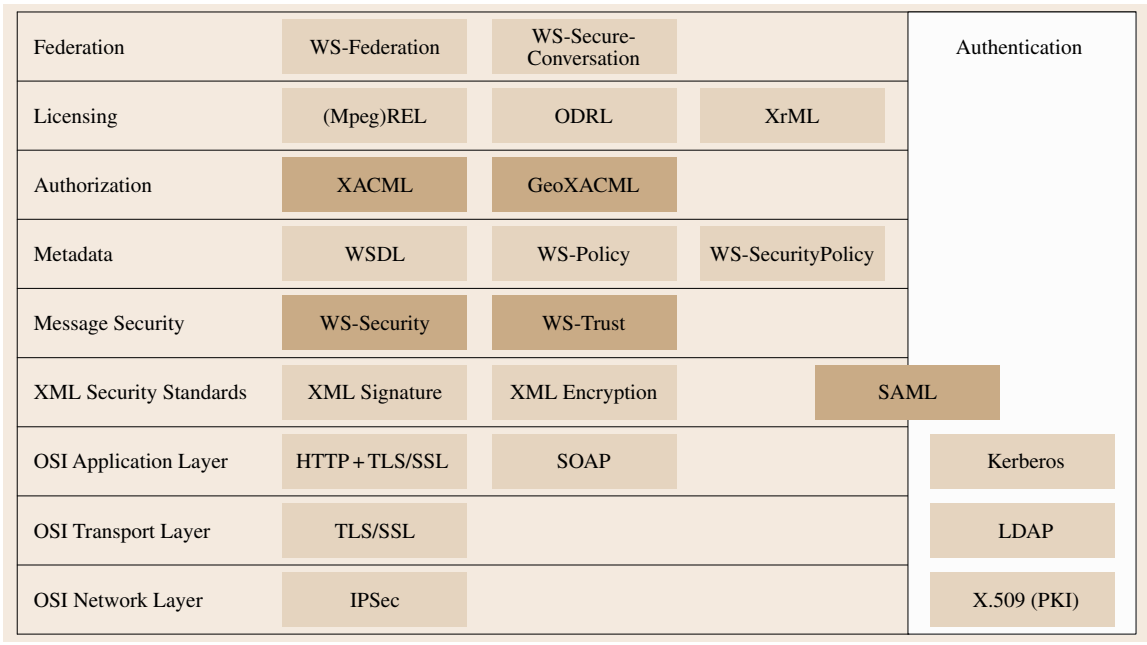

Fig. 17.1 Security standards overview (subset)

The next category, concerned with authorization, contains the OASIS XACML [17.25–27] and the OGC GeoXACML [17.28–30] standards. An extension to authorization is licensing, which is the next category up. It contains the ISO standard (Mpeg)REL (rights expression language) [17.31], OMA's (Outlook Mobile Access) ODRL (open digital rights language) [17.32] and content guards XrML (extensible rights markup language) [17.33].

Authentication is a cross-layer topic that mainly consists of the IETF RFC for X.509 [17.34] and OASIS SAML (Security Assertion Markup Language) standard [17.35–37]. Also, Kerberos [17.38] and LDAP (lightweight directory access protocol) [17.39, 40] for X.500 fall into this category.

17.2.1 Standards for Implementing Confidentiality and Integrity

Protecting the conversation between two entities can be implemented by leveraging functions from different layers of the OSI reference model; for example, IPSec as a secure extension to Internet Protocol (IP) that resides in layer 4 (network layer) can be used to encrypt the entire communication between communication end systems. Here, the application itself cannot control how the encryption is done, which is good on one side, as it takes away the burden from the application programmer to incorporate security functions. A kind of hybrid solution that involves the application partially but still encrypts the entire communication between end systems is TLS/SSL, which can be located in the OSI transport layer. For use cases that require more flexible control over the protection of XML structured communication messages or end-to-end protection, only functions that can be directly controlled by the application and applied to the XML message are feasible.

It is important to note that, for chaining of web services, where integrity and confidentiality span multiple intermediary services, end-to-end protection is required, and therefore WS-security-based protection should be applied. Point-to-point protection, as provided by the transport layer, is not sufficient, as information is available in the clear on the intermediary services (Fig. 17.2).

WS-security is a standard by OASIS that can be associated with the application layer of the OSI reference model. It defines how to use XML digital signature and XML encryption on SOAP messages to ensure confidentiality and/or integrity. Because how and which parts of the message are protected can be controlled by the application in a very flexible manner, WS-security comes into play, as it defines exact patterns for applying a digital signature to an XML document (or parts of it)

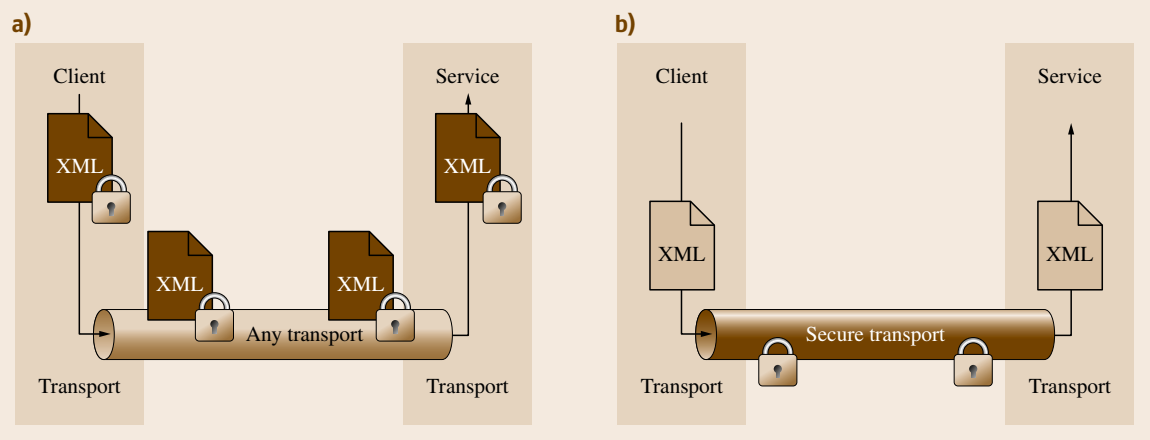

Fig. 17.2a,b Transport layer (a) versus application layer (b) integrity/confidentiality

and how to encrypt parts of the document and create the relevant metadata for the receiver in XML to undo the encryption or use signed hash values to check integrity. As a full introduction to WS-security and the related standards would exceed the size of this chapter, the interested reader is encouraged to follow the links given in the references section.

17.2.2 Standards for Implementing Authentication

The security assertion markup language (SAML) is an OASIS standard that first of all specifies a markup language for describing assertions about a subject. SAML distinguishes between three different types of assertions.

1. *Authentication assertion*, which provides information about the asserted subject regarding the means by which a subject was authenticated, by whom, and at which time;
2. *Attribute assertion*, which provides information about the characteristics of the asserted subject;
3. *Authorization assertion*, which states that access to a particular resource is permitted or denied for the asserted subject.

SAML is one ideal standard to implement authentication in distributed systems, where the user (principal) is known by the identity provider (asserting party) and the protected services are hosted by the service provider (relying party). These two are typically separate entities. To establish secure exchange of assertions concerning the identity of and additional information regarding the user between these parties, SAML specifies profiles and bindings. XML digital signatures and XML encryption or both can be applied to guarantee the integrity and or confidentiality of the assertions. The most important profiles are (not ordered)

- *Assertion query and request protocol*, which defines the processing rules for how existing assertions can be queried and the structure of the messages.
- *Authentication request protocol*, which enables the relying party to request assertion statements about the means by which a subject was authenticated.
- *Artifact resolution protocol*, which defines how SAML artifact references can be exchanged instead of the assertions itself.
- *Name identifier management protocol*, which defines how an asserting party can change the name of an identifier that was previously established and is been used by relying parties.
- *Single logout protocol*, which defines a sequence of message exchange with the goal of terminating all existing sessions of the subject with other relying parties in close to real time. However, there is no confirmation message because the logout with all relying parties cannot be guaranteed.
- *Web browser SSO profile*, which defines how a Single-Sign-On (SSO) can be established using a (regular) web browser as the client.
- *Enhanced Client or Proxy (ECP) profile*, which defines the exchange of request/response messages for a client (not a web browser) that knows which asserting party to contact.
- *Identity provider discovery profile*, which defines mechanisms by which a relying party can discover

which asserting parties a principal uses for the *web browser SSO profile*.

The actual use of one or more of these profiles depends on the deployment environment for the services. To accommodate different characteristics, SAML defines multiple bindings for the profiles listed above.

- *SAML SOAP binding*, which defines how SAML assertions are to be exchanged using SOAP messages and how SOAP header elements are to be used to do so.
- *Reverse SOAP (PAOS) binding*, which describes a mechanism where the client is able to act as a SOAP relay relevant for implementing the ECP profile.
- *HTTP redirect binding*, which enables the exchange of SAML messages as Uniform Resource Locator (URL) parameters. To ensure the length limit of a URL is not exceeded, message encryption is used. This binding is relevant where HTTP user agents of restricted capabilities are involved in the message exchange.
- *HTTP POST binding*, which defines how SAML messages can be sent inside a (X)HTML form using base64 encoding.
- *HTTP artifact binding*, which defines how SAML request and response messages are exchanged using a reference – an artifact. This binding is essential for implementing the *artifact resolution profile*.

It is worth mentioning that the applicability of a binding depends on the identified threat model: The Internet threat model allows leveraging of any profile, whereas the browser threat model mandates the artifact profile. This is because the artifact profile requires a secure *back-channel* between the service and the identity provider to exchange the actual assertion(s). The client just gets hold of the artifact, which is a protected, Internet-wide unique reference to associated assertion(s). However, because the client is missing the keys to set up a trusted back-channel with the identity provider, this profile is safe even if the attacker has prepared the client to intercept and wire-tape the communication. With the browser POST profile, for example, the user assertion(s) is (are) pushed from the identity provider to the service provider through the client. A manipulated client could fetch the assertions and potentially use them for performing attacks.

An alternative approach using a secure token service (STS) is defined in WS-trust [17.41]. Web services trust (WS-trust) is an OASIS standard that defines extensions to WS-security for managing (issuing, renewing, canceling, validating) security tokens for the purpose of establishing brokered trust relations between web services of communication partners through the exchange of secured SOAP messages. To support brokered trust, this standard introduces the concept of a STS. To use the STS in an interoperable way, XML message formats are defined. It is important to note that this specification does not define any security token types. It specifies how to deal with them to establish trust between web services and or clients of not directly trusted communication partners.

17.2.3 Standards for Implementing Access Control

The major concern of access control is to prevent unauthorized use or disclosure of protected information. The typical solution is to assign identity rights on objects for particular actions that can be invoked on the object. This is a very challenging task already and becomes even more complicated for a distributed system, because harmonization of access rights across jurisdictions requires a language so that rights declared by one party can be interpreted unambiguously by another involved party.

The Extensible Access Control Markup Language (XACML) by OASIS defines such a language to support the declaration of access rights in XML. It is also possible (of course) to derive authorization decisions based on the rights declared in the policy and an authorization decision request. As the service that derives the decisions (a so-called PDP, policy decision point) can be deployed as an autonomous service, XACML defines the interface and the message format for the XACML authorization decision request and the XACML authorization decision response. XACML further defines different profiles, among which the role-based access control (RBAC) profile defines how to model RBAC0 (pure RBAC) and RBAC1 (role inheritance) [17.42] in an XACML policy. It is important to note that XACML also supports the Bell–La Padula and Biba models to ensure valid information flow control. Through the use of obligations, it is possible to create events for security audit and alarms.

The request to a protected resource is intercepted by the policy enforcement point (PEP). Before the protected resource can be accessed, the PEP involves the context handler to obtain all information relevant to construct a XACML authorization decision request to the policy decision point (PDP). This can involve fetching resource information, and information on the user

and the environment through a policy information point (PIP). The PDP, on receiving the authorization decision request, derives an authorization decision based on available policy(ies). The decision is sent back to the PEP, which permits or denies the intercepted request. A decision received from the PDP can optionally contain an obligation, which is to be executed when permitting or denying the request. The policy administration point (PAP) is not involved in runtime processing, as it provides an administrative interface for the creation and maintenance of policies.

As the declaration and enforcement of geo-specific access rights is not supported by XACML, the OGC has released a geo-specific extension to XACML 2.0 called geospatial extensible access control markup language (GeoXACML) 1.0, which builds on top of XACML by using the available extension points. It extends XACML 2.0 by defining the data type *Geometry* and geo-specific functions based on ISO 19125-1 *Geographic information – Simple feature access – Part 1: Common architecture*, which is identical to OGC document #06-103r3 [17.43]. The functions allow testing and processing of geometries involved in the process of deriving an authorization decision.

Topological functions allow testing of the topological relation between two geometries; *bag and set functions* allow construction of results or test conditions based on a collection of geometries. Note that the XACML standard defines a bag as an unordered collection of elements with possible duplicates, whereas a set is considered free of duplicates. *Geometric functions* contains constructive and scalar functions for processing new geometries or to request characteristics of a geometry. Finally *conversion functions* (not from ISO 19125-1) support the conversion of length and area values to meters, the mandatory unit of measure.

GeoXACML defines two conformance classes that apply to an implementation of the policy decision point (PDP) as it is a part of the XACML standard informative component diagram (Fig. 17.3). The conformance class BASIC requires a PDP implementation to support the functions listed as topological, bag/set, and conversion functions. The STANDARD implementation of a PDP requires implementation of all functions

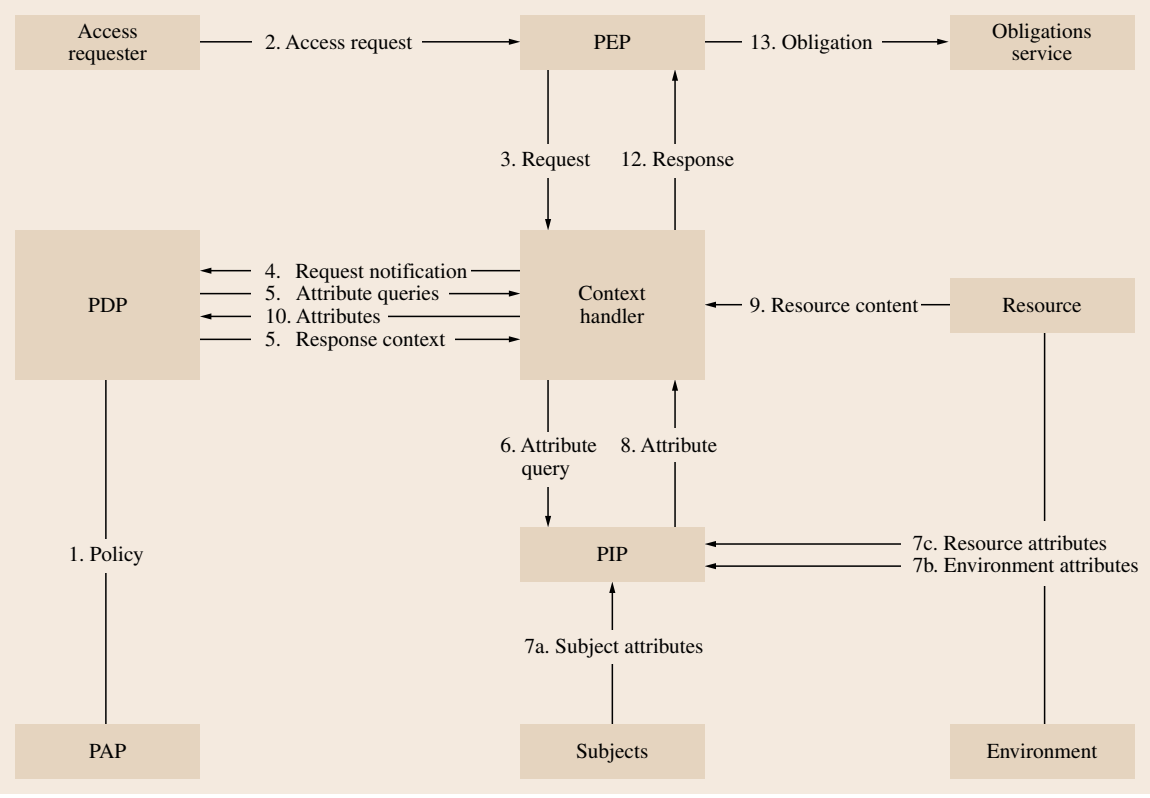

Fig. 17.3 XACML information flow

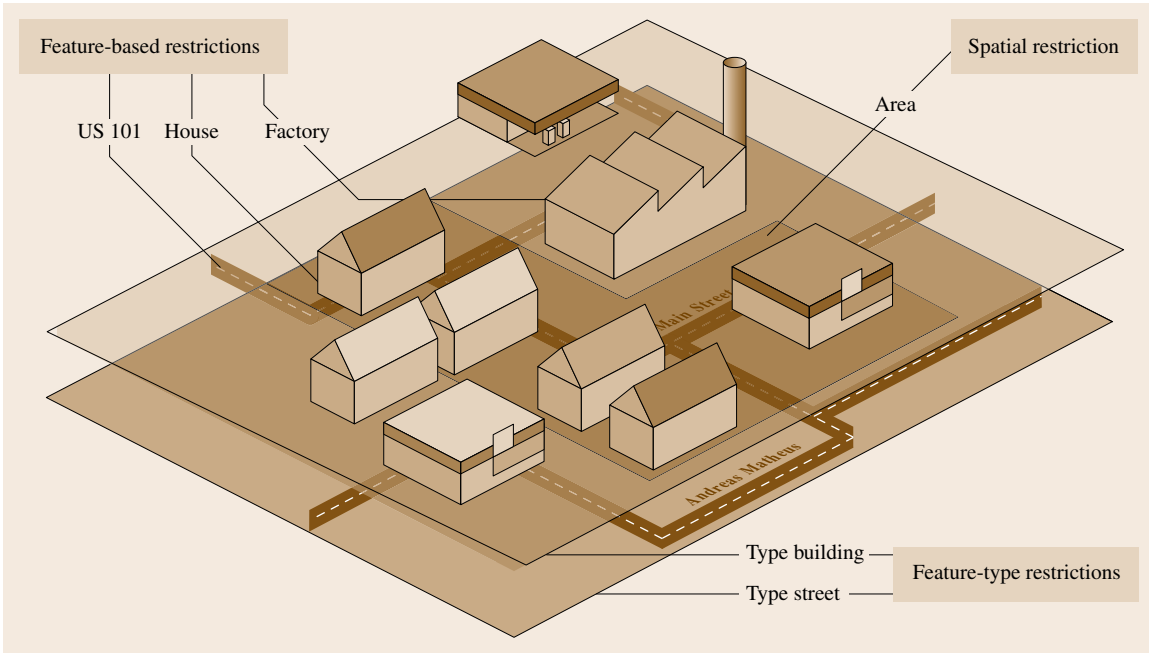

Fig. 17.4 GeoXACML access right example

mandatory for the BASIC conformance class plus the functions listed as geometric functions. In addition, a BASIC or STANDARD implementation must also implement at least one extension (or perhaps all). Currently the GeoXACML 1.0 core specification is accompanied by two extensions that support the OGC standards GML2 [17.44] and GML3 [17.45] encoding of geometries. Because GeoXACML defines an extension to XACML, all of its profiles can be used with GeoXACML too.

Figure 17.4 summarizes the typical capabilities of GeoXACML to control access to a geographic feature.

Rights can be associated with feature types, a particular area, or individual features, as illustrated in Fig. 17.4. As these different types of rights can be combined in any way, one can create very flexible and relevant access policies. One example that does combine all three types could permit access for the feature type *Building*, where all buildings must be inside a given spatial area, but the feature with the name *house* is exempt. This example right could be extended by user location such that the right is only permitted if the user is within the given area and on the feature *Street US 101*. Also, geo-specific rights can be declared by combining nongeographic and geographic attributes to establish the need-to-know principle: A first responder (at the scene) can see requested features even if they are classified, as long as his location is within a distance of 1 km around the hotspot center; he cannot request those features from his office.

17.3 Summary

Securing a distributed geospatial system mainly involves non-geo-specific standards – it requires knowledge of mainstream information technology (IT) to leverage existing standards and implementations in an appropriate way. In this chapter, we introduce an important set of standards covering this subject. The only identified requirement that is geo-specific is access control. Here, an existing standard from the OGC supports the declaration and enforcement of access rights for geographic information.

References

17.1 OASIS: Reference Model for Service Oriented Architecture 1.0, OASIS Standard (2006) http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf

17.2 United States Government Department of the Defense: Trusted Computer System Evaluation Criteria (1985)

17.3 ISO/IEC 10181-1:1996, Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=24404

17.4 ISO/IEC 10181-2:1996, Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18198

17.5 ISO/IEC 10181-3:1996, Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18199

17.6 ISO/IEC 10181-4:1996 Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=23615

17.7 ISO/IEC 10181-5:1996, Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=24329

17.8 ISO/IEC 10181-6:1996, Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=24330

17.9 ISO/IEC 10181-7:1996, Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18200

17.10 ISO 7498-2:1989, Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture

17.11 D.E. Bell, L.J. LaPadula: *Secure Computer Systems: Unified Exposition and Multics Interpretation*, MTR-2997 Rev. 1 (MITRE Corp., Bedford 1976)

17.12 K.J. Biba: *Integrity Considerations for Secure Computer Systems*, MTR-3153 (MITRE Corp., Bedford 1977)

17.13 IETF RFC 1457: Security Label Framework for the Internet (1993) http://tools.ietf.org/pdf/rfc1457

17.14 IETF RFC 3552: Guidelines for Writing RFC Text on Security Considerations (2003) http://tools.ietf.org/pdf/rfc3552

17.15 ITU-T: X.200: Information technology – Open Systems Interconnection – Basic Reference Model: The basic model (1994) http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.200-199407-I!!PDF-E&type=items

17.16 IPSec: IP Security – IETF RFC 4301 (2005) (sobo-letes RFC 2401 from 1998) http://tools.ietf.org/html/rfc4301

17.17 HTTP: IETF RFC 2616 (1999) http://tools.ietf.org/html/rfc2616

17.18 SOAP: Simple Object Access Protocol (SOAP), W3C Recommendation, 2nd edn. (2007) http://www.w3.org/TR/soap/

17.19 XML Digital Signature: XML-Signature Syntax and Processing – W3C Recommendation (2002) http://www.w3.org/TR/xmldsig-core/

17.20 XML Encryption: XML Encryption Syntax and Processing – W3C Recommendation (2002) http://www.w3.org/TR/xmlenc-core/

17.21 Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) – OASIS Standard Specification (2006) http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

17.22 WSDL: Web Services Description Language (WSDL) 1.1, W3C Note (2001) http://www.w3.org/TR/wsdl

17.23 WS-Policy: Web Services Policy 1.5 – Framework, W3C Recommendation (2007) http://www.w3.org/TR/2007/REC-ws-policy-20070904/

17.24 WS-SecurityPolicy: WS-SecurityPolicy 1.2, OASIS Standard (2007) http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.pdf

17.25 XACML: eXtensible Access Control Markup Language (XACML) Version 2.0, OASIS Standard (2005) http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

17.26 XACML RBAC Profile: Core and hierarchical role based access control (RBAC) profile of XACML v2.0, OASIS Standard (2005) http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf

17.27 XACML SAML Profile: SAML 2.0 profile of XACML v2.0, OASIS Standard (2005) http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-saml-profile-spec-os.pdf

17.28 GeoXACML: Geospatial eXtensible Access Control Markup Language (GeoXACML) v1.0, Open Geospatial Consortium, Inc. (2008) http://portal.opengeospatial.org/files/?artifact_id=25218

17.29 GeoXACML Extension A: Geospatial eXtensible Access Control Markup Language (GeoXACML) Extension A – GML2 Encoding Version 1.0, http://portal.opengeospatial.org/files/?artifact_id=25219
17.30 GeoXACML Extension B: Geospatial eXtensible Access Control Markup Language (GeoXACML) Extension B – GML3 Encoding Version 1.0, http://portal.opengeospatial.org/files/?artifact_id=25220
17.31 REL: Information technology – Multimedia framework (MPEG-21) – Part 5: Rights Expression Language, ISO/IEC 21000-5:2004, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36095
17.32 ODRL: Open Digital Rights Language (ODRL) Version 1.1, W3C Note (2002) http://www.w3.org/TR/odrl/
17.33 XrML: XrML - eXtensible rights Markup Language, ContentGuard, http://www.xrml.org/
17.34 X.509/PKI: IETF, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (2008) http://tools.ietf.org/html/rfc5280
17.35 SAML: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard (2005) http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
17.36 SAML-Bindings: Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard (2005) http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
17.37 SAML-Profiles: Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard (2005) http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
17.38 Kerberos: The Kerberos Network Authentication Service (V5) – IETF RFC 4120 (2005) obsoletes 1510 (1993) http://tools.ietf.org/html/rfc4120
17.39 LDAP: Lightweight Directory Access Protocol (LDAP): The Protocol – IETF RFC 4511 (2006) http://tools.ietf.org/html/rfc4511
17.40 IETF: The X.500 String Representation of Standard Attribute Syntaxes: IETF RFC (1993) http://tools.ietf.org/html/rfc1488
17.41 WS-Trust: WS-Trust 1.3, OASIS Standard (2007) http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf
17.42 D.F. Ferraiolo, D.R. Kuhn: Role-based access control, 15th Natl. Comput. Secur. Conf. (1992) pp. 554–563, http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-kuhn-92.pdf
17.43 OGC: OpenGIS Implementation Specification for Geographic information – Simple feature access – Part 1: Common architecture (2006) http://portal.opengeospatial.org/files/?artifact_id=18241
17.44 OGC: OpenGIS Geography Markup Language (GML) Implementation Specification, version 2.1.2, http://portal.opengeospatial.org/files/?artifact_id=11339
17.45 OGC: OpenGIS Geography Markup Language (GML) Encoding Standard, version 3.2.1, http://portal.opengeospatial.org/files/?artifact_id=20509