RESEARCH ARTICLE OPEN ACCESS

Privacy Threat Modelling And Analysis in Access Control Context

U. M. Mbanaso, Ph.D.
Centre For Cyberspace Studies, Nasarawa State University, Keffi, Nigeria
Corresponding Author: U.M.Mbanaso,phd

ABSTRACT
Privacy is concern that must be addressed whenever personal identifiable information (PII) is involved in information systems. Notably, access controlmechanisms make use of PII to determine privileges assigned to users in typical access control scenario, which, potentially puts it at risk. This paper examines privacy issues in access control using Threat Modelling and Analysis approaches. The outcome helps to situate privacy concerns when designing access control engines.

Date of Submission: 24-11-2017 Date of acceptance: 11-12-2017

I. INTRODUCTION

Threat modelling is a formal approach that attempts to uncover application level security threats and vulnerabilities to determine the possibility of risk thresholds [1]. In the investigation, three factual elements, (i.e. privacy, confidentiality and trust) are the variables central to the study. It is important to deconstruct them subjectively to distinguish their characteristics, and further put their relationships in the proper context. For this purpose, the following definitions are assumed.

- Confidentiality is that notion concerned with making sure that only an entity with the right privileges gains access to protected resources.
- Privacy is that notion of ensuring that the legitimate entity that has gained access to protected PII treats the PII trusted to it with respect to the providing party's security preferences.
- Trust is that means to establish the confidence that a resource consuming entity will act in a predictable and/or expected way.

Analyzing the above definitions, prevailing causal assumptions underscore the probability that a legitimate entity may have access to controlled resources, but abuse them by using the resources for other purposes than those originally stated [2]. This phenomenon could be intentional or unintentional; whichever is the case, the potential exists for a privacy violation, bringing anticipated threats into focus [3].

In retrospect, it can be deduced that confidentiality ensures that parties with the appropriate level of access privileges can gain access to restricted resources; but after the access, what they do with the resources has to be addressed by privacy mechanisms [4]. In the privacy context, no subsequent use of resources other than for the originally stated purposes is a contractual obligation that must be respected by parties [5, 7].

Trust on the other hand is the element that focuses on expected behaviour, i.e. the expectation that the communicating parties will act mutually and compatibly without incurring risks to each other based on the trust threshold provided by their properties or attribute-information [6]. Furthermore, this brings the requirement that in distributed transactions involving two or more autonomous security domains, more security constraints are necessary for effective resource control, since requirements can rarely be static. This suggests that authorization and trust establishment have to be treated dynamically, as remote enforcement of obligating constraints is more exigent. To validate the above empirical assumptions, a use-case based on a classic e-procurement service within the construction industry is modelled. The objective is to capture the variables from various interactive steps and deduce successive message flows in order to determine the likely threats to privacy and confidentiality.

The E-Procurement Use-Case

During the procurement phase of a construction project, the main contractor initiates a process aimed at ordering the products, materials and components essential for the construction of the building project. The contractor defines his product needs and publishes a call for tender at a dedicated web service portal aimed at potential product suppliers. The establishment of the call triggers a bidding process, and product suppliers can access the portal to search for calls appropriate to them and make offers, based on the publisher's requirements and other security constraints. Subsequently, the contractor can retrieve all the offers, analyse and rank them accordingly to determine suitable offer(s) before placing a purchase order.

Shown in figure 1 is the basic architecture illustrating the three main participants, possible trust relationship boundaries and typical flows of messages? In the above procurement scenario, certain transactional and security characteristics have to be identified to facilitate the modelling and analysis of the security threats. From the architectural point of view, the following assumptions can be made:

- Three main actors exist, namely; the contractor or supplier, the Security Token Service/Attribute Authority (STS/AA) and the portal services-Tender Call Broker (TCB), with each playing a distinctive but sometimes similar role in separate interactions.
- The contractors and suppliers can act as service clients, and in some instances implicitly as service providers, and have similar characteristics in terms of service interactions.
- The TCB and STS are trusted 3rd parties, and can belong to a particular construction consortium and/or geographical area, but can be multiple and/or federated. The TCB is an intermediary or service discovery broker, which provides a service interface on behalf of the suppliers and contractors, and is governed by a set of defined rules and procedures, to facilitate administration of tenders and biddings. Additionally, the TCB is a platform that provides the federation for trust establishment among participants.

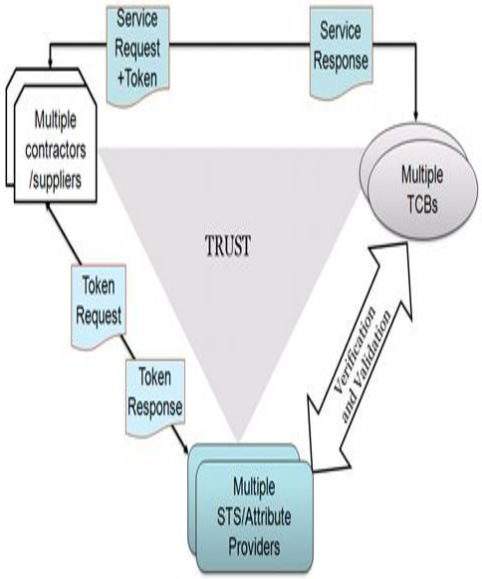

Figure 1 Roles in e-Procurement Use-Case Architecture

- Contractors and suppliers may not necessarily have a previous trust context before the invocation of services or belong to the same TCB and/or STS.
- The participants can exist in multiples with or without the existence of direct trust relationships, but mutual trust should be established before they can exchange sensitive resources.
- The various participants may have properties and/or identity-information that requires privacy and confidentiality protection.
- Either a human user or a software entity, can initiate the process, and has similar properties and/ or identity-information.

In figure 2 the basic architecture is shown plus the underlying steps involved.

1 The client prepares a service request message with a suitable software application. It initializes and presents an authentication request to its local authentication provider -STS/AA. The client presents an identifier or proof-of-possession in the form of a username/password pair to perform this phase.

1 The STS/AA authenticates the client's claim(s), to verify and validate its identity or confirmation that the client has successfully authenticated with another trusted broker (if in a federation). The STS/AA can determine whether to issue a security token based on the local policy, and if the client belongs to a particular role i.e.

membership role, the STS/AA issues a security token and passes it to the client.

2 The client packages the web service message with the token and makes a service request to the TCB portal. In the case of a contractor, it is attempting to publish a call-to-tender, whereas the supplier would be attempting to retrieve some tender calls.

3 The TCB portal through its security handler sends a validation request or asks for more attributes of the client, to determine the access rights of the requesting client.

4 The STS/AA processes the validation request or attributes request and presents an appropriate response to the TCB.

5 The TCB validates the STS/AA response, completes the client's request and sends an appropriate response to the client. For example, in the case of a supplier attempting to retrieve calls, it needs to match the request against the advertised policy of the contractor that placed the call, and determine whether this supplier can be allowed. A contractor may place certain constraints on potential suppliers, which can act as initial filter, i.e. the supplier must possess membership of certain consortium and a proof of annual turnover of a certain amount. On the other hand, a supplier may place similar obligating constraints on the contractors, i.e. validity period of bids (in privacy terms: maximum retention period). Some or a subset of these contractual obligating constraints can be advertised in the web service policy, if desirable.

In practice, a contractor client retrieves the bids, analyzes and selects the one that best suits its criteria and places an order for the goods. It is expected that the above steps would be followed by either the contractor or supplier, and the TCB must ensure that the contractor retrieves only the call-to-tender it has advertised.

The above interactions give rise to some empirical deductions and understanding, which can be summarized as follows:

1. The interactions involve client initiators making a service request to protected services that require access control measures. The resource release is governed by access control rules that determine who does what and when. The owners of the resources may advertise their complete policies or subset of their policies and other obligating constraints.
2. Several assets of the actors are involved and may require privacy and confidentiality. These include conventional resources; participants' attribute information; meta-information; and contractual business level information.
3. The actors may not all share a common security domain, so trust establishment is a critical factor in the overall interactions, and is paramount to the security of the web services conversations.
4. An actor can place obligating constraints on a participating party, and should be able to say what it is able and willing to do for the other party.
5. The TCB is a service broker governed by an enforceable set of rules and procedures.

Figure 3 shows a simple Data-Flow Diagram (DFD) in the context of XACML distributed actors, and gives a detailed description of the flow of messages from one XACML actor to another. Here, the STS/AA replaces the PIP. The above understanding exposes the fact that the client initiator is scared to submit all attribute information pertaining to the request at one go, so it considers leaving out sensitive attribute information in the initial service invocation. In contrast, the service is unable to allow access to the initiator without the complete set of attributes that will satisfy the access rules. Decomposing the DFD, security vulnerabilities[1] and threats can be identified particularly within the untrusted interactions. Outlined below is a summary of identified threats in the context of the use-case with respect to privacy and confidentiality.

[1] Here, security vulnerabilities are considered purely in the context of the thesis; other inherent security vulnerabilities are assumed to have been dealt with in other related work.

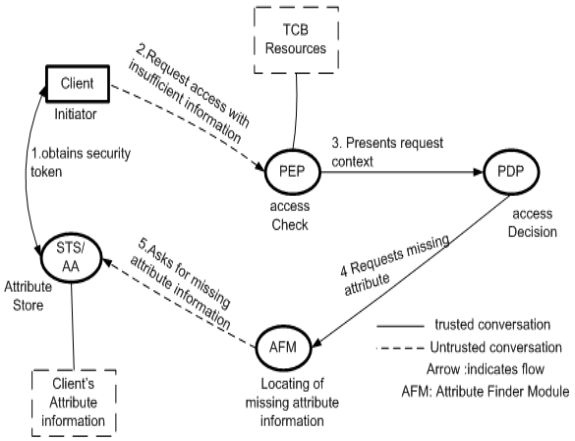

Figure 3: Data-Flow Diagram (XACML Distributed Context)

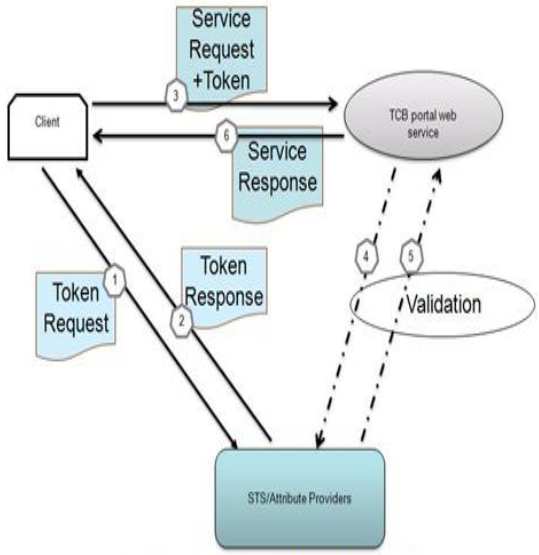

Figure2: Use-case actors' Interactions

***Undesirable Information Disclosure*:** It may be desirable to restrict some calls-to-tender to certain groups of suppliers or consortia. The bids need to be kept secret until the close of the call; in this case, the suppliers' offers are vulnerable to undesirable exposure i.e. a supplier entity may require that its bid be handled with utmost confidentiality, and not disclosed to competitors before the close of the call. For example, a malicious contractor can retrieve a call-to-tender it did not publish, or a supplier may gain access to a competitor's offer. From the viewpoint of privacy principles, requirements that can be deduced from these scenarios include the notions of *use limitation. choice/consent, etc.*

***Tampering*:** The tendering process may be vulnerable to unwarranted manipulation by malicious participants. A malicious contractor or supplier gains access to the published call-to-tender or bids and modifies them. In privacy terms, this is simply a data security issue.

Repudiation: A malicious contractor or supplier performs an action that cannot be traced back to them i.e. a supplier makes a lower offer in order to win a bid, and later denies making the offer. Furthermore, a party obtains PII and discloses it to a third party which cannot be accounted for in the case of privacy breaches. From a privacy perspective, accountability principles relate to the repudiation security property, which implies or supports the earlier assumption of the need for remote enforcement of privacy obligations.

Elevation of Privileges: A malicious contractor or supplier performs actions it has no privilege to do, i.e. a contractor retrieves bids for a call it did not publish, or a supplier makes a bid that it is not qualified by default to bid for.

***Privacy Support*:** A participant's attribute identity information or meta-information or business information, i.e. memberships of a consortium, price of goods, may be vulnerable to undesirable privacy threats. For example, a malicious party who has access to a supplier's profile can place unjustifiable restrictions on the supplier, which potentially excludes the supplier from making bids. Information obtained legitimately by parties can be vulnerable to unwanted disclosure, misuse or abuse. The underlying privacy consequences is grave risk to the owner.

***Trust Context*:** The various participants require some sort of trust relationship to be established. The reliability of the different interactions depends on the form of the trust established and the ability of a recipient party to accept the claims made by a providing party. Since the process is brokered by a 3rd party, it is potentially vulnerable to trust relationship breaches. The participants may have to rely on the assertions of a 3rd party STS/AA on one hand, and a TCB on the other, as the basis of the trust. The degree of trust establishment that may be satisfactory in certain high-value transactions depends on the form of trust

mechanisms available. The assurance that it will all happen within mutually and acceptable practices, is a major trust concern.

The analysis of the above in terms of security requirements exposes the fact that privacy protection is tightly associated with confidentiality and trust, and as such, requires that they be treated simultaneously. The causal findings complement the assumptions previously made concerning privacy and confidentiality. Often, confidentiality is used as a substitute for privacy, but it has been established that they are not identical, and it is important to accurately differentiate them in order to identify the associated challenges and risks. Arguably, unlike confidentiality, privacy has contractual properties and obligations that are backed up by legal framework as well as FIPs. Moreover, this emphasises the need for privacy guarantees and enforcement of the guarantees when transactions span across autonomous security domains. This is supported by the earlier argument that a party that may have legitimate reasons for the possession of PII, may as well store and use it subsequently without notification. This means that where there are no strong binding obligating constraints between communicating parties, privacy may be overly violated. Based on the above critical appraisal, outlined below are security requirements that can be deduced:

- The TCB should have a fine-grained access control to clear or screen requestors for security or reliability. The TCB must enforce appropriate policy rules and a statement of practices to be followed to ensure compliance with relevant security requirements. Doing this may require the combination of a TCB's site policy with the service owner's policies, i.e. a contractor's policy, to ensure that appropriate security preferences are enforced at runtime, whilst ensuring that the policy does not contradict or hinder the legitimate free flow of information.
- Participants may want confidentiality of their information. For example, a contractor entity may specify a pre-qualification a potential supplier must meet, in order to screen out some categories of acceptable suppliers by defining certain cut off criteria.
- Participants' privacy: the various participants' information requires privacy preservations. The supplier entity may place restrictions on what the contractor can do with its bids, e.g. validity of bids has the privacy characteristics of 'maximum retention period', such as the number of days a bid is valid for. Participants may have various service level agreements that require strong privacy bindings, i.e. disclosure to 3rd parties, choice/consent before information can be used other than for the originally stated purpose.

Given the above security requirements, the exchange of some of this service meta-information between parties needs to be handled dynamically as business requirements are expected to change regularly. This strengthens the earlier argument that the trust provided by PKI may not be sufficient to guarantee the remote enforcement of privacy.

II. CONCLUSION

This paper has addressed threat modelling in the context of privacy protection, especially in distributed environment where parties may not belong to the same security domain. In this context, privacy, confidentiality and trust are unique security challenges that must addressed simultaneously and dynamically too. The modelling has clearly indicated privacy concerns in distributed environment.

REFERENCES

[1]. D. Andert, R. Wakefield, and J. Weise, "Trust Modeling for Security Architecture Development," Sun BluePrintsOnLine, http://www.sun.com/blueprints/1202/817-0775.pdf December 2002.

[2]. B. Carminati, E. Ferrari, and H. Patrick C.K, "Exploring Privacy Issues in Web Services Discovery Agencies," IEEE Security and Privacy, vol. 3, pp. 14-21, 2005.

[3]. A.Acquisti, "Privacy and Security of Personal Information- Economics Incentives and Technological Solutions," presented at Workshop on Economics and Information Security, University of California Berkeley, 2002.

[4]. K. E. Seamons, M.Winslett, T. Yu, L.Yu, and R.Jarvis, "Protecting Privacy during On-line Trust Negotiation,," presented at 2nd Workshop on Privacy Enhancing Technologies, San Francisco, CA, 2002.

[5]. B. J.-B. VanjaSenicar, TomazKlobucar, "Privacy-Enhancing Technologies-approaches and development" Computer Standard & Interfaces," Computer Standard & Interfaces 25, pp. 147-158, 2003.

[6]. E. Bertino, E.Ferrari, and A. Squicciarini, "Trust Negotiations: Concepts, Systems and Languages," IEEE Computer, pp. 27-34, 2004.

[7]. OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," http://www.oecd.org/home/ 1980.

International Journal of Engineering Research and Applications (IJERA) is **UGC approved** Journal with Sl. No. 4525, Journal no. 47088. Indexed in Cross Ref, Index Copernicus (ICV 80.82), NASA, Ads, Researcher Id Thomson Reuters, DOAJ.

U. M. Mbanaso, Ph.D. "Privacy Threat Modelling And Analysis in Access Control Context." International Journal of Engineering Research and Applications (IJERA) , vol. 07, no. 12, 2017, pp. 30-35.