TOWARDS A CONTENT-BASED BILLING MODEL: THE SYNERGY BETWEEN ACCESS CONTROL AND BILLING

Peter J. de Villiers and Reinhardt A. Botha
Faculty of Computer Studies,
Port Elizabeth Technikon, Port Elizabeth
peterd@petech.ac.za, rbotha@computer.org

Abstract   In the internet environment the importance of content has grown. This has brought about a change in emphasis to provide content-based services in addition to traditional Internet transactions and services. The introduction of content-based services is the key to increase revenues. To effectively increase revenues through content-based services efficient billing systems need to be implemented. This paper will investigate a presumed synergy between access control and billing. The investigation identifies three phases. Subsequently the similarities and differences between access control and billing in each of these phases are investigated. This investigation assumes that information delivery takes place in an XML format.

Keywords: access control, billing, XML

1.   INTRODUCTION

The global economy has made a transition from an economy with an industrial focus to being an economy based on knowledge and information. This new paradigm is enabled by the use of Information and Communication Technologies (ICT).

The increasing pace of technological innovations in the field of ICT has given rise to new ways of communicating, learning and conducting business. The Internet has facilitated the establishment of a "borderless" environment for communications and the electronic delivery of certain services. This is known as electronic business (e-business). Electronic business is the key to doing business in the new global economy that is based on knowledge and information [15].

E-business applications include e-commerce, e-learning, gaming, on-line communities and TV-quality streaming media for communication with employees and partners. All of these applications are enabled through the web [4]. The web is a major source of varied digital content.

"Content is the defining essential. Those with content will set the pace." says Sandy Climan, Managing Director, Entertainment Media Ventures [13].

This kind of realization led to there being a change in emphasis to not only provide traditional Internet transactions and services, but content-based services as well. The key to increased revenues is the introduction of content-based services. With the introduction of these services telecommunications operators will have the opportunity to span a much broader section of the value chain. In order to do this effectively they will have to make effective use of their existing assets, such as their subscriber base. They will also have to form new partnerships in order to create attractive applications and provide quality content. However, the key to increasing revenues will be implementing efficient billing systems [13].

Billing is a financial service and therefore it is assumed that it needs security. This paper investigates this presumed synergy between access control and billing by specifically focussing on the applicability of Role-Based Access Control (RBAC) [14] for billing purposes. To this means three phases common to both access control and billing will be investigated. Due to the proliferation of presenting billable content across the Internet this paper will also investigate information delivery on the Internet.

2.   INFORMATION DELIVERY

Web pages are created with the Hypertext Markup Language (HTML) that tells the browser how to display the information. HTML provides a simple, common language to create web pages that could easily be viewed by just about anyone more or less as intended. The problem with HTML is that it is a limited language, and you have trouble effectively separating content and presentation [12].

Presentation and content is effectively separated by the Extensible Markup Language (XML) [16], which describes the information itself. Because XML separates content and presentation, an XML file doesn't contain any presentation information. The presentation information is contained in a style sheet. This allows the same document to be displayed on different media, and it also enables users to view the document according to their preferences and abilities, just by modifying the

style sheet. XML has a hierarchical structure that can be mapped as a document tree. This fact is used extensively by the stylesheet. The stylesheet is created using the Extensible Stylesheet Language (XSL) [10]. XSL uses a XML notation. In XSL, the formatting object tree can be radically different from the source tree, and not the source tree. Inheritance of formatting properties is on the formatting object tree. XSL is targeted at XML, in particular highly-structured, data-rich documents that require extensive formatting [17]. XML is often used for structured documents like XHTML, rendering or transformation languages like Extensible Stylesheet Language Transformations (XSLT) [5], and as the basis for extensible network protocols like SOAP [11].

Therefore XML is key to creating a more dynamic web through various standards that are using its structured nature as a basis. This structured nature of XML also allows for greater security than HTML. XML imposes strict rules to the structure of XML documents. An XML document that adheres to these rules is said to be well-formed. In addition, the structure of XML documents may be specified by an XML Schema [9]. The structured nature of an XML document also allows elements within the document to be addressed.

2.1. ADDRESSING XML DOCUMENTS

Addressing XML documents occurs by using an XPath [6] expression. In addition to addressing functions, XPath provides basic facilities for manipulation of strings, numbers and booleans. XPath operates on the abstract, logical structure of an XML document, rather than its surface syntax. XPath also has a natural subset that can be used for matching (testing whether or not a node matches a pattern).
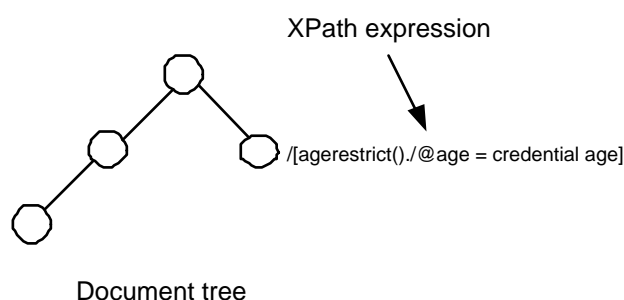

Figure 1   XPath modelling of a document tree

XPath works by modelling an XML document as a tree of nodes as depicted in figure 1. There are different types of nodes, including element

nodes, attribute nodes and text nodes. XPath defines a way to compute a string-value for each type of node. Some types of nodes also have names. The primary syntactic construct in XPath is the expression.

An expression is evaluated to yield an object. This object is a part of the document tree which can consist of one or more nodes. Because of this ability to identify a specific part of the document tree, access control can be performed on the document tree.

Expression evaluation occurs with respect to a context. XSLT and XPointer [8] specify how the context is determined for XPath expressions used in XSLT and XPointer respectively. All these facts already ensure a greater level of integrity in XML documents than HTML documents. In addition to this, the separation of content and presentation in XML documents yields further security opportunities.

2.2. SEPARATION OF CONTENT AND PRESENTATION

Due to the separation of content and presentation, focus can be given to protecting the information content without being concerned with the presentation of information. Since the tags that define the contents can be created by the author of the document, specific semantics can be associated with each tag that can be used to interpret the document and its security requirements [2].

For example, suppose there is an online catalog document written in XML that lists available goods sold on the Internet. As the content is separated from the presentation access control policies could be applied to the information. One access control policy could be that only premium members can view the special discount price information in the document. When a regular member views the catalog, any information provided for the premium members would be hidden.

This kind of access control is known as fine-grained access control, allowing certain parts of a document to be accessible to certain users only. This is made possible by the fact that the tags defining the document are defined by the author of the document [7] .

XML has been chosen for the platform for information delivery in this paper because XML has a flexible and extensible architecture, and it has a great potential impact on the next generation web, as well as XML's structured nature facilitating access control.

Access control and billing share common ground and billing is key to increasing revenues.

3. THE SYNERGY BETWEEN ACCESS CONTROL AND BILLING

Billing and access control both essentially consists of three phases as depicted in figure 2. The first phase in both instances is identification or authentication of the client. In both cases the next phase is an attempt to access a resource. The third phase, however, differs slightly. In traditional access control the third phase consists of either permission being granted or denied for the requested service. In billing the third phase consists of the actual monetary transaction or payment for the received content or service.
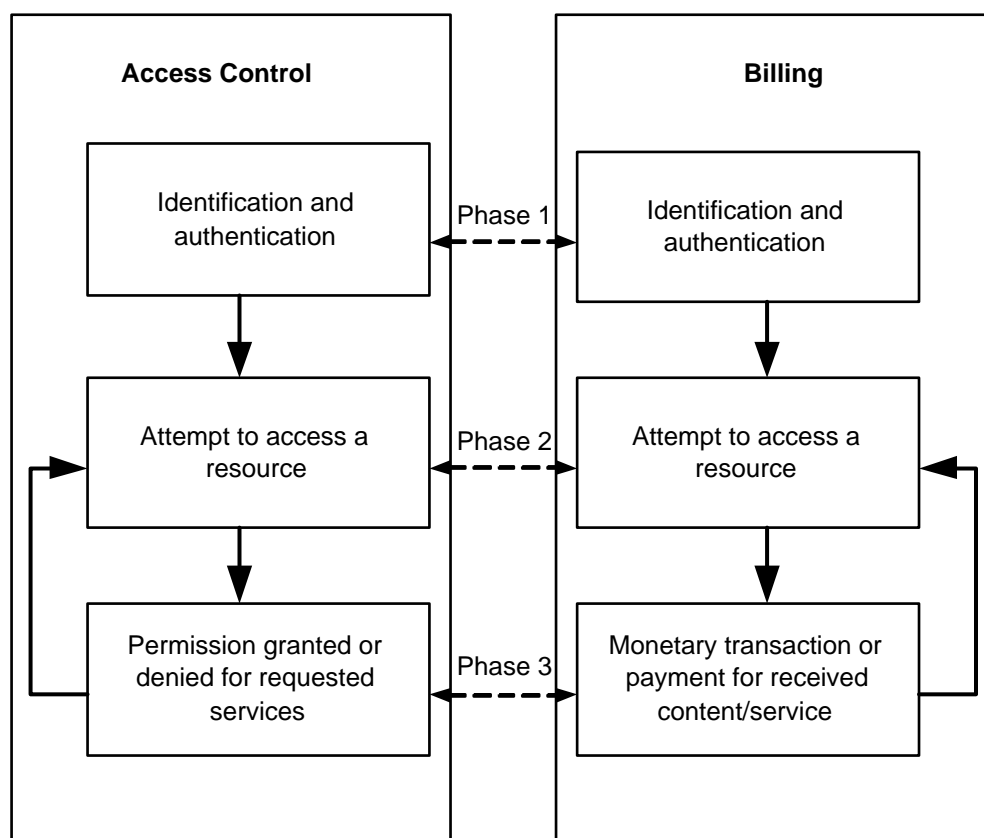

Figure 2 The Three Phases of Billing and Access Control

Although three phases can be identified it is generally accepted that they should be transparent to the user as mentioned by Bullock and

Benford [3]. They identify three properties that the implementation of an access control service should adhere to. The access control service should be unobtrusive, simple and maintainable. To a certain extent these three principles also apply to a billing system. A billing system must be simple, and it must be easy to maintain. However, a billing system would differ from an access control service with respect to unobtrusiveness. A billing system would require feedback due to the fact that it has a contractual nature requiring the user to pay for the supplied resource.

4.   THE PHASES OF ACCESS CONTROL AND BILLING

For the purpose of discussion the three identified phases are named: Identification and Authentication, Attempt to Access a resource and Access Resolution.

4.1.   PHASE 1: IDENTIFICATION AND AUTHENTICATION

Identification and Authentication is the first phase identified for both access control and billing. In this phase the user is identified and authenticated.

In the case of **access control** the user is then assigned a role. Roles follow the structure of an organization. A role is a job function within an organization that describes the authority and responsibility conferred on a user assigned to the role [14]. As roles are related to a organizational hierarchy they would not be as suited for billing which has different needs to traditional access control within an organization.

In the case of **billing** there is a greater need for information classifying the user based on properties describing the user than on knowledge of the user's relationship to other users in a hierarchical organizational structure. Therefore the user is assigned credentials. A credential is a set of properties concerning a user that are relevant for security purposes. Authorizations are then expressed by specifying the user receiving the authorizations in terms of conditions against user credentials. User credentials thus represent a way to support access control based on user qualifications and profiles. For example, credentials could be properties such as the user's age and credit rating. By using credentials one can directly formulate policies such as "The user can only have the option to buy an article from the online journal if he does not have a negative credit rating". Credential-based access is more useful for billing purposes than roles would be.

After Identification and Authentication have taken place, a session is established to create an environment in which the user can attempt to perform actions. This leads to the second identified phase.

4.2.   PHASE 2: ATTEMPT TO ACCESS A RESOURCE

The second phase identified is the attempt by the user to access a resource. In **access control** the user's session permissions will determine which resources the user can view. In the case of an operating system the user can view all the resources on the connected network. Once a resource is selected for an access attempt phase three will take place determining if permission to access the resource is allowed or denied.

Workflow systems differ from operating systems in the method they use to provide a user with a view of resources he can access. In a workflow system the user can only view the tasks that he has to perform[1]. The method to provide the user with a view in billing would relate more closely to workflow systems than to operating systems in that only the material designated as "free" or "public" would be initially viewable.

In the case of **billing** this phase would consist of the evaluation of an XPath [6] expression which will determine what the user can view based on his credentials. For example, non-member users visiting an online journal will only be able to view the abstracts describing the articles in the journal that they can purchase. If after viewing the purchaseable material the user is allowed to buy an item, and he decides to do so the third phase will take place.

4.3.   PHASE 3: ACCESS RESOLUTION

The third phase identified performs access resolution, which is the determination of whether permission is granted or denied with regards to accessing the requested service or resource.

In **access control** the various permissions assigned to the possibly multiple roles of the user have to be resolved. These possibly conflicting role permissions are resolved by determining the highest set of permissions according to the role hierarchy. For example, a person's one role may give him permission to access information available only to managers, and another role gives him access to information available to clerks. Therefore after resolution of the roles this user will get the highest set of permissions which would be access to both managerial and clerk information.

This phase differs with regards to **billing** in that not only does permission have to be granted or denied, but also a method would be re-

8

quired which will perform pricing and the necessary financial transaction needed to pay for the purchased resource or service. In this phase the document tree is pruned (shown in figure 3) to obtain the view that the user is paying for. During pruning conflict resolution takes place to determine the user's permissions [7].
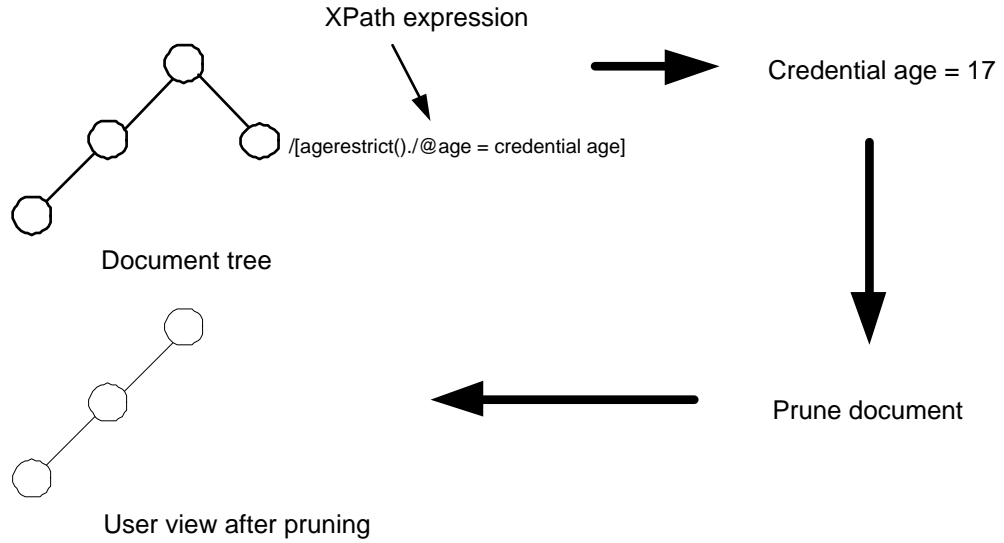
XPath expression

/[agerestrict()./@age = credential age]

Credential age = 17

Document tree

Prune document

User view after pruning

Figure 3   Pruning of the Document Tree

Within role-based environment these conflicts are typically resolved by obtaining the highest set of permissions according to the role hierarchy. Credentials differ in the way they are resolved. Credential resolution is a logical AND, in that if one condition is false the expression is false. For example, if the material to be viewed is restricted to users over the age of 18 and a user's credentials indicate that he has a good credit rating, but he is under 18 then access is denied as he fails the condition of being over 18.

5.   CONCLUSION

Throughout the three phases identified similarities can be seen between access control and billing.

Firstly, both access control and billing initially require identification and authentication to take place, only differing in the assignment of roles for access control and credentials for billing. Both then require the establishment of a session.

Secondly, both access control and billing allow for an attempt to access a resource to allow the user to see which resources he can attempt to access.

Thirdly, both access control and billing require access resolution. They differ with respect to how this is done. In the case of access control role conflicts are evaluated into the highest set of permissions. However, in the case of billing credentials are resolved as a logical AND where if one condition evaluates to false the whole expression will be false. Billing also has an additional requirement in that it must make provision for a monetary transaction to occur.

This paper has shown a synergy between access control and billing.

An initial study into existing billing models show that they don't seem to based on a standardized model. Due to the synergy between access control and billing it is believed that existing access control models can be used as a basis for developing a billing model. Future work will thus concentrate on adapting and customizing the access control models to incorporate the identified billing requirements needed to create a billing model.

References

[1] Reinhart A. Botha. *CoSAWoE A Model for Context-sensitive Access Control in Workflow Environments.* PhD thesis, Johannesburg, South Africa, 2001.

[2] Reinhart A. Botha and Jan Eloff. *An Access Control Architecture for XML documents in workflow environments.* 2002. To appear in South African Computer Journal no. 28.

[3] Adrian Bullock and Steve Benford. An access control framework for multi-user collaborative environments. In *Proceedings of GROUP'99*, pages 140–149, Phoenix, Arizona, 1999. ACM.

[4] Cisco World. *Standards-Based Group Seeks Advancement of Content Networking.* Available from: `http://www.ciscoworldmagazine.com/backissues/back2001.shtml`, 2000. Last cited: 25 January 2002.

[5] James Clark, editor. *XSL Transformations.* W3C Recommendation, Available from: `http://www.w3.org/TR/1999/REC-xslt-19991116`, 1999. Last cited: 26 February 2002.

[6] James Clark and Steven DeRose, editors. *XML Path Language (XPath) Version 1.0.* W3C Recommendation, Available from: `http://www.w3.org/TR/1999/REC-xpath-19991116`, 1999. Last cited: 26 March 2002.

[7] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati. *A Fine-Grained Access Control System for XML Documents.* 2002. in ACM Transactions on Information and System Security (TISSEC), vol. 5, n. 2, May 2002, pp. 169-202.

[8] Steven DeRose, Eve Maler, and Ron Daniel Jr., editors. *XML Pointer Language (XPointer) Version 1.0.* W3C Candidate Recommendation, Available from: `http://www.w3.org/TR/2001/CR-xptr-20010911/`, 2001. Last cited: 20 May 2002.

[9] David C. Fallside, editor. *XML Schema Part 0: Primer.* W3C Candidate Recommendation, Available from: `http://www.w3.org/TR/2000/CR-xmlschema-0-20001024`, 2000. Last cited: 15 February 2002.

[10] Max Froumentin, editor. *The Extensible Stylesheet Language (XSL).* W3C, Available from: `http://www.w3.org/Style/XSL/`, 2002. Last cited: 26 February 2002.

[11] Martin Gudgin, Marc Hadley, Jean-Jacques Moreau, and Henrik Frystyk Nielsen, editors. *SOAP Version 1.2.* W3C Working Draft, Available from: `http://www.w3.org/TR/2001/WD-soap12-20010709/`, 2001. Last cited: 26 February 2002.

[12] Kip Hampton, editor. *Web Content Validation with XML::Schematron.* XML.com, Available from: `http://www.xml.com/pub/a/2000/11/29/schemas/part1.html`, 2002. Last cited: 19 February 2002.

[13] Nokia. *3G Market Overview.* Available from: `http://www.Nokia.com/3G`, 2002. Last cited: 1 February 2002.

[14] R. S. Sandhu, E. J. Coyne, H. L. Fenstein, and C. E. Youman. Role-based access control models. *IEEE Computer*, 29(2):38–47, Feb 1996.

[15] South African Department of Communications. *A Green Paper on Electronic Commerce for South Africa.* Available from: `http://www.ecomm-debate.co.za/greenpaper/`, 2000. Last cited: 9 March 2001.

[16] W3C. *Extensible Markup Language (XML).* Available from: `http://www.w3.org/XML/`, 2002. Last cited: 6 March 2002.

[17] W3C, editor. *What is XSL?* W3C, Available from: `http://www.w3.org/Style/XSL/WhatIsXSL.html`, 2002. Last cited: 26 February 2002.