Efficient Basic Access Control Policy Framework for Electronic Digital Certificates Using XACML

Praveen Kumar M[1], *Asst. Prof., Dept of IT, Bapatla Engineering College, AP, India*
Srinivasa Rao N[2], *Asst. Prof., Dept of IT, Bapatla Engineering College, AP, India.*
Prasad G[3], *Asst. Prof., Dept of IT, Bapatla Engineering College, AP, India.*
Bhaskar K[4], *Asst. Prof., Dept of IT, Bapatla Engineering College, AP, India.*

Abstract

Recent advancements in basic access control are to provide an optional mechanism to protect unauthorized reading and possibly eliminating duplicates of any important documents like e-passport, e-commerce or citizen digital signatures. For overcoming these disadvantages, earlier they focused on the secure communication channel based on two 3DES keys, which ended up with low entropy. Now we present a framework, which evaluate and generate access control policies. Based on the study it reveals the framework containing a modeling formalism called RW, which is supported by a model-checking tool. RW is designed for modeling access control policies and verifying their properties. It converts a policy written in the RW language into a policy file in XACML. We propose an access control system that can then be built on the converted policy file. Our proposed scheme will be illustrated towards proceeding with the efficient security algorithm**,** which overcome the drawbacks such as low entropy and provides a high secure communication channel along with access control management which helps to provide restriction over access requests.

Keywords: RW-(Read and Write), XACML- (eXtensible Access Control Markup Language), DES (Data Encryption Standard).

I. Introduction

A biometric passport is a combination of a paper and an electronic identity document that is used to authenticate the citizenship of travelers. The biometric passport is valid for 5 years for first time applicants, compared to 10 years passports without biometric features. The biometric passport is planned to have digital imaging and fingerprint biometrics placed on the radio frequency identification chip. A biometric passport uses the most advanced technology to verify a person's identity, looking the same as a regular passport, with the exception of the computer chip on the photo page.

Passports and ID cards are unlikely to actually use most of the thirteen biometric indicators the government proposes to collect on all citizens. Passports are to be now based on biometric testing, and the passport's critical information is stored on a tiny RFID computer chip, much like how information is stored on smart cards. Biometric passports first appeared in Belgium around 2004, putting the country a pioneer in the field. Biometric passports cannot be changed due to information only being able to be written to it once. Biometrics automates the process that verifies an individual's identity based on their physical characteristics. Biometrics included in a static chip provides a means by which the identity of visitors may be verified, and hinders entry by imposters and the use of fraudulent documents. Further advances in biometrics technology are growing all the time.

Biometric passport is a technology advancement that will spread across the world, and countries that have not adopted it will be alienated from rest of the world. The biometric passport is believed to be as a foolproof method to stop passport cheats in their tracks. A biometric passport takes scanned information of your photograph and stores it in a chip, which is built into the passport itself. The DNA biometric passport is in development and has yet to be implemented fully, and governments that wish to implement it need to plan to ensure a smooth transition from the present system to the new system. Because of the increasing threat of identity fraud we need to strengthen security features in passports. The International Civil Aviation Organization which sets international Standards, chose facial recognition as the main biometric measure. Iris and fingerprint recognition are a back up, but they are not compulsory.

A) IS THE BIOMETRIC PASSPORT SECURE?

Fig1: The new Biometric passport

IPS takes security and privacy very seriously. The new British biometric passport meets international standards as set out by International Civil Aviation Organization we are confident that it is one of the most secure passports available. The new biometric passport has many new security features including a chip. The new design will be harder to forge, the new security features will show if the passport is genuine or that it has been tampered with and the facial biometrics on the chip will help link the passport holder to the document. The data on the chip will be protected against skimming and eavesdropping, through the use of advanced digital encryption techniques. The chip will complement the security features currently inherent in the passport, including the 'machine readable zone'.

B) WHAT IS THE PROBLEM WHEN CONSIDERING SECURITY AND PRIVACY ISSUES?

Researchers have already exposed a number of security and privacy issues regarding the possession and the use of e-passports. As expected, there are several potential e-passport threats, due to two factors: (a) The proximity (RFID) communication of the passport with other systems, and (b). The existence of sensitive biometric data within its chip. A basic security concern is the unauthorized skimming or eavesdropping of the information stored in the passport, resulting in an identity theft. This concern is further intensified due the contact less nature of the passport's chip, giving the possibility of skimming its contents without the awareness of its holder.

We focus our attention on the weakness related to the cryptographic functionality of the e-passports: Entropy of Basic Access Control keys provide the specifications for implementing an optional mechanism to protect unauthorized reading of the contents of an e-passport. It is called 'Basic Access Control'. According to this mechanism, a secure communication channel between the reader and the passport must be established, before reading the identity contents. The secure channel is based on two 3DES keys, which are stored in the passport. The same keys are computed at the inspection point; the software at the inspection point computes the symmetric keys, based on information contained in the MRZ (Machine Readable Zone) of the passport, which must be optically or manually read from a physically opened passport. In other words, security is based on the fact that nobody can derive the cryptographic keys and read the passport's contents, unless it has physical access to it.

However, it seems that the entropy of the basic access control keys is low. Since the keys are derived from readable, and sometimes known- information stored in the MRZ, it is possible for someone who knows something about the holder and about the policy of the passport issuing authority, to decrease the entropy of the keys at unacceptable levels.

II.Related work

In the paper proposed by Mr. Paul L. Yu, John S. Barras[1] the paper introduces a general analysis and design framework for authentication at the physical layer where the authentication information is transmitted concurrently with the data. By superimposing a carefully designed secret modulation on the waveforms, authentication is added to the signal without requiring additional bandwidth, as do spread-spectrum methods. The authentication is designed to be stealthy to the uninformed user, robust to interference, and secure for identity verification. However, with a long enough authentication codeword, a useful authentication system can be achieved with very slight data degradation.

The problem of non-interactive message authentication[2] using an insecure broadband channel and an authenticated narrow-band channel is considered. This problem has been considered in the context of ad hoc networks, where it is assumed that there is neither a secret key shared between the two parties nor a public-key infrastructure in place. A formal framework for protocols of this type is presented, along with a new protocol, which is as efficient as the best previous protocols. The security of the proposed protocol is based on a new property of hash functions called 'hybrid-collision resistance' here they assumed that there are two channels available for communication insecure broadband channel and authenticated narrowband channel. In comparison with this latter protocol, the proposed NIMAP reduces the amount of information sent over the insecure channel significantly.

The article on Optical Watermarking for Printed Document Authentication by Sheng Huang and Jian Kang Wu [3] describes a novel visual information concealment technique, referred to as optical watermarking, for the authentication of original printed documents. The basic watermark layer has parallel line gratings as its information carrier structure; hence, the key space is very limited. Here whenever there is frequency difference, like when the decode key and the watermark has a frequency difference there will be a "beat frequency".

The basic concepts of RBAC[6] (Role Based Access Control) originated with early multi-user computer systems. The resurgence of interest in RBAC has been driven by the need for general-purpose customizable facilities for RBAC and the need for general-purpose customizable facilities for RBAC and the need to manage the administration of RBAC itself. As a consequence RBAC facilities range from simple to complex. This article describes a novel framework of reference models to systematically address the diverse components of RBAC, and their interactions.

In the paper on "Access Control Systems through Model checking[7] a framework of evaluating and generating access control policies has been explained. The framework contains a modeling formalism called RW, which is supported by a model-checking tool. RW is designed for modeling access control policies, and verifying their properties. The RW language is very expressive, allowing us to model complex access conditions.

III. Proposed schema

In this paper we will be using different security algorithms related to our problems. We present a framework for evaluating and generating access control policies. The framework contains a modeling formalism called RW, which is supported by a model-checking tool. RW is designed for modeling access control policies, and verifying their properties. The RW language is very expressive, allowing us to model complex access conditions, which can depend on data values, other permissions, and agent roles.

Given a model built based on a policy and a property, the model-checking algorithm decides whether the goal defined by the property is achievable by the coalition within the permissions the policy provides. In the case that the goal is achievable, the algorithm outputs strategies, which may be used by the coalition to achieve the goal. The unachievability of legitimate goals may suggest permission to carry out their actions. The achievability of malicious goals may reveal certain security holes in the policy. When malicious goals are achievable, the resulting strategies help to provide clues on amending the policy. The tool implements the algorithm and thus performs the RW model checking. It can also convert a policy written in the RW language into a policy file in XACML. An access control system can then be built on the converted policy file.

1) What does Access Control Mechanism MEAN?

Access control is the ability to permit or deny the use of a particular resource by a particular entity. Access control mechanisms can be used in managing physical resources, logical resources or digital resources Item Control or electronic key management is an area within an access control system which concerns the managing of possession and location of small assets or physical keys.

A) THE RW ACCESS control formalism

The modeling formalism, which is used to model access control policies, is based on prepositional logic. A novelty of this formalism is its built-in abilities to express permissions about permissions. The RW

formalism considers permissions as data in the same way as it considers ordinary data in a system. Thus, permissions are objects of reading and writing actions just as other ordinary data are.

PROPOSED APPLICATION ALGORITHM

STEP 1: First input will be taken as e- Documents, e-passport, e-commerce etc.

STEP 2: The given input will be encrypted using blowfish algorithm.

STEP 3: we will be getting an encrypted file.

STEP 4: The encrypted file will be sent to the XACML tool, and the tool will be checked using a model-checking algorithm.

STEP 5: This model-checking algorithm will be having an xml program which checks for the role of the user so that it checks with the database.

STEP 6: After checking with the database the users will be given read, write or both read and write permissions according to their role and the tool will display the output.

STEP 7: we now had an encrypted file with read write or both read and write Permissions.

STEP 8: We now decrypt the encrypted file by doing reverse process of encryption.

STEP 9: Final output plain text will be obtained upon decryption.

B) THE RW ACCESS CONTROL POLICY DESCRIPTION AND SPECIFICATION LANGUAGE

This is a machine- readable language, which is used to express access control policies modelled in the RW formalism and properties be verified against the model. A property is a query, given a set of agents and a goal, whether the agents can achieve the goal by carrying out strategies consisting of permissible reading and overwriting actions in each step. Goals amount to either learning about the state of the system to which the policy applies, or changing it to satisfy certain conditions, or some logical combinations of these.

C) THE RW MODEL-CHECKING ALGORITHM

This algorithm takes a model of a policy and a property as input and answers whether the property holds on the model. The algorithm uses the technique of symbolic model checking. If the property holds, which means the agents can achieve the goal, the algorithm outputs strategies that may be used by the agents to achieve the goal. For legitimate goals, the achievability shows that the policy provides enough permission to the users. However, for malicious goals, the achievability may reveal certain weaknesses in the policy. In these cases, the strategies that outputs will provide clues regarding how to amend the policy. The decision procedure can figure out whether there are strategies available for that the policy does not provide the users enough agents to achieve the goal. In the case of malicious goals, the resulting strategies may give us clues that how the goals can be achieved and thus the policy can be amended accordingly.

D) BLOWFISH ALGORITHM FOR SECURE COMMUNICATION CHANNEL

In cryptography, Blowfish is a keyed, symmetric block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard now receives more attention. Schneier designed Blowfish as a general-purpose algorithm, intended as a replacement for the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries.

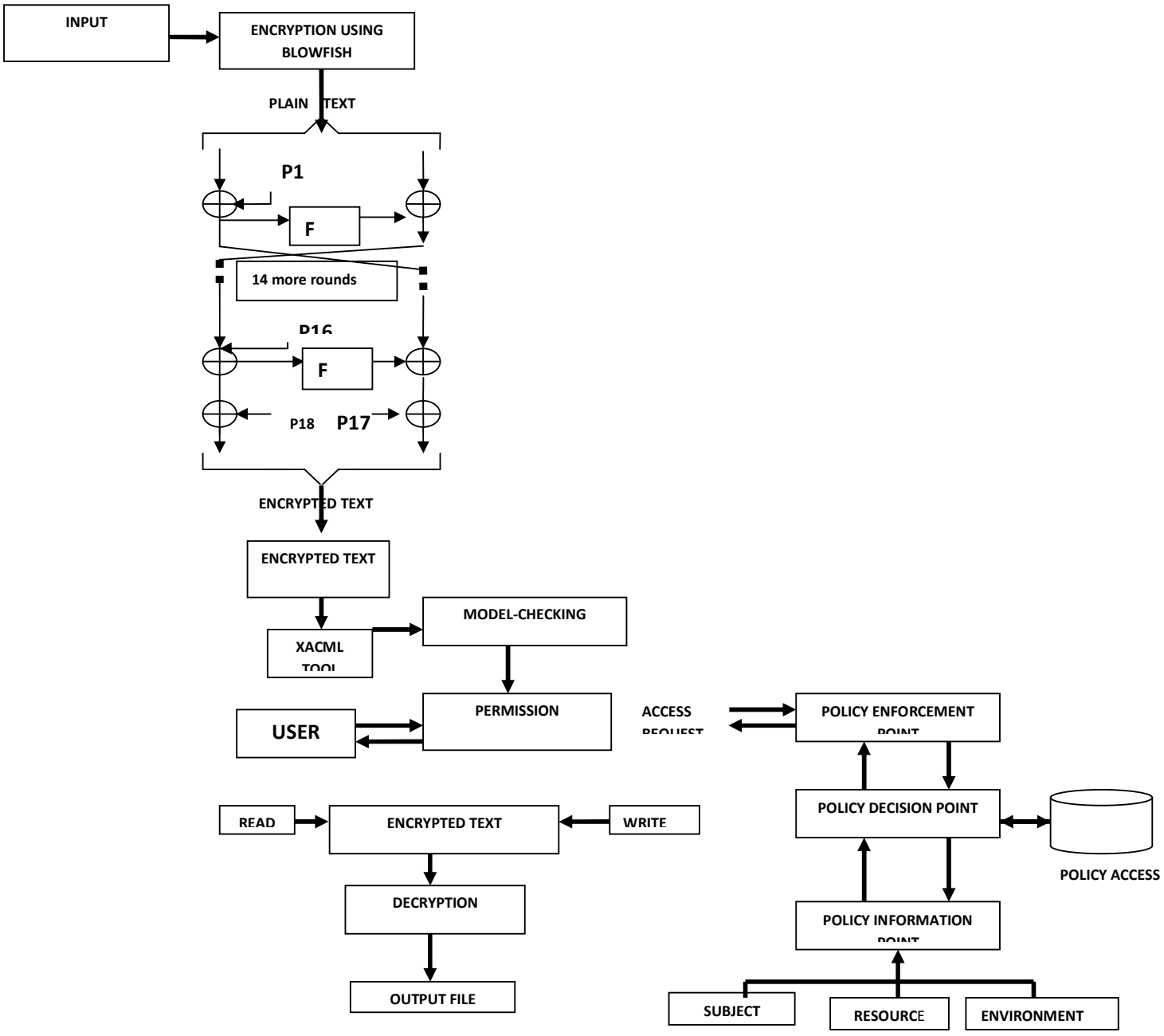

Fig 2: Proposed Application Scenario Model

Blowfish has a 64-bit block size and a variable key length from 32 to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes It is similar in structure to CAST-128, which uses fixed S-boxes.The diagram in Fig 3 shows the action of Blowfish. Each line represents 32 bits. The algorithm keeps two subkey arrays: the 18-entry P-array and four 256-entry S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used in every round, and after final round, each half of the data block is XORed with one of the two remaining unused P-entries. key schedule starts by initializing the P-array and S-boxes with values derived from the hexadecimal digits of pi, which contain no obvious pattern.

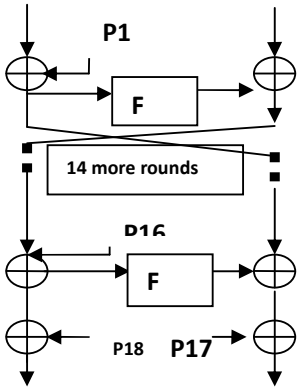

Fig 3: Action of Blowfish

The diagram in Fig 4 shows Blowfish's F-function. The function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 2^{32} and XORed to produce the final 32-bit output. Since Blowfish is a Feistel network, it can be inverted simply by XORing P_{17} and P_{18} to the cipher text block, then using the P-entries in reverse order.

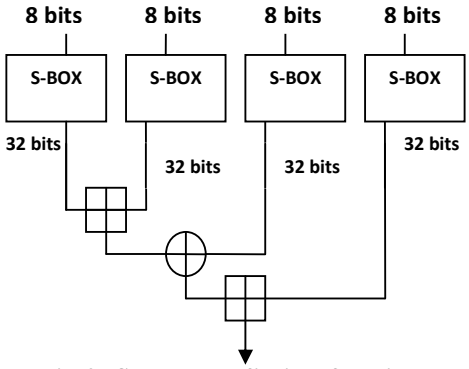

Fig 4 : Shows Blowfish's F-function

Blowfish's key schedule starts by initializing the P-array and S-boxes with values derived from the hexadecimal digits of pi, which contain no obvious pattern. The secret key is then XORed with the P-entries in order (cycling the key if necessary). A 64-bit all-zero block is then encrypted with the algorithm as it stands. The resultant cipher text replaces P_1 and P_2. The cipher text is then encrypted again with the new sub keys, and P_3 and P_4 are replaced by the new cipher text. This continues, replacing the entire P-array and all the S-box entries.

EXPERIMENTAL ANALASYS

With the existing UMU-XACML-Editor we are going to create some new policies which are created and maintained in the policy sets along with that we can check the created policies and validate the schemas using the schema validator. Based on the XACML standard the tool manages access control policies and allocates the right policy to the request and gives out the result as to ‘permit’ or ‘deny’.

IV CONCLUSION

Present days we come across the problems like, unauthorized reading of the documents and also there is no secure communication channel between the sender and the reader. For overcoming these disadvantages we proposed a framework for evaluating and generating access control policies with modeling formalism .The tool implements the algorithm and thus performs the RW model checking. But to make ensure of secure transmission between the sender and the receiver an access control system, which can be in-built with Secure Algorithm will overcome the emerging issues in the future.

REFERENCES

[1] Paul L. Yu John S. Baras,"Physical layer authentication", proc. *IEEE TRANSACTION ON INFORMATION FORENSICS AND SECURITY,* vol3, NO.1, March 2008.

[2] A.Mashatan and D.R.Stinson,"Non-interactive Two Channel Message Authentication Based On Hybrid Collision Resistant Hash Functions", *proc, IEEE*, vol1, no.3 sep2007.

[3] Sheng Huang and Jian Kang Wu,"Optical Water Marking For Printed Document authentication", proc. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,* vol2, No.2, June 2007.

[4] L.Dang W.Kou, N.dang, H. "Mobile Ip Registration In Certificate Less Public Key Infrastructure", *IET inf.secur*, vol.1, No4, Dec 2007.

[5] Robert Wilson, David Tse and Robert A Schultz, "Channel Identification: Secret sharing Using Reciprocity in Ultra Bandwidth Channels", *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, Vol.2, No.3sep 2007.

[6] Ravi S. Sandhu Edward J. coyne Hal L Fienstein Charles E You man, "Role based access control model", *IEEE Computer,* Vol 29, no 2, Feb1996.

[7] K. L. McMillan. Symbolic Model checking. PhD thesis, School of Computer Science, Carnegie Mellon University, 1993.

[8] B. Chess. "Improving computer security using extended static checking". In 2002 *IEEE Symposium on Security and Privacy*, Washington, DC, USA, 2002. IEEE Computer Society.