The Solution to Prevent Multi Identity Forgery Inside the Public Security Information System

Wei-Hua ZHANG
Law School of Jiangxi Science & Technology Normal University, China
zhangwh197708@hotmail.com

Keywords: Internal loophole, Overlying Mode (OM), Biological Characteristics, Identity Forgery.

Abstract. The recent exposure of several scandals of civil servants has multiple ID certificates have aroused people profound consideration to the internal loophole of public security data management. This paper discussed adopting Overlying Mode (OM) to transform the current public information system, and proposed a new application security system, the core part of our overlay is a biometric database in the new system, which combined with PKI infrastructure will become the necessary infrastructure for the future information systems. Utilizing digital abstract of biological characteristics as primary key of the identity database table can guarantee information integrity. Based on the biological characteristics of the data center and PKI, the security mechanism can be designed to effectively prevent internal personnel identity forgery operation.

Introduction

With the network plays a more and more important role in people's life, the information security has increasingly become the core topic of social concern. The recent exposure of several scandals of civil servants has multiple certificates of identification accounts make people realize that the threat for the information system security comes from internal factors. The reason for this problem is technical, but more is a loophole in the system and mechanism [1]. Despite all kinds of measures are taken to ensure information security, including: the promulgation of information security related laws, using mathematical encryption, the establishment of public key infrastructure (PKI), dominate the key technology standard, and trying to develop new encryption algorithms. But, these are unable to solve the problem of identity forgery and multiple identities coming from internal authority. How to prevent insider staff abuse of information control power in the administrative organs? Many old information systems of government have been constructed in order to improve work efficiency, original, more is to consider the external defense, rarely consider the safety factor inside. In recent years, the frequent occurrences of false identity account make the domestic scholars to think more about the deep-seated problems in public information system [2]. Why people can get past a series of hurdles and take another’s place by counterfeiting to the University? Why do people have a number of different identity account status? So, this paper aims to explore the effective method to solve multiple identity account issues and present some simple but effective technical solutions.

The Present Situation of Government Information System

Some of the government's internal staff forged a number of identity information in order to obtain the purchase permits of multiple sets of commercial housing and other benefits, the scandal shocked the world. This fully exposed the government information system's internal design loopholes and regulatory blind zone. First, the robustness of system design is not strong. The data layer design can not guarantee the integrity of the data, meanwhile, this type loophole failed to get up through the logical layer and application layer. The various government departments have their own independent information systems, have their own independent database, mutual isolation between the various systems, using the different data standards, and the different architecture of information system, unable to achieve interconnection, intercommunication, interoperability. The fragmentation of government information system led to the development of today's society informatization faces
serious obstacles. It is because information in different systems cannot verify each other, so that your
dad should be proved to be your father, your son should be proved to be your son. Part of the reason
for the information system isolated from the outside world is to prevent public platform security
threats, which is understandable because the information technical strength is weak in the original.
However, with the advent of the information society, the isolated information systems unable meet
the needs of efficiency, fairness and security. There are many domestic scholars put forward the need
of top-down system design of information system in the public sector, including identity certification
system which is one of the core equipment[3]. Meanwhile, government information systems should
be reviewed from the perspective of data security. With the government realized that to solve these
problems has become more and more urgent, the gray zone will become small gradually.
However, due to the current institutional mechanisms, to break the status of compartmentalization
is not easy in the short term. Adopting Overlying Mode (OM) to transform public information system
is the most effective way. OM can make use of the original information assets, to enhance the system
safety performance and service performance under the condition that can not increase too much cost.
Utilizing plenty of middleware to integrate the original information systems, plus some little
modifying the basic database can realize great promotion of system performance.

The Problems of Identity Authentication in Current System

First, in the data layer of public security information system, ID is the basic certificate of personal
identity recognition, using 18 decimal numbers encoding to identify the unique personal identity. The
18 digit symbol is artificially designed, and its related objects are also artificially specified, there are
no internal relations between 18 digit symbol and the objects. So, in the public security household
registration system, there must be some loopholes in the database table related the identity. The
identify entity does not necessarily really exist. That is to say, it cannot guarantee the entity integrity
requirements of database design. If the integrity of the data can not be guaranteed, the data security is
in doubt.

Second, the closed and isolated system brings many problems. It can not achieve the referential
integrity by external reference. The integrity of the data cannot be verified and supervision through
third party independent institution. Once the internal staff tampering with the identity data for some
purposes, it is difficult to found in a short time. Although for the sake of safety, now data using
hierarchical storage system guarantee that data distorted in one place can not influence with data in
other storage place. However, local data forgeries in most cases are difficult to be found in a long time,
it will still have great harm for the social system.

Third, End users are unable to verify whether their identity is fraudulent or not via the old public
security information system. Today, the legal case of identity theft still often occurs, some identity
cards are fraudulent used to open an account of the Bank, to apply for bank loans and open mobile
phone account. The trades of identity card which are lost because of a variety of reasons are very hot
via illegal website.

The OM Solution for the System

As shown in figure 1, the core part is a biometric database (BD) added in the original system.
Biometric database can be placed under the control of the Civil Affairs Bureau, while biometric
acquisition can be handed over to the public security organs. The biological features are carried out
Hashing Operation to get digital abstract which contain biological features. This digital abstract can
be used for Primary key of the identity of the database table. In this way, the internal personnel of
public security system can not easily modify the identity data in the database to fake identity. Because
the fingerprint, etc biological features are unique, even if the internal staff obtains fake identity by
modifying the identity database, in this system, the fake identity is easy to be recognized.

Each data transmission authentication needs the digital signature of the administration authority
institutions [4], to ensure the credibility, correctness and completeness of identities data. The new ID
card contains at least three pieces of information content, including ID number, digital abstract of biological features, and the digital signature of issuing authority.

Figure 1. The Identification OM Solution Principle for Identification.

This solution requires little investment. As little as possible to modify the original information system. With the improvement in PKI and network infrastructure, the security of original system can be economically enhanced by the OM method.

Analysis of the New System

Assume someone inside the public security system forged a fake identity card for someone others by modifying the identity data table, the fingerprint have been submitted to the fingerprint database and get pass through the internal system. When the end user using forged identity cards for loans, banks need collection the users own fingerprint, however, because the digital abstracts of fingerprint in identity card is forged, the two digital abstracts of fingerprint must be inconsistent, so as to judge the identity card is false. Thus, the bank will submit the fake ID fingerprint and real user fingerprint to biometric data center, which can found fake fingerprints, and find the forgery identity and forger in the internal public security system. Because of using the digital abstract of biological features as the primary key, to fake ID digital encoding is not possible.

BD is the core of the new information in the system. BD not only can be used for the identification of public security system, it can also be used in the internal authentication system of other organizations and also can be used for identity authentication in the process of electronic transactions such as B2C, B2B, B2G and so on. Therefore, BD and PKI together constitute the infrastructure of future network security. The most typical application is the management of the school roll, which can effectively prevent someone taking another’s place by counterfeiting to attend university.

Summary

In public security, there are many loopholes in the government information system. Frequent multi identity ID and imposture college events prompted us to think about how to use the technology and management to prevent the occurrence of similar cases.

In order to minimize the cost of building the information system, the Overlying Method (OM) can be used to transform the old system. So as to make use of the original information assets, to enhance the system safety performance and service performance under the condition that can not increase too much cost.

In the new system, the core part of our overlay is a biometric database, which combined with PKI infrastructure will become the necessary infrastructure for the future information systems. Utilizing digital abstract of biological characteristics as primary key of the identity database table can guarantee information integrity. Based on the biological characteristics of the data center and PKI,
the security mechanism can be designed to effectively prevent internal personnel identity forgery operation. Of course, first of all, we should do a good job in the top-level design. That is to say, the government should take the lead, and mobilize social forces together to improve the public security information system.

References


