Cybersecurity through an Identity Management System

Elli Androulaki, Maritza Johnson, Binh Vo and Steven Bellovin
{elli, maritzaj, binh, smb}@cs.columbia.edu

Published in the proceedings of the *Engaging Data Forum Conference (EDF)*, 2009

***Abstract*—**
Cybersecurity is a concern of growing importance as internet usage continues to spread into new areas. Strong authentication combined with accountability is a powerful measure towards individuals' protection against any type of identity theft. On the other hand, such strong identification raises privacy concerns. In this paper, we argue that authentication, accountability and privacy can be combined into a single, deployable identity management system which can be adopted to current citizenship database infrastructures. More specifically, we present the properties that such a system would need in order to meet the applications of current infrastructures, aid in general operations of day to day life, and take into consideration the privacy of individuals.

I. Introduction

Increasingly, the online and offline worlds are converging. Not only do they rely on one another; requirements for one often become requirements for the other. One place this has been seen is authentication: people need to authenticate themselves both to computer systems and to other people or organizations. While there are definitely challenges [KM03], there is sufficient commonality that some people have sought to combine the two. In particular, the suggestion has been made that a single credential could serve as a login token — "something you have" — and as a national identity document as well. Either alone is difficult (see [KM02] for a discussion of some of the issues with national identity documents); combining the two complicates the issue even more.

The need desire for national identity documents is often driven by the perception that they aid in law enforcement, national security, or effective border control. Many countries already have such documents; some of those that do not, such as the United States [H09] and the United Kingdom [B09], are considering introducing them.

In the online world, the advantages of token-based authentication to computer systems have long been known. A recent major report *Securing Cyberspace for the 44th Presidency* [L08], though, took it further: it asserted that for nationally-important systems (such as government systems or those connecting to critical infrastructure computer networks, such as those controlling the power grid), a token tied to a real person was essential. Furthermore, the report said that "the United States should allow consumers to use strong government-issued credentials . . . for online activities, consistent with protecting privacy and civil liberties".

From the report, it is quite clear that such an identity system is little more than a digitally-enabled national identity document. In this paper, we take no position as to the intrinsic merits (or the lack thereof) of such a scheme; those interested in some of the issues should consult [KM02]. (A broader critique of the report may be found in [B08].) That said, if the report's caveat — "consistent with protecting privacy and civil liberties" — is to be met, we need to define the privacy requirements of such a system. That is the purpose of this paper.

A. Criteria

Cybersecurity vs. Authentication. Cybersecurity aims to provide a combination of confidentiality, integrity and availability of the data exchanged over the internet. This is a concern of growing importance as internet usage continues to spread into new areas. More specifically, it is apparent that lack of data integrity or confidentiality in online activities such as bank account management or medical record logins would have serious ramifications both in finance and integrity of personal data, which may may lead to identity theft. It is becoming increasingly clear that we will move towards mandatory strong authentication as a means to securing online interactions for critical cyber infrastructures, a point raised in [L08]. This would require new means of personal identification and authentication that require no passwords, offer accountability, and protect against weak impersonation attacks (masquerade attacks based on acquired personal information).

Strong Authentication vs. Id-based centralised system: Growing Privacy Concerns. Accountability and authentication are non-trivial requirements in a system, and difficult to achieve in conjunction with protection of confidentiality. Authentication means that each individual has provable identity, while accountability means that misbehaving individuals are identified. Because of these needs, it is evident that we are moving towards the universal institution of "strong government-issued credentials", which will be used in every online transaction activity (online banking, signing up with an ISP) of *importance*[1]. However, a centralized authentication scheme of this nature threatens individual users' privacy, as activities could ultimately be traced back to a single individual.

subsectionOur Contribution. In this paper, we explore issues related to the combination of the three properties, Authentication, Accountability and Privacy, into a single deployable

[1] We may consider *important* every infrastructure which involves money or exchange of confidential information

identity management system. More precisely, we will focus on the requirements and restrictions that would need to be met to satisfy the conflicting goals of user privacy and confidentiality, and security in the face of a card-based identity management system that addresses all current financial activities ranging from online purchases to taxation and employment.

B. Organization.

In the following section we will describe the main attributes of the proposed system, including the entities from which it consists of. In section III we will refer to the collaboration opportunities and motives each one of the system's entities may have against our requirements, while in IV we specify our requirements for each user-activity. In the two last sections, we deal with other issues making the deployability of such a centralized systen more difficult in real world; we also provide an overview of previous work on the topic.

II. The concept of a centralized privacy-preserving credential system

As mentioned above, our goal is to present the issues arising from the need to combine authentication, accountability and privacy in a single system that will be used in the real world. More precisely, we will refer to a system where individuals have a single identity, register with a public authority, and obtain government-issued credentials. These credentials can be used by the individuals to participate in a number of real-world *interactions*. These interactions include — without being limited to — the most important (id-based) activities of an individual, such as handling of employment, management of bank accounts, fair and accurate income tax reporting, fair credit score update, verification of specific attributes of the individual — for example, that the individual is above the drinking-age limit — and registration in multiple online or offline clubs, associations or services.

In order to cover the most common activities, a centralized identity management system would need to include the following entities:

- *Users*, who may interact with other users or organizations in order to perform various tasks. Users represent the citizens and other residents of a country.
- *Employers*, who form employment relationships with users and are responsible for reporting income and corresponding tax withholding. Employers may be any type of real-world employers.
- *Banks*, who allow users to open (possibly pseudonymous) accounts for the purpose of storing cash and handling financial transactions. They are responsible for reporting interest for income tax purposes.
- The *Registration Authority* (RA), which is responsible for registering the legal users and manages the construction, modification, and destruction of government-issued users' credentials. Given the fact that users represent a country's citizens, RA may represent the official citizens' registry, i.e., Social security office for USA.
- The *Tax Authority* (TA), which is responsible for ensuring that correct income taxes are paid by all users.
- *Non-financial organizations*, who may wish to extend membership to users and are not responsible for tax reporting. Such organizations may be hospitals, gym centers, schools, any electronic commerce oriented website, etc.

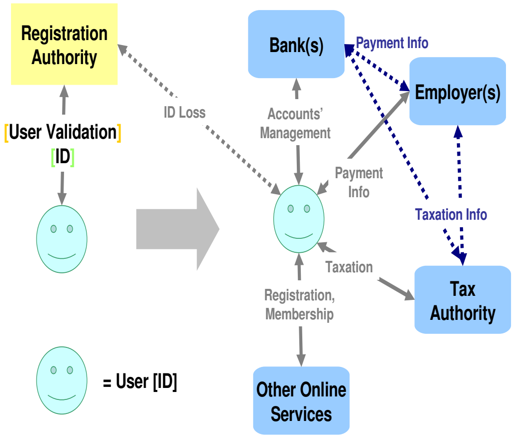

Fig. 1. Chain of procedures in real world.

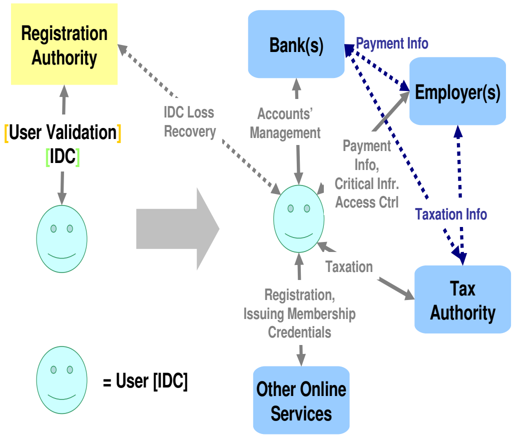

Fig. 2. Chain of procedures in the Identity Management System.

Fig.1 gives a high level view of the current interactions between the entities, showing the series of transactions in current identification systems. Citizens collaborate with an authority similar to RA to issue a national identity card, which they use later on to open accounts in banks, to be employed and receive their payments, and to prove their age. However, we can see that in online communications — and if payment is guaranteed wherever required — proof of identity is not required (i.e., to obtain membership to a website). In this way, users suffer no consequence if behaving dishonestly, i.e., if they visit a site they are not supposed to visit or if they steal confidential information. In order to deal with this, we suggest the architecture given in fig.2. In this architecture, each valid user interacts with RA to obtain credentials stored in an identity card IDC. Each user with an IDC can prove his validity without revealing his entire identity, open bank accounts, register to many other online and offline organizations, while being held accountable for misbehavior, depending on each organizations' policy. In the following section we will describe specific requirements of the proposed system in greater detail.

A primary goal of a privacy-preserving system is the a way to avoid unnecessary *linkage*. That is, it should be impossible for anyone, in the public or private sectors, to determine if two different uses of an identity card correspond to the same individual. At the same time, legally-required auditing and reconciliation (such as for income taxes) should be able to take place.

III. A "real world"-based threat model

Our real world deployability assumption defines our threat model completely. In particular, we assume that

- *Users may try to cheat.* A user may try to avoid paying taxes or paying for his purchases, lie for not having received his payment. In addition, a user may try to impersonate other users to use their funds (impersonation attack) or frame other users to appear guilty for the his malicious actions. Under the aforementioned assumptions, we further assume that a user is motivated enough to attempt any type of forgery.
- *Banks are "honest but curious".* Aiming to maintain their clientele, banks are trusted to perform all their functional operations correctly, i.e., they issue credentials, open and update accounts as instructed by their customers. On the other hand, we assume that banks may use the information they possess for their customers for other reasons, i.e., to sell credit card based profiles to advertising companies, while they may collaborate with tax authority or employers to reveal the identity behind a (swiss) anonymous account.
- *Employers may be either "honest" or "malicious".* In the general case of powerful employers, we assume "honesty" in payments towards the users, while they may try to avoid paying taxes properly. On the other hand, smaller employers may try to avoid paying employees on time or avoid paying amounts due to former employees.
- *Tax* (TA) *and Registration* (RA) *Authorities are considered to be "honest"*, as we assume that they are operated by the government who wants to protect honest users. However, they are not assumed to protect privacy; indeed, there have been a number of incidents in the U.S. of privacy violations by tax authorities or by unscrupulous individuals employed by the tax authorities.
- *Online Commercial Websites are considered to be "honest but curious".* They have to be "honest" in their functional operations to attract more users, while they use any related internet-provided information and collaborate with other websites to trace individuals' transaction activity. This is particularly beneficial for targeted ads' techniques, which base their ad-efficiency on ads' relevence to users' profiles.
- *All entities may collaborate only with governmental permission.*

Having mentioned what our assumptions are regarding the entities in a centralized privacy preserving identity management system, in the following section we will elaborate on the specific requirements of the proposed system.

IV. More specific "real world"-based requirements: How *ideal* and *reality* are combined

Authentication, *Accountability*, *Privacy* and *Deployability* are the fundamental requirements of the system proposed. *Authentication* requires making sure that each party in the system cannot lie about who he is. *Accountability* requires that misbehaving parties are traced and punished. *Deployability* is reflected on the assumptions we made on our threat model, which represent the real world environment, as well as on the system's *applicability* requirement. More specifically, we require that the identity management system should be designed in a way so that it scales for large systems, while it takes in consideration most financial activities of current citizens, ranging from banking, taxation, to ecommerce. *Privacy* requirements, in the context of a centralized identity management system with so broad range of activities, can be restricted as to honest citizens' *activity untraceability with respect to all the entities*. In particular, we require that honest users' activities should not be to be traceable — or even linked one to the other as done by the same individual — without the latter's concent.

In what follows, we will elaborate on each of our core requirements in the context of the of users' most importatn financial activities, i.e., Bank Account Management, Taxation, Employment and Registration to other online services.

General ID System Requirements. First of all, as we require a centralized strong authentication scheme, each identity should be ultimately uniquely identified. In particular, we require that each user U in our system

1) interacts with the RA *o*nce to issue a *single* valid identity card. We will refer to this card as IDC. Privacy requires that IDCs are created with citizens' collaboration such that only them can reissue tham. The requirement for the one-to-one correspondence between users and IDCs resembles the way current citizenship logs operate: *each citizen is only registered once to his country of citizenship.* As birth certificates or current citizenship-related identity cards, IDCs should be enough to prove users' validity. (We recognized that this is a very difficult process. Solving it is outside the scope of this paper; we assume that governments have sufficient motive for doing it reqardless. Again, see [KM02] for some of the issues.)

2) should not be able to create an IDC by himself or by collaborating with any other U or organization (IDC-unforgeability). This requirement is linked to the per person uniqueness of the IDC.
3) should be the only one able to prove ownership of his IDC. In current identity systems, this is achieved through the photo attached to the ID card. However, as we want IDCs to provide no information regarding its owner to any unauthorized third party, photos cannot be used in this case.
4) can demonstrate ownership of his IDC multiple times, in a way so that no one can reveal U's name (untraceability). In addition no one should be able to link two IDC ownership demonstrations as been originated by the same user (unlinkability).
5) may use his IDC in order to prove specific attributes related to himself without revealing anything more than what required. Attributes of this type may be his age or adulthood in bars in various countires, his driving license, or his criminal record.
6) may use his IDC to obtain membership to different types of services, i.e., online customer services, banks, football clubs, etc. In fact, depending on the type of the organization and the corresponding user-registration procedure, organization-issued membership credentials may be linked to its members' IDC. In this way local misbehavior of a member will lead to overall user-identification.

Bank Account Management. In terms of user interaction with banks, we require that

1) each valid user should be able to open no more bank accounts than the ones he is entitled to open based on his financial status. For privacy purposes, we may consider enabling the bank system to support two types of accounts:
    - *Anonymous but traceable accounts*, namely accounts which cannot be linked to a particular identity and more specifically to their owners, but whose activity may be observable by the bank — i.e., through credit cards. It is critical that anonymity in this case does not violate the accountability requirement. Users should only be able to open such accounts if they are financialy eligible to, while they should be taxed accordingly.
    - *Accounts with someone's name attached*, which are similar to the accounts currently supported by most banks.
2) An account's ownership should be able to be revoked or changed in the following cases:
    - its owner dies; user's inheritors should be provided access to their heritage.
    - its owner is in serious debt to the bank, because of i.e., credit card use.
3) A user should be taxed on the overall amount of money he keeps in a bank regardless of in how many accounts his savings are distributed. In the special case of anonymous accounts, taxation should be done in a way so that no privacy breach is caused.

Employment. It is likely that complete user anonymity is not an issue towards employers. Employers do need to know the full identity of their employees. In fact, in some extreme cases of national security organizations, details of the personal life of the individual are necessary to decide for that individual's credibility. Consequently, the privacy definition in the context of users' employement systems is restricted to the avoidance of any bank-account privacy breach due to employers' interaction with the banks or taxation authority throughout employees' payment and taxation respectively.

In particular, we require that payment proceeds in such a way that the employer-bank collaboration will not reveal the identity of a particular anonymous account to which the payment takes place. However, the payment should be conducted in an accountable and fair way. In addition, the employer must interact with the TA to provide payment information regarding its employees. No privacy issues arise from this interaction since both entities know the identities of the users and the taxes withheld.

Another employment-wise cybersecurity concern is be access control for specified sites. We emphasize the common case where we need to have strong authentication within the company but complete anonymity outside the company. A typical example for that would be in critical infrastructure systems: when an employee of a particular company logs in to a critical infrastructure's website, such as a SCADA system, the employee's exact identity should be knowable by that particular company's department, while for any entity outside the company, the employee should be hidden among the employees of that department (company). In any case, it should be possible to trace a misbehaving party.

Taxation. Tax Authority (TA) should be able for each individual user U to verify the latter's income, verify that the appropriate bank-account withholding taxes have been applied and exempt U— if eligible — from taxes on particular purchases. Privacy, as in employers' case, does not require that TA does not know the identities of the users. However, we want to enforce that his employment or bank-account privacy is not compromised through TA's interactions with the banks or employers.

Other Online Services. Online services may include Usubscriptions to various websites, such as magazines, travel agencies, concert venues, gyms, etc. A user's medical account login may also constiture another online activity of his. In all these cases, we do require that

1) a user's identity is not revealed, unless with the latter's consent.
2) a user's online activity cannot be monitored, i.e., we want to enforce that no third party — other than U and in many cases the online service system — should be able to link two different browsing or purchase activities

of the same user. In this way, we want to avoid any user-profiling without user's consent.

V. A critical Issue: IDC Management

In the previous section, we discussed the requirements of a privacy-preserving identity management system in users' interactions with the various authorities, i.e., banks, tax authorities, employers, etc. However, the real world nature of this system, as well as the importance of a user's IDC to his privacy, require a special class of privacy-preserving protocols related to the management of IDCs. More specifically, assuming a user U who has obtained an IDC, special privacy-preserving mechanisms should address the following:

1) it should be possible for U to "change" his IDC for security reasons so that no user-interactions related information leaks to unauthorized parties.
2) it should be possible for U to reissue his IDC if he loses it, i.e., he should be able to invalidate his old IDC and substitute it with a new one. In particular, to avoid any impersonation/identity theft attacks, the following procedures should take place:
   - recovery of his IDC's content;
   - IDC-loss declaration and automatic blacklistability of all the U's registrations with the old IDC; in this way, we aim to restrict the attacker from using U's membership credentials contained in the card or learn any thing about U's past activity. Under this assumption, we need to enforce that IDCs should have an extra layer of protection so that its owner's information is protected from a third party;
   - automatic update of all U's registrations with U's new IDC.
3) it should be possible for the content of IDC to be recovered when U dies or is in an serious medical condition, but only by authorized individuals.
4) The system should be usable and comprehensible by ordinary citizens. Too many online systems are too complex. Here, we are suggesting a scheme involving many different identities for each person. It is crucial that people know which identity is being used for each activity, and to understand the privacy and functional consequences of the identity selection. The system should "do the right thing" by default, and without excess confusion.

All these issues are very important. The real world nature of our system posits deployability of any protocols suggested a critical property. Consequently, any mechanism attempted to address the management of such an identity management system should be efficient enough to serve many requests at the same time. When it comes to lost identity cards, citizens cannot wait forever for their new cards to be issued; at the same time, the longer the credential blacklisting, takes the more time an attacker would have to exploit the stolen card.

VI. Related Work

Cybersecurity has been addressed in the past in a centralized way. As mentioned before, Sen. Schumer in [H09] has suggested the need for a biometric-based identification system to restrict the issuing of fake identities. Many countries are embedding biometric data in passports, in conformance with ICAO standards.

There has been some work indicating the problem of online privacy. In particular, Brands [B00] was one of the first to provide a big overview of privacy issues caused by the extended online use of PKI. Brands showed how an ordinary PKI would enable the construction of public dossiers of each individual's online activity. Instead, he provided a series of constructions of privacy preserving credentials, tickets and certificates based on blind signatures and zero knowledge proofs. Camenish and Lysyanskaya suggested in [CL01] a credential system with guaranteed user anonymity and credential showing unlinkability.

Although the concept of a privacy preserving identity management system with so broad range of applications has not been proposed in the past, centralized identity management systems applying the primitives of Brands, Camenisch and Lysyanksaya have been suggested in the past.

Being a prototype of [CL01], Idemix [CVH02] is the most representative example. In addition, in [CVH02], Camenisch and Herreweghen developed additional functionality for service providers and credential issuers to configure and enforce resource access control and credential issuing decisions.

Higgins [F] is an open source identity framework, which enables users to integrate identity and profile information across various data sources and protocols. In Higgins each digital identity is represented as a separate, visual iCard, while its attribute service provides to identities anonymous but authorized demonstration of their attributes.

The PRIME project [G] is a European initiative for management of the multiple identities a consumer may have obtained through his online interactions in the internet for commerce operations as airline and airport passenger processes or collaborative e-Learning, so that consumer's privacy is maintained.

OpenID [FPVFOGTOIT] and iCard [JLLP03] Foundation are examples of frameworks handling many identities of the same user across different websites. Icard, plugged into a mobile device serves as the centerpiece that provides enhanced networking and application capabilities to the mobile host.

As we can see, cybersecurity has been an issue in all the aforementioned cases. In particular online logins and proof of particular attribute procession have been addressed in the past in a centralized way. However, they do not deal with particular financial operations such as bank account management and taxation, which require a degree of identification. Similarly, master identity revocation and update and card loss recovery are very important real world issues which have not been discussed in previous work.

VII. Conclusion

In this paper, we presented the requirements of a centralized identity management system, where each individual owning an identity card IDC can perform all his current financial operations in a privacy preserving nevertheless accountable way. We claim that such a system may substantially support cybersecurity mechanisms though the IDC-based authentication mechamisms suggested, as IDCs are required to provide sufficient information to achieve both: their owners' privacy — if honest — their owners' identity revealment when having misbehaved.

VIII. Acknowledgement

The authors would like to thank the anonymous reviewers for their useful comments on this work.

References

[B00] S. A. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. MIT Press, Cambridge, MA, 2000.

[B08] S. M. Bellovin. The report on ”securing cyberspace for the 44th presidency”, 15 December 2008. Blog posting.

[B09] BBC. Q&A: Identity cards, 2 July 2009.

[CL01] J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Advances in Cryptology - EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 93–118. Springer-Verlag, 2001.

[CVH02] J. Camenisch and E. Van Herreweghen. Design and implementation of the idemix anonymous credential system. In *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*, pages 21–30, New York, NY, USA, 2002. ACM.

[F] T. E. Foundation. Higgins: Open source identity framework.

[FPVFOGTOIT] O. Foundation and I. C. F. publish vision for open government through open identity technologies. Openid foundation.

[G] P. R. Group. Prime project.

[H09] S. S. Hsu. Senate democrats address immigration. The Washington Post, 24 June 2009.

[JLLP03] Z. Jiang, H. Luo, Y.-N. Li, and H. P. icard - foundation for a new ubiquitous computing architecture. In *ICC '03: Proceedings of the IEEE International Conference on Communications, 2003.*, pages 1211– 1217, 2003.

[KM02] S. T. Kent and L. I. Millett, editors. *IDs—Not That Easy: Questions About Nationwide Identity Shystems*. National Academies Press, 2002.

[KM03] S. T. Kent and L. I. Millett, editors. *Who Goes There? Authentication Through the Lens of Privacy*. National Academies Press, 2003.

[L08] J. A. Lewis. Securing cyberspace for the 44th presidency, 2008.