Using Personal Electronic device for authentication-based service access

Abhishek Gaurav*, Ankit Sharma†, Vikas Gelara‡, Rajat Moona§
Department of Computer Science and Engineering
Indian Institute of Technology Kanpur
Email: *abhiga, †ankitsh, ‡vikasg, §moona@iitk.ac.in

***Abstract*—A person usually carries multiple authentication tokens in the form of various cards to access services electronically. Often the service outlets are equipped with a strong infrastructure to permit the user interactions. The network connectivity is usually a must for the service outlet to authenticate the user with the server. In this paper, we propose a solution which uses the personal mobile devices held by the user to interact with the service outlets. Such a system can then alleviate the needs for interaction console and communication infrastructure at service outlets.**

I. Introduction

In today's world, scenarios in which we have to access services using electronic means are common. These include services such as bank Automatic Teller Machines (ATM), petrol dispensing stations etc. Presently, such services typically involve an authentication card (such as magnetic stripe card) that needs to be presented to the service outlet. Additionally, the user may have to enter a password or biometric imprint for authentication. After authentication the user interacts with the service outlet console to request specific set of services. The console carries input output devices such as keyboard and screen for this purpose.

This paper proposes a different model of authentication and service-access. In this model a user carries a personal intelligent ubiquitous device such as a mobile phone or a PDA. This personal device authenticates itself to the service outlet on behalf of the user. This new model of authentication and service-access has several advantages over the currently used techniques. For instance, personal devices are usually equipped with a screen and a keypad which can be used for the user interaction alleviating the need of these interfaces on the service console. These devices can store the authentication related information for several services. Therefore a user need not carry multiple cards for multiple services. Proposed scheme also poses several technical challenges in implementation.

The authentication of services and documents have been tried by several researchers in variety of applications[2][3][4]. Horn et. al. [4] has given a protocol for mutual authentication between mobile device and server. They assumed limited computation power of mobile device and proposed a protocol where little cryptographic computation is done by the mobile device.

Amir Herzberg proposed an architecture for payments and banking with mobile devices [5]. In this paper, he addressed several critical security aspects and trust model and presented an authentication mechanism to overcome that.

The rest of the paper is organized as follows. In section II, we introduce the current model of authentication. In section III, we introduce the proposed model vis-a-vis the shortcomings of the present model. We describe the proposed model in section IV and the implementation and simulations in section V and summarize the work in section VI.

II. The current model of authentication based service access

There are numerous examples of services where service-access requires authentication. In such services, the customer is asked to authenticate himself and upon success, is allowed to access the service. Examples include Automatic Teller Machine (ATM) services by banks where the user inserts a magnetic stripe card and enters a password to authenticate himself, before being allowed to make financial transactions. Many bookstores and food outlets provide the customers with a loyalty card so that they can access certain privileges. Petrol dispensing outlets also have similar method of authentication and service-access.

The present model of authentication based service-access can be summarized as follows. The service provider gives an authentication material, usually a magnetic stripe card[6] or a smart card[7][8][9][10], to the customer. This authentication card[1] carries information about the customer. In order to access a service, the customer presents his authentication card to the service outlet. The customer is asked to enter a password which is used to authenticate the customer. The service outlet extracts customer information from the card and sends this information (including the entered password) to a central server for authentication. Sometimes, the authentication may include biometric mechanisms which are usually matched at the service outlet. After authentication, the customer is allowed to access services. The customer usually interacts with the outlet using a keypad and a screen provided at the outlet.

A. Cryptography

In our system and in many other systems, the authentication mechanism also incorporates cryptography[1] in some form.

[1]In this paper, we interchangeably use the terms "authentication material" and "authentication card"

There are two general ways of encrypting and decrypting messages.

In Public Key or Asymmetric Key based cryptography systems, there is a pair of public and private keys. A message can be encrypted using the public key of the receiver and decrypted by the receiver using the corresponding private key.

In Symmetric Key Cryptography, there is a common key shared between the sender and the receiver. The same key is used for encryption and decryption.

III. Weaknesses of the existing systems and proposed solution

A. Weaknesses of the existing system

There are certain shortcomings in the existing model of authentication and service-access.

1) Necessity to trust the service outlet: In the existing model of authentication and service access, the user is forced to trust the service outlet. The existing model does not provide means to establish the authenticity of the service outlet. In case, the service outlet is not authentic, it can potentially store the private data entered by the user and use it for a playback attack later.

2) Infrastructure requirement: The service provider has to provide an infrastructure with each service outlet. This includes a display screen, a keyboard and other peripherals, which are required for the user to interact with the machine. These common peripherals needs are in addition to the service-specific needs which include, for instance, a money dispensing slot for an ATM machine, a petrol dispensing nozzle with the petrol dispensing outlet etc.. In the prevalent model, these common needs are being provided with the service outlet.

Further, the outlet, in general, also needs to have a connection to the service provider's network because such services usually have a centralized database where the user data is stored.

3) Extra baggage with each new service for the user: Every service provider, who needs to authenticate the user, before providing the service, generally provides the user with some personalized or generic authentication material to authenticate himself. We use a generic term "card" to denote such authentication material, which may include entities such as magnetic stripe card[6], smart card[24], RF cards[11], e-tokens etc.

If a user subscribes to many services, he carries on himself many such cards which means an extra card per new service.

4) Means of authentication and user-specific interaction: For most services today, the service outlet initially authenticates the user. In such authentication mechanisms, generally an "input" (such as password or biometric imprint etc.) is taken from the user and is matched against an "expected or correct user input". which is usually stored in a central database. In case of certain authentication mechanisms such as biometric authentication, this access to the central database may require large amount of data transfers. Thus network and infrastructure requirements limit the use of computationally-intensive or data-intensive authentication schemes.

B. Proposed Solution to the shortcomings

We believe that all the above described drawbacks can be addressed if we use a ubiquitous device belonging to the user to authenticate him to the service-outlet. For this, the device needs to carry authentication material on itself.

If in addition, the personal device of the user is equipped with a screen and a keypad, then the user can use the device to type in his service-requests and view the response from the service outlet on the device's screen. The user no longer needs a screen and a keypad to be provided at the service-outlet.

For example, in an Automatic Teller Machine service provided by the banks, our proposed solution requires the user to get his personal device registered with the bank. In the registration process, the bank securely stores enough information into the device so that the device is able to authenticate itself to an ATM later.

In order to access a service, the user has to authenticate himself to the device first. This authentication is done either by means of a PIN or biometrics or some other suitable authentication mechanism.

The device can then establish its own authentication and can conduct subsequent communication with the ATM. Here, the ATM need not communicate with the back-end to establish authentication, since the device securely carries enough information to establish its own authentication.

The user can avail the services provided by the ATM by using the interface of the device for interactive actions such as typing in the amount of money the user wishes to withdraw. The information is sent to the ATM and the ATM processes the request. The user can receive the money through a money-dispensing slot.

This changed authentication model has certain advantages over the existing scheme.

1) Service outlet authenticates itself to the personal device: In the proposed solution, the personal device authenticates the user to the service outlet. In addition, the proposed model as described in Section IV, ensures that the personal device can authenticate the service outlet as well. This implies that the user no longer needs to trust the service outlet without establishing authenticity.

2) Infrastructure requirement is reduced: The proposed solution tries to capture the common needs of all services (such as display screen, keyboard etc.) and fulfill them through a ubiquitous enabled-device, which is with the user rather than it being provided at each outlet. This implies that the service outlet needs to only provide infrastructure which is specific to the service being provided. This also means that the service outlet can be smaller, cheaper and easier to protect against vandalism.

Further, as the device is able to authenticate itself to the service outlet without the service-outlet requiring to contact the central database, the network access would reduce from one per transaction to few a day.

3) All authentication material is stored in a single device: The proposed model tries to incorporate authentication materials for all services into a single device which should be

Fig. 1. Trust Model

familiar, easy to use and carry and sufficiently ubiquitous so that the user carries and uses it everywhere and has it with himself all the time.

4) Computationally intensive means of authentication become feasible: The device carries the user authentication material in a secure fashion. In order to authenticate the user, the outlet can take a fresh sample (such as biometric) from the user and compare it with the "signed sample" carried within the authenticated device. This reduces the transaction requirement with the central database. Moreover, in tasks such as authentication, the computational power of the device can also be used. For example, an "authenticated" program, installed by the service provider, can run on the device and can process the data required by the outlet, if the computational power of the device allows it. This ensures that even computationally intensive and data-intensive authentication measures can be used.

5) User-specific interaction is possible: User-specific interaction can also be done since user-specific data such as past history of user and any special offers or bonus points specific to the user can all be stored in the personal device and passed on to the outlet, if needed. Further, the user can personalize the device to suit his needs. For example, a visually-challenged person can choose a personal device which meets his specific needs and can use the device to access the service.

IV. Design of Proposed Authentication Model

The service outlet and the personal device build trust (figure 1) by authenticating each other.

In the proposed model, the personal device performs the following functions.

1) The personal device authenticates the user to the service outlet. As an added security user may need to authenticate himself to the personal device, so that a misplaced device is unusable by a fraudulent.
2) The personal device acts as an interface for the user to access the services.
3) The personal device provides information (signed by the service provider) about the user so as to obviate the need of the service outlet to communicate with the server.

The personal device that is used to authenticate and access control should have the following minimal set of features.

1) ability to store and process cryptography related data such as a key in a secure fashion.
2) an input device such as keyboard through which the user can interact with the device and issue commands to the service outlet.
3) an output device such as a display unit to convey information received from the service outlet to the user.
4) ability to communicate with the service outlet of the service provider.

A mobile phone with smart card based authentication and security mechanism and a wireless communication technology such as Bluetooth[13] or NFC[21] is an ideal device for such an application.

Since, the device has to authenticate the user to the service outlet, it needs to carry enough information required for authentication to the service outlet. Hence, the service provider needs to securely store authentication material in the device. We term this procedure of storing authentication material in the device as "registration of the device with the service provider".

Each time the user wishes to access the service, the following steps are required.

1) Authentication of the user to the outlet using user's personal device.
2) Establishment of a secure channel between the personal device and the service outlet.
3) Access to the service.

A. Modeling the proposed scheme of authentication and service-access

We use Public Key Infrastructure for mutual authentication of the service outlet and the personal device in our model.

In the model, there are three parties — the service provider (P), the service outlet (O) and the user(U) with his personal device(D). Each party has a public-private key pair.

In the discussion below, we use the following notations.

P_{pb}: Service Provider's public key

P_{pr}: Service Provider's private key The private key of the service provider is stored securely with the service provider

U_{pb}: User's public key

U_{pr}: User's private key The private key of the user is stored securely in the smart card with D

O_{pb}: Service Outlet's public key

O_{pr}: Service Outlet's private key The private key of the service outlet is stored securely at the service outlet.

Sign(X,Y): Digital signature of X using private key of Y

Certificate(X,Y): A tuple containing the public key of X, along with the credentials of X and digital signature[22] of Y on the first two items.

Verify(X, Y, Z): Boolean function that evaluates to true or false depending upon whether Y provides the digital signature of entity Z on message X

ExtractPublicKey(certificate, Y): Public Key embedded in the certificate, provided the certificate is verified for signature and credentials using the public key of Y.

1) Registration of the user with the service outlet: In this one time process, the service provider securely stores the authentication related information in the personal device which is then used at the time of service access. The registration involves the following.

- A user certificate (Certificate(U,P)) is generated for the user's public key by the service provider. The certificate comprises of U's public key, Credentials (such as certificate validity period etc.) and Digital signature on these informations by P.
- The information of account of U with P is first signed by U, which is then countersigned by P and loaded into D.

The reason for this is to prevent a fraudulent user from providing someone else's account information as his own without having the corresponding private key.

- The necessary user interface software is loaded into D, so that it can communicate with O. This step is optional since the software may also be provided by O as long as it is signed by P and verified by D.

2) Authentication of $U$to D: U authenticates itself to D using authentication mechanisms such as password or biometric authentication.

3) Mutual authentication between D and O:

- D authenticates itself to O:
  D presents U's certificate to O. O verifies the certificate and extracts U_{pb}.
  O then issues a challenge (usually a large random number) to U in order to verify whether D possesses the corresponding private key.
  D passes the challenge to the smart card which operates on the challenge using the private key and provides the response from the smart card to O.
  O verifies whether the response is valid using the public key of U and the challenge.
- O authenticates itself to D:
  O then authenticates itself to D in a similar manner. For this purpose O provides Certificate(O, P) to D.

4) Direct authentication of U to O: In case O wishes, it can authenticate U directly through some authentication mechanisms such as biometrics. For example, O can ask U to present his finger-print and then match this against a signed fingerprint specimen provided by D.

5) Presentation of U's information: D presents U's information signed by U and countersigned by P to O. This information shall convey to O, details regarding U's account with P. For example, if P is a bank, then the information can be bank account information of U.

6) Establishment of a secure channel between D and O: O and D then generate a random session key using key exchange protocols with the help of the public keys of U and O.

7) Accessing the service: U can now use D to issue requests/commands to O on the secure channel and view the response of O on D's screen.

8) End of Session: The session may be ended upon user request or on time-out. Even if the session is not ended, a fraudulent shall not be able to perform malicious activities since he is not aware of the session key.

V. Implementation

We chose ATM service facility to implement the proposed model. We have chosen the mobile phone as the personal device since mobile phones come equipped with keypad, screens as well as network connectivity such as Bluetooth.

Secondly, for mutual authentication of the mobile phone and the service outlet, we use Public Key Infrastructure. Smart cards[24] provided in mobile phones can provide support for cryptography related operations (e.g. SIM[12] card).

A. Steps in the proposed model

1) **Registration of the user with the bank:** After the registration, the mobile phone carries the public key of the user which has been signed by the bank as well as the public key of the bank. Smart Card(SC) contains the private key of the user and is responsible for carrying out any processing which uses the private key. Optionally, the mobile phone also carries an application which enables it to communicate with the ATM.
2) User authenticates himself to the mobile phone using his password as shown in Algorithm 1.
3) Mobile phones authenticates itself to ATM by presenting the user's certificate and responding on ATM's challenge as shown in Algorithm 2.
4) ATM authenticates itself to the mobile phone by presenting its own certificate.
5) Mobile phone presents the bank account information of the user signed by the user and countersigned by the bank to the ATM.
6) ATM and mobile phone establish a session key using standard key exchange protocols such as Diffie-Hellman Key Exchange[23] along with an integrated authentication to avoid man-in-middle attack.
7) User now access the service of the ATM using the signed application either loaded by the bank during registration or by the ATM as shown in Algorithm 3.

Algorithm 1 Password based user authentication to device

```
Display("Please enter password")
passwd= get_input_from_user()
verifyUsingSC(passwd)
if verified then Authentication Successful
else Authentication Failed
end if
```

Algorithm 2 Authentication of mobile phone to ATM

```
establish communication with ATM
if failure then Display("ATM busy, please try later") and exit
end if
send user-certificate to ATM for verification
if failure then Display("Bad certificate") and exit
end if
get challenge from ATM
send challenge to SC and get response from SC
send response to ATM for verification
if failure then Display("User Authentication Failed") and exit
else Authentication Successful
end if
```

We explored various platforms for simulation which satisfy the needs of the proposed model. Sun Java Wireless Toolkit 2.5[15] for CLDC[14], Beta provides a simulation platform for device like a mobile phone supporting J2ME and Bluetooth. For Public key cryptography, RSA algorithms[17][18] are used. SHA-1[19] and triple-DES algorithms[20] are used for calculating hash value (required for creating signature) and for symmetric key operations respectively.

Algorithm 3 Service access

```
Display("Welcome to atm")
Display("Balance enquiry: press 1")
Display("Withdraw money: press 2")
Display("Exit: press 3")
get input from user
if button one is pressed then
   request ATM for balance
   display balance on screen
else if button two is pressed then
  Display("How much money to withdraw")
  X= get input from keypad
  request ATM to withdraw X from account
  if successful then
    Display(X + "deducted from account, collect money from the
    ATM slot")
  else Display("operation failed")
  end if
else if button three is pressed
   close connection with ATM and exit
else Display("invalid button pressed")
end if
```

1) Challenges in Implementation: GSM SIM[12] does not support public key cryptography. Hence it can at best be used to store the private key, which is then presented to the outside world protected by a password. This compromises much of the security of the proposed model.

In our approach, we propose to use phones such as NFC[21]-enabled phones[25] which provide an additional smart card that can process PKI based services.

VI. Conclusion

In this paper, we proposed a model of authentication and service-access in which a personal device is used for authentication to a service outlet and to enable the service access.

With the proposed model, a service outlet needs to provide only service-related infrastructure. The peripheral required to interact with the user need not be provided at the outlet since the personal device purveys such needs. This minimal infrastructure makes the service outlet better resistant to vandalism and reduces the infrastructural and maintenance costs.

The proposed trust model does not require access to server for authentication thereby reducing the demand on network and server. Further, services can be provided even in remote areas, lacking network accessibility.

In our proposed model, the user needs to carry only his personal device to access various services. Further the personal device can be customized to suit the user's needs and requirements. For example, if the user is visually challenged, the personal device can be chosen accordingly.

The trust model ensures that in addition to the customer being authenticated, the service outlet is also authenticated. This reduces possibility of a fraudulent outlet storing customer's personal information and making a play back attack. The use of secure device such as smart cards also enhances security for the user.

References

[1] Schneier B., "Applied Cryptography", John Wiley and Sons Inc., 1999

[2] Nandagopal, Thyagarajan "Authentication and Verification for third party vendors using mobile devices", International Application No.: PCT/US2007/002996, Publication Number: WO/2007/092366. Publication Date: 16.08.2007

[3] Bellare M., *et.al.*, "Design, Implementation and Deployment of the iKP Secure Electronic Payment System", IEEE Jl. of Selected Area in Communications, April 2000, Vol 18, No. 4

[4] Horn G. and Preneel B., "Authentication and payment in future mobile systems", Proc. of ESORICS'98, Louvainla- Neuve, Belgium, Sep. 6–8, LNCS, Springer Verlag, 1998, 277–293.

[5] Herzberg Amir, "Payments and Banking with mobile personal devices", Communications of the ACM, May 2003, Vol. 46 No. 5

[6] ISO/IEC 7810, Identification cards - Physical characteristics, Third ed. 2003-11-01, Ref. no. ISO/IEC 7810:2003(E)

[7] ISO/IEC 7816-4, Information Technology - Identification cards - Integrated circuit(s) cards with contact- Part - 4: Interindustry commands for interchange, First Ed. 1995-09-01, Ref. no.: ISO/IEC 7816-4:1995(E)

[8] ISO/IEC 7816-6, Information Technology-Identification cards-Integrated circuit(s) cards with contact-Part-6: Interindustry data elements, First Ed. 1996-05-15, Ref. no. ISO/IEC 7816-6:1996(E)

[9] ISO/IEC 7816-8, Information Technology-Identification cards-Integrated circuit(s) cards with contact- Part - 8: Security related interindustry commands, First Ed. 1999-10-01, Ref. no. ISO/IEC 7816-8:1999(E)

[10] ISO/IEC 7816-9, Information Technology-Identification cards-Integrated circuit(s) cards with contact- Part - 9: Additional interindustry commands and security attributes, First Ed. 2000-09-01, Ref. no. ISO/IEC 7816-9:2000(E)

[11] Ian Hickman, Practical RF Handbook, EDC, Fourth Ed., 2006, ISBN:0750680393

[12] GSM 11.11, Specification of the Subscriber Identity Module, GSM Technical Specification, Version 5.0.0, Dec. 1995

[13] Bluetooth Special Interest Group, http://www.bluetooth.org

[14] Connected Limited Device Configuration, Sun Developer Network Inc., Sun Microsystems Inc., http://java.sun.com/products/cldc

[15] Sun Java Wireless Toolkit, Sun Microsystems Inc., http://java.sun.com/products/sjwtoolkit/

[16] Java Card Technology, Sun Microsystems Inc., http://java.sun.com/products/javacard

[17] RSA Cryptography Standard, Public Key Cryptographic Standards, RSA Cryptography Standard, 2002, v 2.1

[18] Rivest R.L., Shamir A., Adleman L.M., "A method of Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, v. 21, n. 2, Feb. 1978, pp 120-126.

[19] Secure Hash Standard, FIPS Publication 180-2, NIST, Washington, DC,2002 August 1, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

[20] Barker W.C., "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher", NIST, ver 1, May 2004

[21] Near Field Communication, NFC Forum, http://www.nfc-forum.org

[22] Whitfield Diffie, Martin E.Hellman, "New Directions in Cryptography", IEEE Trans. on Information Theory, Vol. IT-22, No. 6, Nov. 1976, pp. 644–654

[23] Whitfield Diffie, Martin E. Hellman, "Multiuser Cryptographic Techniques" National Computer Conf., New York, June 1976, pp. 109–112

[24] Rankl W., Effing W., "Smart Card Handbook", John Wiley & Sons, Ed.3

[25] Nokia 6131 phone, Nokia, http://europe.nokia.com/A4142118