Using Personal Devices For Authentication

Contrary to what many people believe, it is perfectly possible to make a counterfeit ATM and siphon money out of customers' accounts. A group of students is looking at ways to counter this danger!

Cholena Deb
'i.t.' Bureau

The automated teller machine (ATM) has now become an integral part of our cities. Indeed, it has emerged as the preferred option for depositing and withdrawing money from bank accounts. However, in the present scenario, users have no choice but to trust the ATM. However, there can be a bogus ATM too, which can read the users' details from the card and even take their personal identification number (PIN), without dispensing services. The identification details thus stolen can be misused to transfer money from the bank account of such gullible users. A group of students and their professor have come up with a system to tackle this problem.

The invention is based on a system where your personal device (such as a mobile phone, PDA or a laptop) is used for authentication and secure communication with the service provider's equipment (for example, a bank ATM) for access to the services (such as a money transaction). Employing strong cryptographic technology that is built using Java-enabled mobile phones with Bluetooth or near field communication (NFC) technology, the system works both ways; it helps the ATM/ bank to identify the users and also confirms the genuineness of the ATM machine. Once authenticity is established, both sides are sure about the identity of the other party and can go ahead with the transaction.

The invention is a combined effort of Ankit Sharma, Vikas Gelara, Abhishek Gaurav, Nitin Munjal and Professor Rajat Moona of IIT Kanpur.

A matter of security

Currently, mobile phones are used to authenticate the service provider's equipment in order to pass the information related to the user's identity. At the time of registration, users are supposed to carry their mobile phone to the bank, and the

Employing strong cryptographic technology... the new authentication system works both ways—it helps the ATM/ bank to identify the users and also confirms the genuineness of the ATM machine.

bank enables their mobile phone with a software that includes strong cryptographic technology. The users thereafter, get a public key. This public key can be used to establish contact with a genuine ATM. After the authentication, the mobile phone's display and keyboard can be used to access ATM services.

From the user's perspective, keeping account information on the phone may also prove risky as the phone may get lost or accessed by someone else. A smart card provides greater security, as even if the smart card is lost, the information is protected, as the keys cannot be deduced from the card.

If a smart card is used, the phone just acts as a smart card reader and an extension to the ATM. Otherwise, the phone has to be kept safely so that the keys and other information are not leaked out.

Thus for enhanced security, the user is also provided with a smart card (if NFC technology is used, it can be a contactless smart card) by the service provider such as a bank, for using its services. The smart card carries the user's information, which is digitally signed by the bank. Only a genuine ATM would be able to read the card and save the user from being taken for a ride.

"We created a model of this technology in the summer of 2006 but patented it in March 2008. We built a small prototype where the ATM was replaced by a personal computer. Since then we have developed several modules including the smart card-based approach, user authentication to the mobile phone, and mobile phone authentication to the smart card to ensure that a mobile phone lost by you is unusable for service transactions. We are currently talking to several companies in this regard," reveals Moona.

Implementing the idea

When you use an ATM in your vicinity, you are sure about its authenticity, but what if you are travelling to an unfamiliar place? You could be fooled by an ATM designed to steal information from you. This issue motivated the students to come up with a solution. "We noticed a basic flaw in the ATM-based service where a user is forced to trust the ATM. In addition, we were also aware of the financial inclusion issues concerning India where a large part of the population is not covered by banking services due to large transaction costs, which turn out to be huge overheads for the micro-finance sector. These were the reasons enough for us to think innovatively," states Moona.

The biggest hurdle for the team was to identify problems, model them and come up with a solution that was robust and would work for both urban and rural populations. "Any solution to the financial inclusion problem, which does not include the urban population, is likely to fail, as it will create a parallel system of banking which is not sustainable. With our technology we will be able to create a public call office (PCO) model wherein operators would implement an ATM to dispense money, etc. Currently, the banking sector owns the ATMs, making the costs of the transactions very high. With our model, it will be possible for an ATM owner to serve several banks, possibly on a transaction commission basis and provide the banking services to people who are based in remote areas and cannot directly access banking services. It is best suited for the rural set-up where users transact a small amount of money, which is sometimes lower than the cost of a single transaction," clarifies Moona.

IIT Kanpur is funding this novel endeavour. For a deployable solution, the team is still seeking funding aid. The team has also received technical assistance from several firms, including smart card companies, reader companies, and semiconductor manufacturers.

Moona reveals that the team is looking for partners who will be able to use this technology and deploy it. The group will be approaching banks and other service providers for implementing this technology in their service portfolios.

Given its benefits, we think they will find this solution hard to ignore. Customers won't be complaining! IT