

Login to the future with.....



.....
PRAYAG NARULA, DEEPANK GUPTA, PRACHI KALRA NSIT, NEW DELHI, INDIA

MOTIVATION

102-1099346786
naaz811, 1103586921
KK234597770011G
.....

Well this is no gibberish. This is how Airtel, Gmail, and India's electoral office know me. As of now, this is my identity. Now you know about it, so you can do a lot of things, from hacking my account, spamming, causing me financial losses (amounting to HUGE if I had also provided my credit card number). And considering the current state of security provided during data transfer on the net, getting someone's personal information is not a challenging job. You can design a fake webpage, well quite similar to a well known site's; and fool the poor person into giving his private information just because he could not notice www.bankofamerica.com has an 'a' missing. This is called **phishing**. Visitors are encouraged to input personal information, usually after receiving an email requesting they confirm log-in details or check the status of an order. Such emails are sent out to millions of addresses and usually contain warnings that action must be taken immediately in order to frighten the recipient into acting without thinking.

Web monitoring and hosting companies work hard to shut these websites down within days but they can harvest thousands of account details in that time. Online banks in particular have been targeted but so have been eBay and Pay Pal.

The damage caused by phishing ranges from loss of access to email to substantial financial losses. This style of identity theft is becoming more popular, because of the ease with which unsuspecting people often divulge personal information to phishers, including credit card numbers, security card numbers, and mothers' maiden names.

Once this information is acquired, the phishers may use a person's details to create fake accounts in a victim's name, ruin a victim's credit, or even prevent victims from accessing their own accounts.

It is estimated that between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by phishing, totaling approximately \$929 million USD. U.S. businesses lose an estimated \$2 billion USD a year as their clients become victims.ⁱ In the United Kingdom losses from web banking fraud — mostly from phishing — almost doubled to £23.2m in 2005, from £12.2m in 2004ⁱⁱ, while 1 in 20 users claimed to have lost out to phishing in 2005.ⁱⁱⁱ

PRESENTING.....THE P-Card



*Feeling insecure already...thinking of giving up online transactions...why should you? Internet shopping and online banking are one the most convenient methods to do your chores. You have every right to enjoy and use them; and we help you do so through **the P-CARD.***

Fingerprint Scanner

Smart Card and Reader



The **P-CARD** is an electronic smart card that contains your *personal information in encrypted* form which can be accessed only after you have been **verified by your fingerprint** and **your card has verified the service you are using.**

Oh yes this is the catch, a renaissance can be brought about in the domain of online transactions. Picture this.....

“.....The banks you visit online, the shopping sites, your email service providers have our service, **the P-Service** (client side smart card framework). To use their services you have a P-Card. Your P-card authorizes you as a valid user after matching your fingerprints. Then the P-Card sends its serial number encrypted by the P-Service's public key. The **P-Service** receives the serial number, decrypts it using its private key. The P-Service being available directly as the server, checks against your serial number and makes the web-service available to you. **So the fingerprint has authorized you hence preventing impersonation even if you lose your card; and our P-Service authorizes you to a genuine service, so you can feel secure about sending out your information.....**”

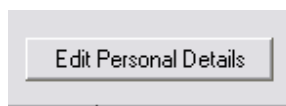
TECHNICAL TALK AND USABILITY

THE P-CARD TOOLBAR



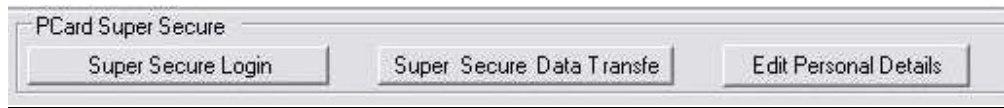
Though everyone wants security against identity thefts, but the inconvenience caused is the biggest deterrent. No one wants to switch from their browser to some other application just to log into their Email accounts. That's where the novelty of P-Card Toolbar comes in. This toolbar is the interface between the P-Service (present at requested service's server) and the P-Card. **As you run the P-Card application, the tool bar appears in your web-browser (currently developed for MS Internet Explorer 6.0). There is no need to run any separate application. Everything is just a click away.**

1) Edit Personal Details



This button helps you enter your personal details when running the application for the first time which can be edited later. Verification through fingerprints is required to edit these details. Your original fingerprint is stored when you run this application for the first time. You are authenticated against this original fingerprint every time you login.

2) P-Card Super Secure



The central theme of our application that aims at combating identity thefts is the P-Card Super Secure. It would terminate the era of using user-names and passwords to use online services. It would practically terminate phishing and key logging by the provision of P-Service at the back end and the 'Super Secure Data Transfer' that automatically feeds data online from the smart card without you typing it.

In this application we demonstrate its use with the help of a dummy service you want to use, which could be any bank's site or your email.

- Hit 'Super Secure Login' to use our dummy service.
- A message box appears asking for your fingerprints.

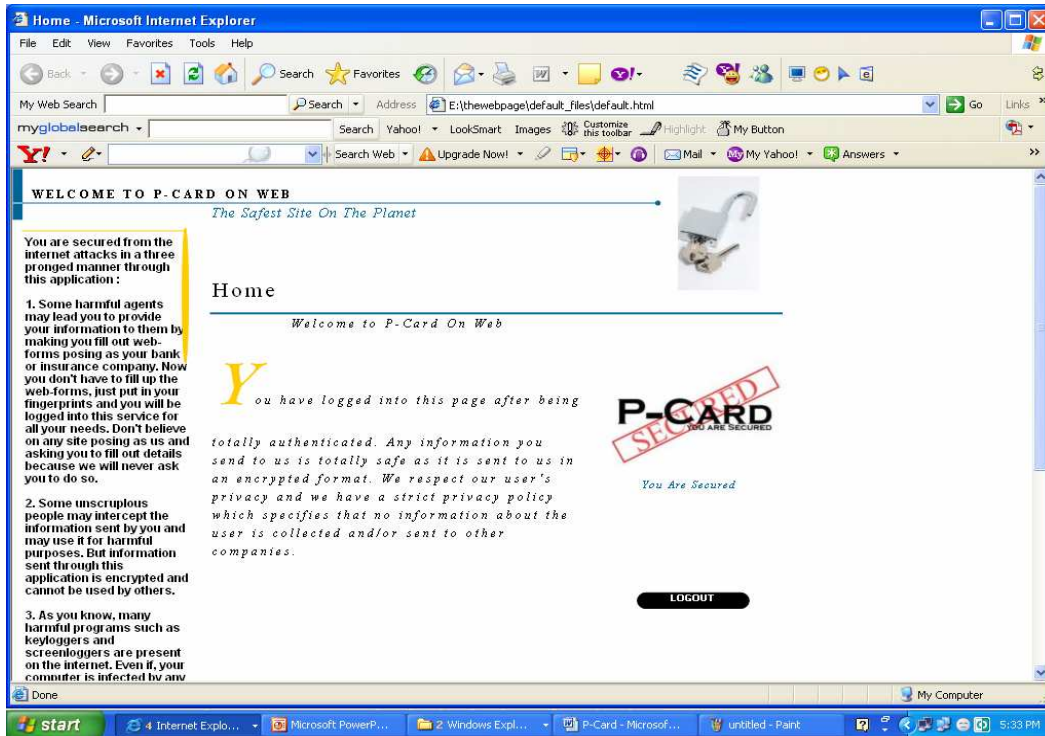


- After you provide your fingerprints, the P-Card checks against your original fingerprint.

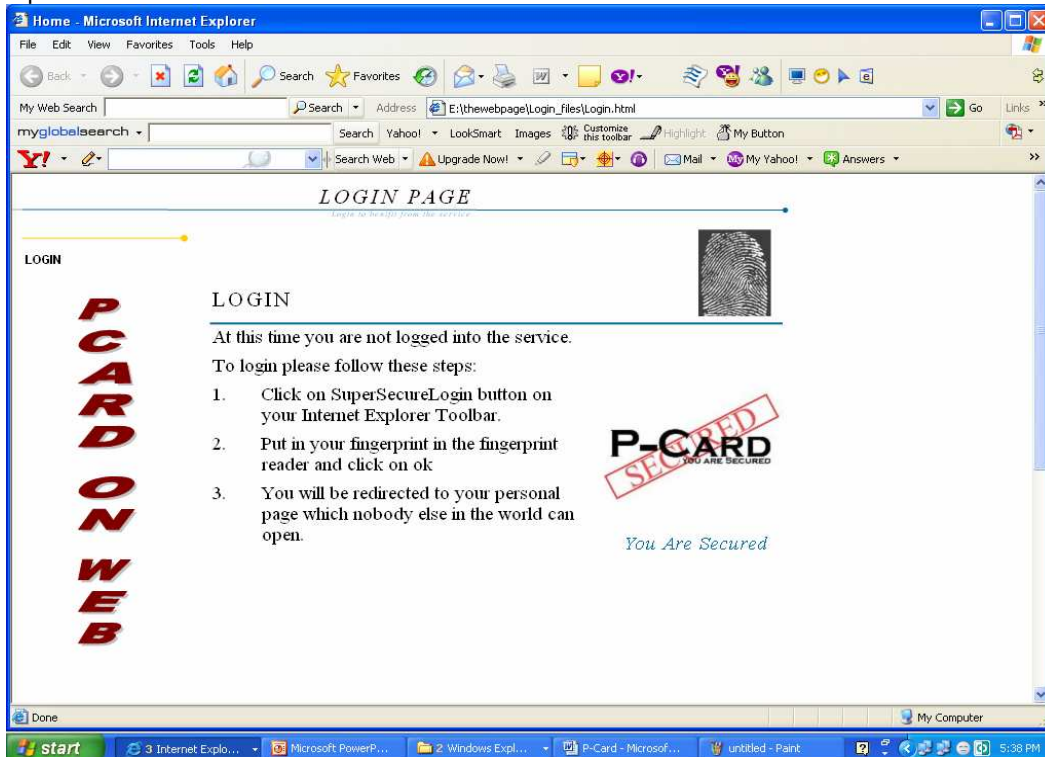


- If verification is successful, the card sends its 'serial number' to the P-Service using the RSA algorithm for encryption, which is one of most powerful methods of encryption in present time.
- The P-Service present at the dummy service's server opens your account using the serial number provided.

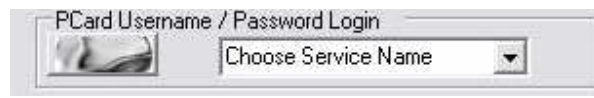
Upon successful login




Upon unsuccessful verification



3) P-Card Username/Password Login



Till the time online services start using P-Card Super Secure Login, we provide a variant to the present users. Press  to add a service in the 'choose Service Name'. You provide a user-name and the P-Card automatically generates a random password for that service. Once you update your password to this you can login to the service by just click of a button. Simply select that service from the drop down menu and the P-Service would automatically enter your user-name and password to that service. This not only saves from key and screen loggers but also saves someone from "guessing" your password. You don't need to remember your passwords anymore. Neither do you have to save these passwords in word files anyone can access. Your passwords are safely locked inside the security of the smart card.

INSIDE THE APPLICATION

1) Internet Explorer Toolbar: The toolbar is developed using c#, using the age old method given by Pavel Zolnikov. The code can be found at <http://www.codeproject.com/csharp/dotnetbandobjects.asp>. The dll built is loaded into the Global Assembly Cache (GAC) along with all the dependencies to make it visible to the internet explorer.

2) Fingerprint analysis: The software for fingerprint analysis has been developed using MatLab. The MatLab function was compiled into a COM component and converted to strong named COM component named interop.fpdata.dll. This was necessary because only a strongly named assembly can be installed in GAC. It was assumed that the fingerprint reader places the image as 'C: \c0.bmp'.

3) Fingerprint authentication on smart card: This required float type support, implemented using string manipulation. RSA encryption was implemented along with file manipulation using the standard library.

4) Web service: A web service was developed which provide the RSA decryption functionality. This web service implements 'dot net smart card off card runtime'.

5) Website: A dummy website was developed which implemented this web service. It consisted of two pages, login and default. The web service

redirects the user to the default page if he is authenticated and to the login page otherwise.

YOU ARE RIGHT.....P-CARD IS UNIQUE

- ◆ P-service would only be available to genuine service providers; hence the data transfers over the net would be absolutely secure.
- ◆ The P-service would be directly available at the service provider's server, hence all middle man attacks are futile as the communication between the P-card and P-service takes place through encryption using the RSA algorithm.
- ◆ Phishing can be terminated most effectively with the use of P-card and hence millions of dollars lost each year due to identity frauds can be saved.
- ◆ The application provides a toolbar in your browser itself, no separate applications need to be launched.
- ◆ The fingerprints are verified in the P-card itself.
- ◆ The practice of keeping user-names and passwords can be ended as the P-Card's serial number would now identify you; moreover this serial number is provided by the card only after fingerprint verification. Hence security has been increased manifold.
- ◆ This would be a first of its kind campaign taken by online service providers to protect and preserve their users' identity, hence increasing the trust quotient.

WHY P-CARD WOULD SUCCEED?

1) The appeal of this product lies in its need, its need by millions.

Just Google 'Identity theft/fraud' and in a few seconds you would realize the entire world is suffering from it. You could be next. Losses due to identity frauds amount to billions across the world. Big names like eBay, Pay Pal, CSO, banks, all have suffered from it.

2) P-Card is attractive due to its simplicity.

To the end user, P-Card presents its absolutely convenient toolbar, which makes possible every operation just a click away. Online services would have their customer base increased as online transactions become secure and trustworthy.

3) P-Card is tempting because it is super secure.

The charm of P-Card lies in combination of biometric authentication and direct interaction with the service provider through P-Service using RSA algorithm of encryption.

This application could end the era of user-names and password.

4) P-Card is totally prepared for the following scenarios.

In case the smart card is lost no third person can use it as editing of personal details and login both requires fingerprint verification. In case

a third person has your personal details he cannot misuse them on P-card supported online services as they take your personal details only through Super Secure Data Transfer and that too after fingerprint verification.

THE FINAL LEAP

- The P-Card Package would consist of a P-Card, smart card reader, P-service toolbar launcher, fingerprint reader.
- Today many laptops are coming with biometric authentication, so P-Card can be directly integrated with those without the fingerprint reader. We can update the P-Card to include an application which interacts with the inbuilt fingerprint reader.
- The cost to the end user would prove to be minimal due to the ever-falling prices of smart card and fingerprint readers which are available for as low as US\$30.
- The cost deploying our P-service at the online services' servers would be far far less than the losses they bear due to identity frauds.
- Crimes involving identity thefts are difficult to solve and use enormous resources of the investigating party; this is another factor that would help in deploying the P-Card.
- Hundreds of conferences take place everyday to combat identity theft, many laws and acts have been passed to protect people and organizations. Amidst this ever increasing complexity and confusion, P-Card would prove to be an acceptable application as it can be launched without making any major changes in the existing system.

P-Card is an application of the future

LOGIN To the Future with



-
- ⁱ Kerstein, Paul. "[How Can We Stop Phishing and Pharming Scams?](#)" *CSO*, July 19, 2005.
- ⁱⁱ "[UK phishing fraud losses double](#)", *Finextra*, March 07, 2006.
- ⁱⁱⁱ Richardson, Tim. "[Brits fall prey to phishing](#)", *The Register*, May 3, 2005.