CALIFORNIA STATE SCIENCE FAIR
2011 PROJECT SUMMARY

Name(s) **Paras J. Jain**	**Project Number** **S1414**

Project Title

SmartCheck: Innovating Credit Card Security through Smartphone Based Handshake Protocols, Fingerprinting, and Encryption

Abstract

Objectives/Goals

I have a very strong motivation for my project. Five months ago, VistaPrint stole my parent#s identity and made many fraudulent charges to the card weeks after the initial purchase. The problem with today#s system is that information can be reused. Identity fraud is responsible for a $221 Billion loss every year # my project saves that.

My question was: How can credit card security be improved in online and in-store transactions without reducing consumer ease-of-use? My hypothesis for my question was: Credit card security can be improved without harming consumer ease-of-use by using smartphones to replace the physical card.

Methods/Materials

The first step was to determine the effectiveness of modern day encryption. I ran a test with the three most used hashing algorithms, MD5, SHA1 and CRC16/32 against my two algorithms, SCA and SCB. Five trials were conducted. My two algorithms also included information on the user making the request, making it mathematically at least 1,000x as difficult to break. I found that my SCB algorithm was practically unbreakable with modern hardware. I used a smartphone, a Secure Server Stack, a POS Thin Client, a fingerprint reader and a top-of-the-line test computer.

I then had to create an implementation of my design. I made an iPhone application that would generate a verification code from purchase information and many pieces of user information. The hash is practically unbreakable so this information can#t be accessed. The vendor sends this code to the server and if the code generated on the server matches, payment is authorized.

Results

The results of this were tremendously promising. It took 8.3hours and 12.7hours to crack CRC 16/32, respectively. It took 35.2hours to break MD5. It took 28.5hours to break SHA1 and 92.7 hours to break SCA. Over the period of 2weeks, SCB was unbroken and little progress had been completed. The tests were run in worst-case-scenario where the hypothetical hacker had access to the server, the code and the database.

Conclusions/Discussion

The practical applications of my research are huge. Primarily, the credit card industry could benefit from this. Also, business security and the encryption of military applications can be greatly secured as my SCB algorithm was practically unbreakable. I was able to break the SHA1 algorithm in 30hours # frightening as it is used heavily by the US military. This experiment was a fantastic success.

Summary Statement

This project aimed to find a way to improve the security of credit cards without reducing user ease-of-use; the results are promising as the encryption I created is unbreakable with current hardware and the implementation was secure.

Help Received

All of the project was done independently but I would like to thank: Family and Teacher helped motivate me through the project; Brother helped make board; Mother helped design of board; Sister helped proofread submission; Father inspired me to go into STEM