Research Statement

Payas Gupta
School of Information Systems, Singapore Management University
Tel: (65) 97278657; *Email*: payas.gupta.2008@phdis.smu.edu.sg
Webpage: http://www.mysmu.edu/phdis2008/payas.gupta.2008

1. Background

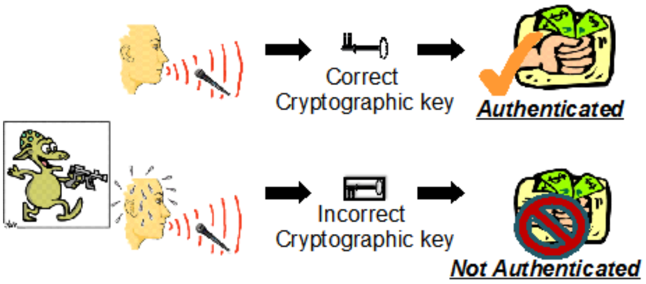
When I was a kid, I read somewhere that "*if you are sick and not well, do not go to pursue a medical degree instead go to a professional and take a medicine*". My motivation for doing research and finding novel solutions to interesting problems stems from thoughts like the former. I sincerely believe that if you are stuck with some problem and do not have a good solution to that problem then start looking into other areas and consult a scholarly person in that field. This we have seen from time to time and the prime examples of this are *speech processing* and *voice recognition* using Hidden Markov Model. It is a perfect blend of what we call an 'interdisciplinary' work. My research philosophy is to think out of the box while sitting inside the box. I strongly believe in the saying "*A picture speaks a thousand words*" and apply it to most of my papers, reports and presentations.

My research revolves around the theme of security and privacy aspects of human behaviour. It is just the starting and around this theme I have figured out numerous novel problems. In particular, I have research thrusts in the areas of Authentication, Human factors design for computer security, Security & Privacy issues in Social Networks, Mobile and Biometric systems.

2. Current and Future Research

2.1 Fight against Coercion Attacks

In computer authentication, there are various mechanisms to verify an individual's identity. These include passwords, hardware tokens and biometrics. We use these methods in our day to day life to authenticate ourselves to computer servers. However, most of these schemes are not resistant to coercion attacks in which the user is forcefully asked by an attacker to reveal the secret information. When the user's life is threatened by an attacker, one would have to surrender the secret information, and the system will be compromised despite all nice security properties.



I am interested in determining answer to two important problems firstly, what happens when an attacker coerces a user to reveal his/her own secret information e.g. cryptographic key. Secondly, I am also interested in determining the scenario when a user is coerced to reveal out the secret information of others (colleague or family member). Emotional response is one such direction to handle this problem. Inclusion of emotional response in the current key generation techniques can be used to fight against coercion attacks in key generation. However, there has to be a few requirements for a key generation technique to be coercion resistant. For a cryptographic key generation technique to be coercion attack resistant, it is required that when the user is under coercion, he/she will have no way of generating the key, or the key generated will never be the same as the one generated when he/she is not being coerced. If this requirement is met, then an adversary would not apply any threat to him/her because the adversary understands that the user would not be able to generate the key when he is threatened to do so.

With this goal in mind, we introduced a new model to incorporate the emotional response parameter (skin conductance) in current biometric (voice) key generation approach to fight against coercion attacks [1]. We formalized and analysed that the extent to which this property can be advantageous in various scenarios. We also analyse the case when a very skilled attacker can obtain a key generated from the stressed skin conductance response to re-engineer a few bits of a key generated from the normal skin conductance response.

2.2 Security & privacy issues in Social Networks

Humans are social animals by nature and social networks are just one other outlet for humans to interact. Social networks are used to make friends and business contacts online. Today's generation love to log each and every thought using status updates, all moments in their life by uploading photos and videos. However, unlike other human social interactions which are transient, e.g. talking to friends over lunch, the Internet keeps a permanent record of what we say to each other. If you are having an online conversation with your friend(s) then you should be aware that conversation can be seen by countless others and that a record of that conversation will be kept somewhere on the Internet. Indeed, now with some social networks introducing geolocation services a record of where we go and how long we spend there will also be maintained.

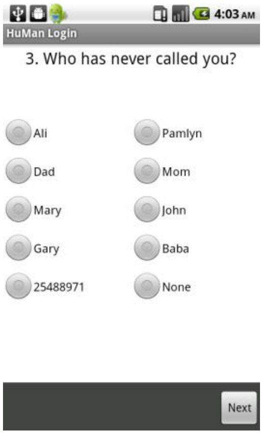
I am interested in profiling users based on their social network activity and how people interact with each other on public forums and later how this '*public*' information can be used to reveal the secret and private information of them. Secret questions (or challenge questions) is one such fine example which can be obtained from these public pages and forums. Secret questions are commonly used to authenticate users who have lost their passwords e.g. "Mother's maiden name", "favorite pets name". This password retrieval mechanism for a number of email and personal banking websites can lead to serious usability and security weaknesses. Today's personal security questions owe their strength to the hardness of an information-retrieval problem. However, as personal information becomes ubiquitously available online, the hardness of this problem, and security provided by such questions, will likely diminish over time.

2.3 Authenticating humans using their behavioral footprints

If we see the trend now, one can clearly predict the future of today's electronic products. In future most of the devices will posses the capability of connecting to the Internet and communicating with each other. Everything will be connected and communicating to everything else, uninterruptedly. Today, we humans leave our behavioral footprints in day to day life while using these devices e.g. mobile phones, biometric devices like fingerprint reader, interaction with digital media like TV or music players, computers, household items like microwaves or washing machines or mixer grinder, social networks and games, air conditioners, motor vehicles or cars, electrical equipments like lamps etc. Microsoft's surface touch table has already started to replace our old and traditional concept of table and in no time we will see sci-fi things like e-wardrobe, e-curtains, e-refrigerator etc to become reality. This list will grow rapidly in the coming decade and to such an extent that for us it will be impossible to think of a product without built-in network connectivity. People interact with these devices in day to day life knowingly or unknowingly. What, when, where and how these devices are used by a particular human being constitute the behavioral footprint of that person.

I am interested in designing a secure system which can authenticate users based on their behavior. If a user knows his/her own behavior then he/she does not need to remember extra stuff to login in to her email account or unlocking the phone using pin numbers. As, many non-technical people do not like to remember passwords and will frequently write them down on post-it notes and stick them to their computer - for example, there have been several studies of hospitals in recent years in which medical staff will do this.

Profiling or fingerprinting human behavior has been widely used in context-aware and security applications. My current research direction focus on generating behavioral fingerprints (a subset of footprints) of cellphone users and in future I would like to profile users based on activities and interactions with other products as well. In particular, I am interested in creating memorable fingerprints that can be easily remembered and validated by end users. These fingerprints are highly useful as they do not require any level of technical competency or literacy from the user, nor do they need to be memorized. We built a system, called HuMan, that generates these memorable fingerprints from cellphone data. To test HuMan, we conducted an extensive user study that involved collecting one month of continuous usage data from 58 Symbian S60 3rd Edition and Android V2.1 and above smartphone users. The data collected included call information and SMS records, application usage patterns, social networking and instant message activities, and game and multimedia usage patterns. We evaluated the memorable fingerprints generated from this rich multi-context data by asking each user to answer various authentication questions generated from the fingerprints. Our results show that the fingerprints generated by HuMan could be remembered by the user and that they were moderately secure against attacks even by family members and close friends (who are most likely to know the user's daily patterns and behavior).



3. Who has never called you?

○ Ali	○ Pamlyn
○ Dad	○ Mom
○ Mary	○ John
○ Gary	○ Baba
○ 25488971	○ None

Selected Publications and Output

[1] Payas Gupta and Debin Gao. 2010. Fighting coercion attacks in key generation using skin conductance. In *Proceedings of the 19th USENIX conference on Security* (USENIX Security'10). USENIX Association, Berkeley, CA, USA, 30-30.