**Security Model for Social Network**

Here are some issues and possible solution that can be handled in our Thesis project under the title name.  
  
**Scenario #1:**  
Say someone is using Facebook/Twitter from another one’s computer and after using, forgot to logout. A very common phenomena. That account can be hacked as it is already logged in.   
  
**Solution:**  
I propose a system that recognizes patterns, habits. A possible solution is that, while we chat/update status/comment, we use some words frequently. Not all the words can be mapped. But, some can be, due to the use of “short forms” as they are considered as spelling error, say “dwnld” is actually “download”. Some people always prefer using “dwnld” instead of “download” yet that same person prefer “upload” over “upld”. A collection on these words can be used as a pattern to identify the owner.   
Another possible solution is the use of general expressions like “hmm”, “yah”, “nope”. This are all simple expression, yet we use them frequently (the frequency can also be a parameter) and one prefer the use of “Yes” over “Yep”, while another may prefer using “hmmm…” over “hmm…” Or “hm” or even “okey” instead of “oka” or “ok”. These can also help to identify the owner.   
Yet another strong point to consider is the use of emoticons. We like to use them frequently, but only a handful of them. Some of us use only :-/ or ☺ or :-D or :’( and some large but common ones. We can also use it as a tool to recognize pattern.   
Apart from that, amount of time spends on homepage, average like/comment/status update per session can also be used.  
  
Put all these together with a threshold, the system can generate a warning of unusual behavior and send a text message to the owner and prompt a password request to stop the hacker from further use.   
  
  
**Scenario #2:**

Let’s think about what we share on social network, on our status updates/tweets/comments. Say something really funny happened while I was at an ATM withdrawing my monthly allowance and the story has something to do with the amount of money that I’ve withdrawn. So, I write down a funny status to share with my friends. Someone follows my status, calls the bank pretending to be me and says that he has lost his Credit Card and requests for another one. A handful of identification related question will be asked to verify the owner. Among those, your father’s name, your mother’s name, nominee of the account, your address etc are already public. What holds me to be me is the last transaction which I put already out there in public. So, my bank account gets hacked or at least I can be harassed.  
  
**Solution:**

Now think that one will somehow get a “warning” before posting that status as “What you are sharing is your private data. Do you want to proceed?” and after seeing that, he or she will reconsider and all that harassment will be avoided.   
So, how the system will know which ones are “private data” and which ones are not? Simple, if the system stores them time to time by asking simple questions. Say you log in to your account and a simple question appears at the top of the page “Who was your childhood best friend?” or “What is your middle name?” or “What was the name of the first pet you had?”. One may or may not answer them, but if they do, the system will enrich itself and in future, it can guide one what to share and what not to.   
One question still remains. Can we trust the system with that much information? Yes, it’s true we already share that publicly, one way or another, but they are at least scattered. But the system will organize that in a file under my name and what if someone sees that file? Two ways we can handle them. One, the system can reassure us with a privacy policy or two, the data can be stored as MD5 or such, in which way, even the system will never know what’s in there but will be able to verify them.

**Scenario #3:**

The era of social networking is about a decade old. The first generation is still using them but it is not far that that generation will pass and a new one will overtake. Hard truth is that, people will eventually die, but their social networking account will remain inactive for years along with all those private information. Some measures need to be taken in this regard.  
  
I propose a nominee system where an account will have a nominee and the nominee can issue a “death request” where all the friends of the owner will get a message to verify his/her death and if the result is above a mark (say 70% voted yes), the nominee will have access the owner’s account for a short period of time (7 days or so) before that account is permanently terminated. Within these period, a package will be available to the account. The package will hold all the necessary information about the owner, along with all the pictures/videos/status he/she updated so that the nominee can download them and keep them. With this system, the social network can sweep off their unused data, as well as the owner’s relative can get all the memories.

Scenario #4:  
We want to share something, but not publicly. So, there’re filters. They work pretty fine. But as days go by, teenagers are more and more getting involved in social networking. But we don’t have a filter for them, an under 18 filter. But we need one, as there are things one might want to share openly, say a TedX talk, which is held internationally to make people aware of different Taboo that we hold and speak openly about them.