A Two-Factor Authentication System using Mobile Phones
Nima Kaviani, Konstantin Beznosov  {nimak, beznosov}@ece.ubc.ca

Motivations

Weak & vulnerable authentication:
- Public PC are not secure for critical interactions
- Ease of accessibility by the attacker
- Existence of malicious software
- Authentication based on typed in username/password
- Chances for logging, shoulder surfing, or phishing
- Exposing long term credentials to the malicious user
- Password reuse is exploited by the malicious user

Usability issues:
- cell phones are hard to interact with
- Small screen size is a burden
- Keypads are cumbersome for data entry

Strong authentication solution:
- Cellphone as the trusted device
- One-time passwords as the second authentication
- One-time passwords are generated randomly

System Architecture

Threat & Benefit Analysis

Authentication Scenario

1. Joe is stuck at the airport, he needs to check his bank account information.
2. Joe decides to use a public computer (PC) at the airport. He knows that these computers might have malicious software installed on them.
3. Joe takes his cell phone, gets connected to the PC, and sends his already stored and encrypted credentials to the bank server via the PC. He does not need to remember his credentials, nor is worried of sniffing his connection from the cell phone to the untrusted client.
4. There is no way for a key logger to store Joe’s long term credentials as nothing is typed in by Joe and his credentials are all encrypted.
5. Joe is asked to enter a one-time password from the list of one-time passwords that has already been given to him from his bank.
6. Joe will be feeling more secure as a result of being able to protect his long time credentials while logging in to the computer that he does not trust very much, and securely using his desired services.
7. Even if a malicious user gets hold of Joe’s cell phone, the attacker still needs Joe’s list of one-time passwords to be able to use Joe’s username and password. The encrypted username and password is also of no use to the attacker.
8. Joe will be feeling more secure as a result of being able to protect his long time credentials while logging in to the computer that he does not trust very much, and securely using his desired services.

References:
2. Screen tear: http://fcfsorg-misc.nileweb.com/~realify/233/1/participants/sessions/fs/index.htm