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 bsed 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
- Long term credentials stored on the cellphone
- Cellphone as the first factor for authentication
- One-time password (OTP) for strong authentication
- One-time passwords are generated randomly
- One-time passwords as the second authentication factor for user identification
- Relying on RSA PKI / OpenSSL encryption
- A successful authentication requires both long time credentials and one-time passwords

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

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

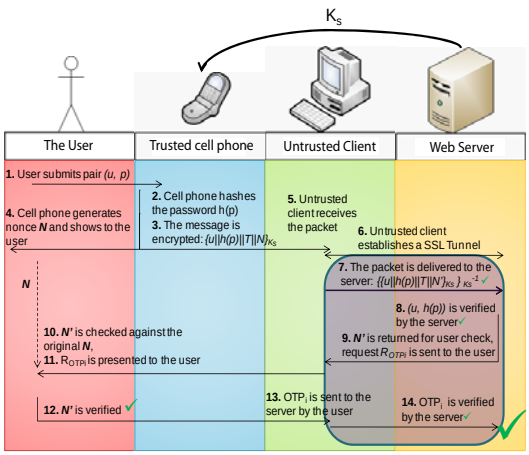
5. Joe is asked to enter a one-time password from the list of one-time password that has already been given to him from his bank.

6. Joe is safe from being shoulder surfed by the attacker as the one-time passwords are generated randomly and can be used only once. Thre is no possibility to reuse or find the next one-time password.

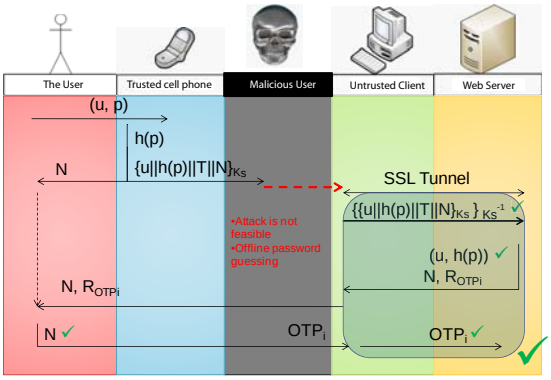
7. Even if a malicious user gets hold of Joe's cell phone, the attacker still needs Joe's list of one-time passwords to be able to use Joe's username and password. The encrypted username and password is also of no use to the attacker.

8. Joe will be feeling more secure as a result of being able to protect his long time credentials while logging in to the computers that he does not trust very much, and securely using his desired services.

System Architecture

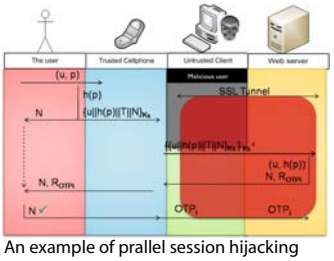


Threat & Benefit Analysis



An example of Active MiM attack when the attacker is intercepting the connection from the cell phone to the untrustedclient

1. Key Loggers (Secure)
2. Man-in-the-Middle
   - 2.1 Phishing (Nonce Verification)
   - 2.2 Active Man-in-the-Middle (Threat)
   - 2.3 Passive Replay Attack (Infeasible)
3. Session Hijacking (Nonce Verification)
4. Parallel Session Hijacking (Threat)
5. Shoulder Surfing (Secure)
6. Lost or Stolen cell phone (Partly Secure)
7. Lost or Stolen Pass Book (Secure)



An example of prallel session hijacking

References:
1. M. Mannan, P.C. van Oorschot. Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer. Financial Cryptography and Data Security (FC'07), Lowlands, Scarborough, Trinidad and Tobago, Feb.12-15, 2007.
2. Screen bean: http://freepages.misc.rootsweb.com/~nielsp/233/clipart/scrbeans/htm/index.htm

Department of Electrical and Computer Engineering
University of British Columbia
5500 - 2332 Main Mall
Vancouver BC V6T 1Z4 Canada

Laboratory for Education and Research in Secure Systems Engineering