15441 Paper Summaries, November 15, 2001

Suman Kumar Nath(sknath@cs.cmu.edu)

Password Hardening Based on Keystroke Dynamic

- *One line summary:* Presents a novel approach to improve security of passwords where legitimate user's typing patterns are combined with user's password to generate a *hardened password*.
- *Main points:*
  - *Problem with conventional textual passwords:* can be broken by an exhaustive search of a relatively small subset of all possible passwords.
  - Solution: Incorporate biometric information into the password to generate the *hardened password*. This makes the exhausted search difficult. The paper shows how user's typing patterns can be used as the biometric information.
  - *Challenges:* 1. Identifying features that reliably repeats, 2. Using the features when user types her password to identify her while identifying attacker who captures system information used to generate or verify hardened password.
  - A feature is represented by a function $\phi : A \times N \rightarrow R$ where $\phi(a, \ell)$ is the measurement of that feature during ℓ-th login attempt to account a. ϕ_i is *distinguishing feature* for the account a if $|\mu_{ai} - t_i| > k\sigma_{ai}$, where μ_{ai} and σ_{ai} are the mean and standard deviation of the past measurements of feature ϕ_i and t_i is some fixed system parameter.
  - The hardened password $hpwd_a$ is broken into $2m$ shares and are stored in an *instruction table*. Depending on the value of distinguishing features, shares are chosen from the table to construct the $hpwd_a$. If the distinguishing features of typing pattern is different from previous history, wrong pieces of shares will be chosen and constructed $hpwd_a$ will be wrong – which will prevent attacker to intrude the system. However, for a legitimate user, typing patterns will conform to the history, correct shares will be chosen from the instruction table, and correct $hpwd_a$ will be formed – which will allow her to access the system.
  - The authors showed the feasibility of the method by implementing their ideas in real system.
- *Flaws:*
  - As the authors mentioned, the system does not work when the typing patterns of the legitimate user changes (due to, say, change of keyboard). This may pose a psychological barrier in acceptance of the scheme to the users.
  - Even if the typing patterns remain unchanged, the scheme may not work when the users telnet to some remote machine – since attacker can record and replay the typing patterns. Solution: modify telnet/ssh clients to add salt to typing patterns while transmitting the typed password (*e.g.* transmit the characters with equal intermediate time space) and send the encrypted typing pattern information separately.
  - Only a very small fraction of real-world cryptosystems failure is because of password hacking. The complex scheme presented in this paper aims to make that *small* portion of attacks difficult.