Reading: The Emperor's New Security Indicators

Human Factors in Security

- Users ignore security functionality
- Psychological acceptability
- “users are idiot”
- “security people ...” ← bad lessons user learn
- Expired certificates
- Unauthenticated emails/phone calls (e.g. professor gave an example of TA received specious message from his bank)
- SSL disabled usually
- Random redirect
- Random failure

Challenges

- Users untrained
- Users may not care about security
- Heterogeneous software
- Different language, ages
- Users are the weakest link
- Security can fail silently
- Users need good feedback
- Dialog fatigue

Solutions

1. Secure Attention Key
   - Ctrl + Alt + Del (Windows)
     - User may forget
     - Fake keyboard attack (custom made keyboard)
2. Machine Registration/ Authentication
   - Answer security questions
   - Send a cookie
   - Can login only with cookie and correct password
3. Reflect action of user when they see question, type it in.
4. Click an link in registration email
   - Phisher must capture email before user checks the link
     - Sniff email
     - Ask user to reveal email
5. Security skins
• Login box with background image of user’s choice
6. Take the hash of certificate to generate random image
7. Password hash
   • User enters password
   • Submitted password as H(url || password)
     • Password hash does not indicate user in secure mode
     • No feedback