

# Human Factors in Security

Friday, May 01, 2009

1:07 PM

## Human Factors in Security

- Users ignore security functionality
- Psychological acceptability
- "Users are idiots"
- "Security people are idiots"

## Bad Lessons Users Learn

- Expired certs
- Unauthenticated emails/phone calls
- SSL Disabled by default
- Random Redirects
- Random Failures

"Trusted Path" - people trust the software and something could change something that the user may not know was able to be changed.

## Challenges

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

## Secure Attention Keys

- Ctrl-alt-del
- Users may forget
- The fake keyboard attack

"Conditioned - Safe Ceremonies" - protocol where you have a human specifically part of it.

## Machine Registration/Authentication

- you need to answer security questions
- Cookie is set
- Can only log in with password and cookie
- Can sniff email
- Ask user to reveal email

## "Security Skins"

Custom background on password prompt

- Weakest link is still the user
- URL Hashing could cause constant changing of picture

## Password Hash

- User enters password
- Submitted password is  $H(\text{url} || \text{password})$
- Password field on page would not automatically load and it didn't tell you if it was on or not.