Cognitive Security for Personal Devices

Rachel Greenstadt (greenie@cs.drexel.edu)
Jake Beal (jakebeal@mit.edu)

AI Sec
October 28, 2008
I must be dancing with Jake, after all, this guy knows Jake’s private key....
Human-style authentication
Computers could recognize other cues

Typing patterns
Touchpad patterns
Use patterns
Camera image
Posture/Device placement

It seems this is Mako and not, in fact, Jake
Cognitive Security

• Humans have rich and subtle mechanisms for handling trust and security

• Goal: Intelligent agents mediate security decisions between users and applications
  • Build user models via continuously-deployed multi-modal behavioral biometrics
  • Use models to aid security decisions
Mismatch Between Users and Machines: An AI and HCI Problem

• We must use human mechanisms sometimes
  • Example: passwords to keys

• Security automation considered harmful? [Edwards Poole Stoole 2007]
  • Context dependent security decisions
  • Can’t be pre-baked in
  • Need an agent to observe the context
Machine Imprint on Users, develop models of their behavior

Obviously not appropriate for all scenarios...
Architecture for Machine Integrity

- Sensitive Information
- Requires isolation
- Lots of research in this sort of model already
- Overhead? (VMMs, classifiers, etc) perhaps...
Once computers know their users, they can infer beliefs and goals

Alice:
* Knows she wants to visit her bank
* Doesn’t know she’s not at her bank

Alice’s device:
* Knows Alice is not visiting her bank
* Doesn’t know that Alice believes she is at her bank
Adjustably Autonomous Security

- Model users’ belief, desires, intentions
- Understand concepts
  - private information
  - expected program behavior
- simulate users’ judgment
- pass decisions up when appropriate
Current work

• Authentication
• Keystrokes
• Stylometry
• Anti-phishing
Thank You

• Questions?
• More detail available as MIT CSAIL Tech Report 2008-016
• http://dspace.mit.edu/handle/1721.1/40810
• Email: greenie@cs.drexel.edu, jakebeal@mit.edu