CSE 484 (Winter 2008)

User Authentication

Tadayoshi Kohno

Thanks to Dan Boneh, Dieter Gollmann, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Goals for Today

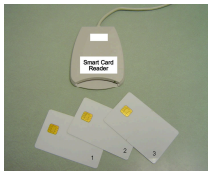
- CELT.
  - Thank you all for taking the time to talk with Jim Borgford-Parnell.
  - Met with Jim yesterday
  - Love to have your feedback on the blog
- User Authentication
  - Graphical Passwords
  - Biometrics
  - More

My goals with the blog

- Security mindset
  - News
  - Products
- Apply **high-level** concepts from class to the "real world"
  - Not technical issues
  - But threat modeling, considering and reflecting on adversaries, thinking about the "big picture"
- Collaborative discussions
  - Security is not something for one person to do on their own.
  - Best way to learn high level issues is to discuss with others
  - How many of you are reading other people's posts?
- Complementary to technical discussions in class
  - In class? In discussion section?
- Open discussion?

What You Have

- Smartcard
  - Little computer chip in credit card form factor



Smartcard Bank Cards [Drimer and Murdoch]

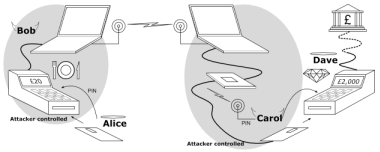


Image from http://www.cl.cam.ac.uk/research/security/projects/banking/relay/

Smartcard Bank Cards [Drimer and Murdoch]

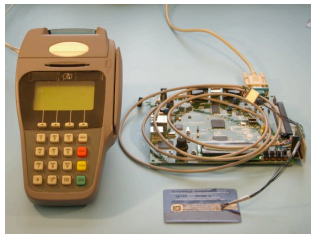


Image from http://www.cl.cam.ac.uk/research/security/projects/banking/relay/

Magstripe Writer

http://www.tyner.com/magnetic/msr206-1.jpg

"Improving" Passwords

- Add biometrics
  - For example, keystroke dynamics or voiceprint
  - Revocation is often a problem with biometrics
- Graphical passwords
  - Goal: increase the size of memorable password space
  - Rely on the difficulty of computer vision
    - Face recognition is easy for humans
    - Present user with a sequence of faces; user must pick the right face several times in a row to log in

Graphical Passwords

- Images are easy for humans to process and remember
  - Especially if you invent a memorable story to go along with the images
- Dictionary attacks on graphical passwords are difficult
  - Images are believed to be very "random" (is this true?)
- Still not a perfect solution
  - Need infrastructure for displaying and storing images
  - Shoulder surfing

- Passfaces slides omitted from online version

Empirical Results

- Experimental study of 154 computer science students at Johns Hopkins and Carnegie Mellon
- Conclusions:
  - "… faces chosen by users are highly affected by the race of the user… the gender and attractiveness of the faces bias password choice… In the case of male users, we found this bias so severe that we do not believe it possible to make this scheme secure against an online attack…"
- 2 guesses enough for 10% of male users
- 8 guesses enough for 25% of male users

User Quotes

- "I chose the images of the ladies which appealed the most"
- "I simply picked the best lookin girl on each page"
- "In order to remember all the pictures for my login (after forgetting my 'password' 4 times in a row) I needed to pick pictures I could EASILY remember... So I chose beautiful women. The other option I would have chosen was handsome men, but the women are much more pleasing to look at"

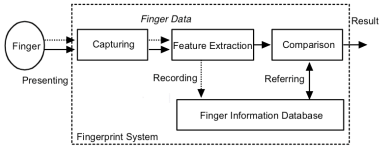
More User Quotes

- "I picked her because she was female and Asian and being female and Asian, I thought I could remember that"
- "I started by deciding to choose faces of people in my own race…"
- "… Plus he is African-American like me"

What About Biometrics?

- Authentication: What you are
- Unique identifying characteristics to authenticate user or create credentials
  - Biological and physiological: Fingerprints, iris scan
  - Behaviors characteristics - how perform actions: Handwriting, typing, gait
- Advantages:
  - Nothing to remember
  - Passive
  - Can't share (generally)
  - With perfect accuracy, could be fairly unique

Overview [Matsumoto]



Tsutomu Matsumoto's image, from http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Dashed lines for enrollment; solid for verification or identification

Biometric Error Rates (Non-Adversarial)

- "Fraud rate" vs. "insult rate"
  - Fraud = system incorrectly accepts (false accept)
  - Insult = system rejects valid user (false reject)
- Increasing acceptance threshold increases fraud rate, decreases insult rate
- For biometrics, U.K. banks set target fraud rate of 1%, insult rate of 0.01% [Ross Anderson]
  - Common signature recognition systems achieve equal error rates around 1% - not good enough!

Biometrics

- Face recognition (by a computer algorithm)
  - Error rates up to 20%, given reasonable variations in lighting, viewpoint and expression
- Fingerprints
  - Traditional method for identification
  - 1911: first US conviction on fingerprint evidence
  - U.K. traditionally requires 16-point match
    - Probability of false match is 1 in 10 billion
    - No successful challenges until 2000
  - Fingerprint damage impairs recognition
    - Ross Anderson's scar crashes FBI scanner

Other Biometrics

- Iris scanning
  - Irises are very random, but stable through life
    - Different between the two eyes of the same individual
  - 256-byte iris code based on concentric rings between the pupil and the outside of the iris
  - Equal error rate better than 1 in a million
  - Best biometric mechanism currently known
- Hand geometry
  - Used in nuclear premises entry control, INSPASS (discontinued in 2002)

Other Biometrics

- Vein
  - Pattern on back of hand
- Handwriting
- Typing
  - Timings for character sequences
- Gait
- DNA

Any issues with this?

Canon Files For DSLR Iris Registration Patent

Posted by kdawson on Tuesday February 12, @07:39PM
from the **biological-metadata** dept.

An anonymous reader writes

> "Canon has filed for a patent for using iris watermarking (as in the iris of your eye) to take photographer's copyright protection to the next level. You set up the camera to capture an image of your eye through the viewfinder. Once captured, this biological reference is embedded as metadata into every photo you take. Canon claims this will help with copyright infringement of photos online."