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

- User Authentication
  - Biometrics
  - Password Managers
  - Authentication schemes

Issues with Biometrics

- Private, but not secret
  - Maybe encoded on the back of an ID card?
  - Maybe encoded on your glass, door handle, ...
  - Sharing between multiple systems?
- Revocation is difficult (impossible?)
  - Sorry, your iris has been compromised, please create a new one...
- Physically identifying
  - Soda machine to cross-reference fingerprint with DMV?

Issues with Biometrics

- Criminal gives an inexperienced policeman fingerprints in the wrong order
  - Record not found; gets off as a first-time offender
- Can be attacked using recordings
  - Ross Anderson: in countries where fingerprints are used to pay pensions, there are persistent tales of "Granny's finger in the pickle jar" being the most valuable property she bequeathed to her family
- Birthday paradox
  - With false accept rate of 1 in a million, probability of false match is above 50% with only 1609 samples

Issues with Biometrics

- Anecdotally, car jackings went up when it became harder to steal cars without the key
- But what if you need your fingerprint to start your car?
  - Stealing cars becomes harder
  - So what would the car thieves have to do?

Risks of Biometrics

BBC NEWS | The News in 2 minutes | News services: Your news when want it

News Front Page | Africa | Americas | Asia-Pacific | Europe | Middle East | South Asia | UK | Business | Health | Science/Nature | Technology | Entertainment

Last Updated: Thursday, 31 March, 2005, 10:37 GMT 11:37 UK

E-mail this to a friend | Printable version

Malaysia car thieves steal finger

By Jonathan Kent
BBC News, Kuala Lumpur

Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system.

The car, a Mercedes S-class, was protected by a fingerprint recognition system.

Accountant K Kumaran's ordeal began when he was run down by four men in a small car as he was about to get into his Mercedes in a Kuala Lumpur suburb.

SEE ALSO:
* Malaysia to act … pirates
16 Mar 05 | As…

RELATED INTER…
* Malaysian police…
The BBC is not r… for the content o… internet sites

TOP ASIA-PACIF… STORIES
* Australians warn… cuts
* Taiwan campus…

http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

Biometric Error Rates (Adversarial)

- Want to minimize "fraud" and "insult" rate
  - "Easy" to test probability of accidental misidentification (fraud)
  - But what about adversarial fraud
    - Besides stolen fingers
- An adversary might try to steal the biometric information
  - Malicious fingerprint reader
    - Consider when biometric is used to derive a cryptographic key
  - Residual fingerprint on a glass

Voluntary: Making a Mold

[Matsumoto]

Put the plastic into hot water to soften it.

Press a live finger against it.

The mold

It takes around 10 minutes.

http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Voluntary: Making a Finger

[Matsumoto]

Pour the liquid into the mold.

Put it into a refrigerator to cool.

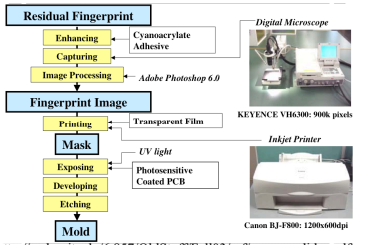
It takes around 10 minutes.

The gummy finger

http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Involuntary

[Matsumoto]



KEYENCE VH6300: 900k pixels

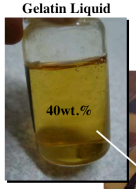
Canon BJ-F800: 1200x600dpi

http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

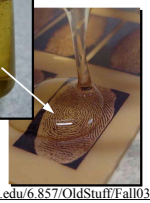
Involuntary

[Matsumoto]

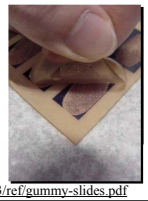
Gelatin Liquid



Drip the liquid onto the mold.



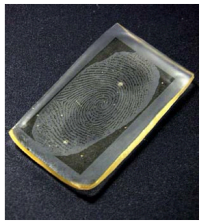
Put this mold into a refrigerator to cool, and then peel carefully.



http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Involuntary

[Matsumoto]



http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Authentication by Handwriting

[Ballard, Monrose, Lopresti]

- Maybe a computer could also forge some biometrics

Generated by computer algorithm trained on handwriting samples

Password Managers

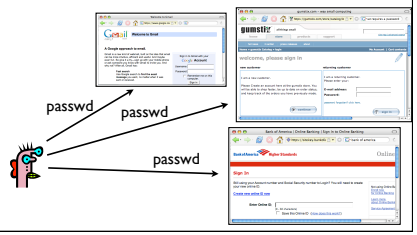
- Idea: Software application that will store and manage passwords for you.
  - You remember one password.
  - Each website sees a different password.
- Examples: PwdHash (Usenix Security 2005) and Password Multiplier (WWW 2005).

Key ideas

- User remembers a single password
- Password managers
  - On input: (1) the user's single password and (2) information about the website
  - Compute: Strong, site-specific password
- Goal: Avoid problems with passwords

The problem

Alice needs passwords for all the websites that she visits



Possible solutions

- Easy to remember: Use same password on all websites. Use "weak" password.
  - Poor security (don't share password between bank website and small website)
- More secure: Use different, strong passwords on all websites.
  - Hard to remember, unless write down.

Alternate solution: Password managers

- Password managers handle creating and "remembering" strong passwords
- Potentially:
  - Easier for users
  - More secure
- Examples:
  - PwdHash (Usenix Security 2005)
  - Password Multiplier (WWW 2005)

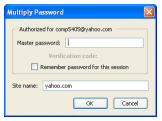
PwdHash

@@ in front of passwords to protect; or F2

sitePwd = Hash(pwd,domain)

Prevent phishing attacks

Password Multiplier



Active with Alt-P or double-click

sitePwd = Hash(usrname, pwd, domain)

Both solutions target simplicity and transparency.

Usenix 2006: Usabilty testing

- Are these programs usable? If not, what are the problems?
- Two main approaches for evaluating usability:
  - Usability inspection (no users)
    - Cognitive walk throughs
    - Heuristic evaluation
  - User study
  - Controlled experiments
  - Real usage

This paper stresses need to observe real users

[Chiasson, van Oorschot, Biddle]

Study details

- 26 participants, across various backgrounds (4 technical)
- Five assigned tasks per plugin
- Data collection
  - Observational data (recording task outcomes, difficulties, misconceptions)
  - Questionnaire data (initial attitudes, opinions after tasks, post questionnaires)

[Chiasson, van Oorschot, Biddle]

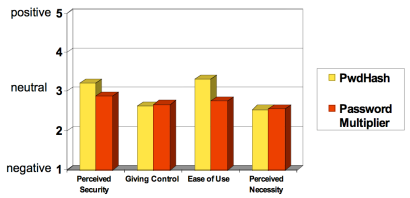
Task completion results

	Success	Potentially Causing Security Exposures			
		Dangerous Success	Failures		
			Failure	False Completion	Failed due to Previous
PwdHash					
Log In	48%	44%	8%	0%	N/A
Migrate Pwd	42%	35%	11%	11%	N/A
Remote Login	27%	42%	31%	0%	N/A
Update Pwd	19%	65%	8%	8%	N/A
Second Login	52%	28%	4%	0%	16%
Password Multiplier					
Log In	48%	44%	8%	0%	N/A
Migrate Pwd	16%	32%	28%	20%	N/A
Remote Login	N/A	N/A	N/A	N/A	N/A
Update Pwd	16%	4%	44%	28%	N/A
Second Login	16%	4%	16%	0%	16%

http://www.scs.carleton.ca/~achiasso/Chiasson_UsenixSecurity2006_PwdManagers.ppt

[Chiasson, van Oorschot, Biddle]

Questionnaire responses



http://www.scs.carleton.ca/~achiasso/Chiasson_UsenixSecurity2006_PwdManagers.ppt

Problem: Transparency

- Unclear to users whether actions successful or not.
  - Should be obvious when plugin activated.
  - Should be obvious when password protected.
- Users feel that they should be able to know their own password.

Problem: Mental model

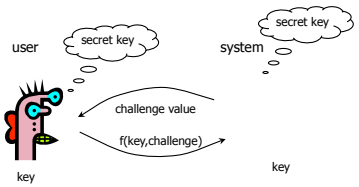
Users seemed to have misaligned mental models

- Not understand that one needs to put "@@" before *each* password to be protected.
- Think different passwords generated for each session.
- Think successful when were not.
- Not know to click in field before Alt-P.
- PwdHash: Think passwords unique to them.

When "nothing works"

- Tendency to try all passwords
  - A poor security choice.
  - May make the use of PwdHash or Password Multiplier *worse* than not using any password manager.
- Usability problem leads to security vulnerabilities.

Challenge-Response (Over Network)



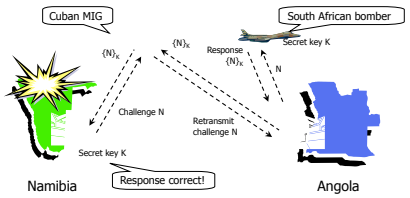
Why is this better than a password over a network?

Any problems remain?

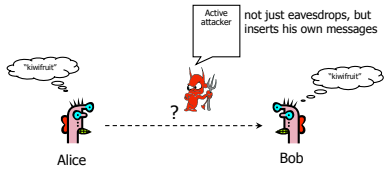
Challenge-Response Authentication

- User and system share a secret key
- Challenge: system presents user with some string
- Response: user computes response based on secret key and challenge
  - Secrecy: difficult to recover key from response
    - One-way hashing or symmetric encryption work well
  - Freshness: if challenge is fresh and unpredictable, attacker on the network cannot replay an old response
    - For example, use a fresh random number for each challenge
- Good for systems with pre-installed secret keys
  - Car keys; military friend-or-foe identification

MIG-in-the-Middle Attack [Ross Anderson]



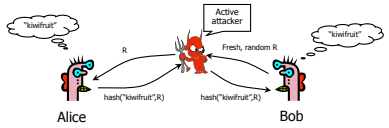
Authentication with Shared Secret



Alice and Bob share some secret.
How can they identify each other on the network?

What have we learned from the systems we've seen?

Challenge-Response

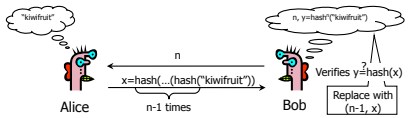


- Man-in-the-middle attack on challenge-response
  - Attacker successfully authenticates as Alice by simple replay
- This is an attack on authentication, not secrecy
  - Attacker does not learn the shared secret
- However, response opens the door to offline dictionary attack

Encrypted Timestamp

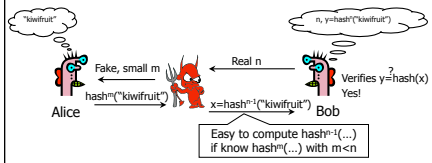
- Requires synchronized clocks
  - Bob's clock must be secure, or else attacker will roll it back and reuse an old authentication message from Alice
- Attacker can replay within clock skew window

Lamport's Hash



- Main idea: "hash stalk"
  - Moving up the stalk (computing the next hash) is easy, moving down the stalk (inverting the hash) is hard
  - n should be large (can only use it for n authentications)
- For verification, only need the tip of the stalk

"Small n" Attack



- First message from Bob is not authenticated!
- Alice should remember current value of n

Adversaries To Consider

- Eavesdropper
- Pretend to be Bob and accept connections from Alice
- Initiate conversation pretending to be Alice
- Read Alice's database
- Read Bob's database
- Modify messages in transit between Alice and Bob
- Any combination of the above
- Offline vs online guessing attacks