Lecture 3 - 09/13/2019

Calculating suitable password size

G = # of guesses that an attacker can make in a single time unit
T = # of time units
N = # of passwords

Probability of an attacker guessing the password is $P \geq \frac{GT}{N}$

Strategies for reducing amount of guesses

Online Attacks	Offline Attacks
Exponential Backoff	Password Salting
Disable Account	One way function

E.g. Passwords composed of S symbols, each symbol comes from an alphabet of 96 characters

96 = 26 upper + 26 lower + 10 digits + 34 special characters

- Assume 10^4 guesses/second (Comes from threat model)
- Want the probability of successful guesses to be 0.5 over a year
- What is a suitable password length?

Start with formula:

$P \geq \frac{GT}{N}$

$N \geq \frac{GT}{P}$

$= \frac{10^4 \bullet (365 * 24 * 60 * 60)}{0.5}$

$= 6.31 * 10^{11}$

$96^S \geq 6.31 * 10^{11}$

$S \geq \frac{log(6.31 * 10^{11})}{log(96)}$

= 5.94 = Passwords should be 6 characters in length

Biometrics

Techniques:

- Fingerprints
- Voice
- Eyes
    - Retenal
    - Iris
- Face
- Hands
- Keystrokes
- Gait
- Earshape

Biological or Behavioural features change over time.

Reading is never identical

- Fales accept and false reject errors must be expected

Bad guy can steal input.

Combinations of Biometrics

Edna in the incredibles uses iris, voice, and hand recognition.

The false accept/reject rates for those are the following:

$FA_H = 1\%$ $FR_H = 10\%$	$FA_i = 5\%$ $FR_i = 1\%$	$FA_V = 10\%$ $FR_V = 5\%$

If the system uses the AND of the three FA/FR rates what would the FA/FR rate for the system be

What about using the OR?
AND:
FA = 1/100 * 5/100 * 10/100 = 50/1000000
$FR = 1 - [(1-FR_H) * (1-FR_I) * (1-FR_V)]$
= 1 - (90 * 99 * 95)
= 15.3%

FIDO (Fast Identity Online)

UAF

- Server stores a public key where the user holds the private key
- A challenge is sent to the user trying to log in where the private key is required

U2F

- A second factor challenge using a hardware token