Authentication with Passwords

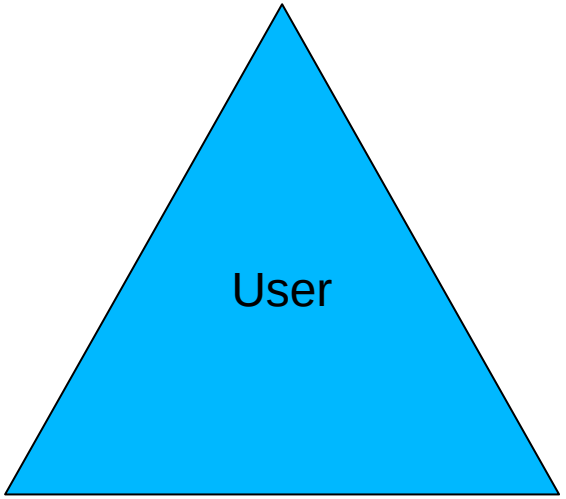
Prof. Ravi Sandhu
Executive Director and Endowed Chair

February 1, 2013

ravi.sandhu@utsa.edu
www.profsandhu.com

User Authentication

Something you know
e.g., passwords



Something you have
e.g., token, smartcard

Something you are
e.g., fingerprint

Single factor
Multi factor

Primary
Secondary

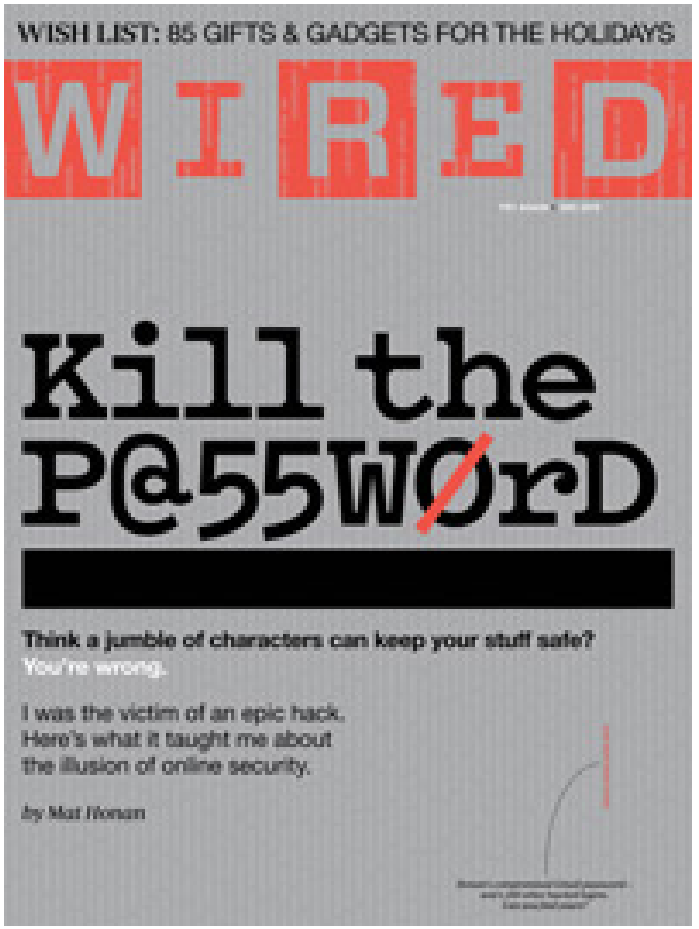
Weak
Strong

On Line Attack
Off Line Attack

Reset
Revocation

Single sign on
Reduced sign on

Kill the Password



Herley-Oorschot 2012 Quotes

- Many things have changed beyond recognition in the past 20 years, but passwords have advanced little.
- Arguably, the Internet could not have grown to its current size and influence without them.
- Repeated and sustained effort has failed to uncover a silver-bullet replacement for passwords. It's time to admit that this is unlikely to change.
- In the absence of a silver bullet, we can't escape the messy work of tradeoffs.
- We assert that passwords are the best fit for many (but alone, not the highest level of) authentication needs.

- We might say that passwords are the worst possible authentication system, except for all the other systems.

Herley-Oorschot Research Agenda

- Ending the Belief that Passwords Are Dead
- Understanding Strength and Attack Resistance
- Policies and Support Tools
  - Password aging policies.
  - Realistic password guidance.
  - Password managers.
- Prioritizing Competing Requirements

"Although passwords might not be viewed as the "rocket science" of security research, their scale of deployment is such that any improvement in their usability would be hard to equal for impact."

Herley-Oorschot Concluding Quote

- Although we lack the data to attach likelihoods to the individual pie-chart threats, we can reasonably conjecture that keystroke logging harvests more passwords than phishing and phishing harvests more than online brute-force attacks.

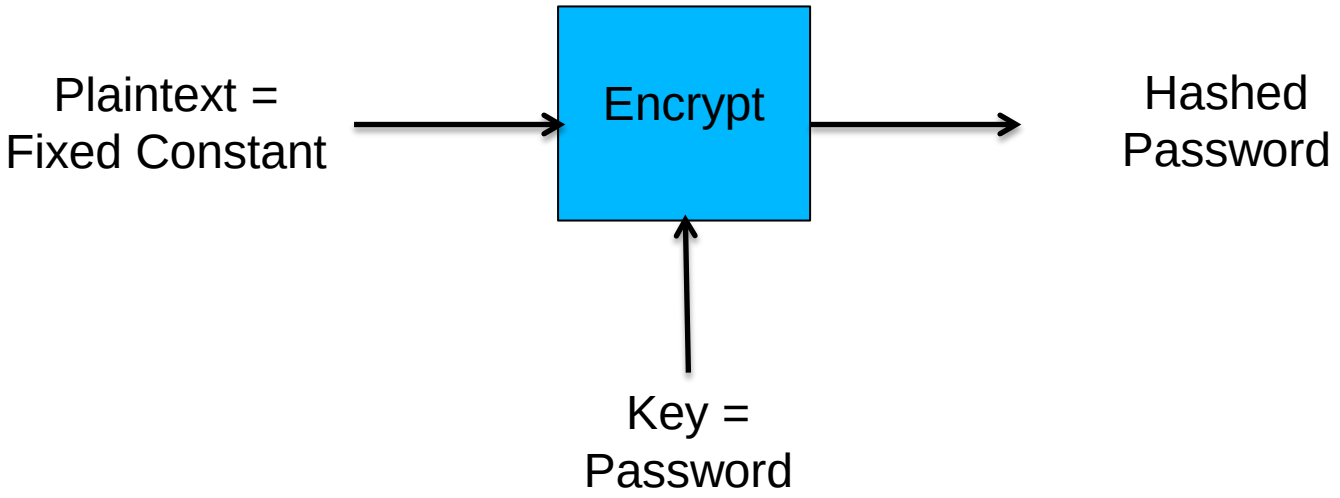
Herley-Oorschot Concluding Quote

- Although we lack the data to attach likelihoods to the individual pie-chart threats, we can reasonably conjecture that keystroke logging harvests more passwords than phishing and phishing harvests more than online brute-force attacks.

Morris-Thomson 1979

Evolution of UNIX password mechanism

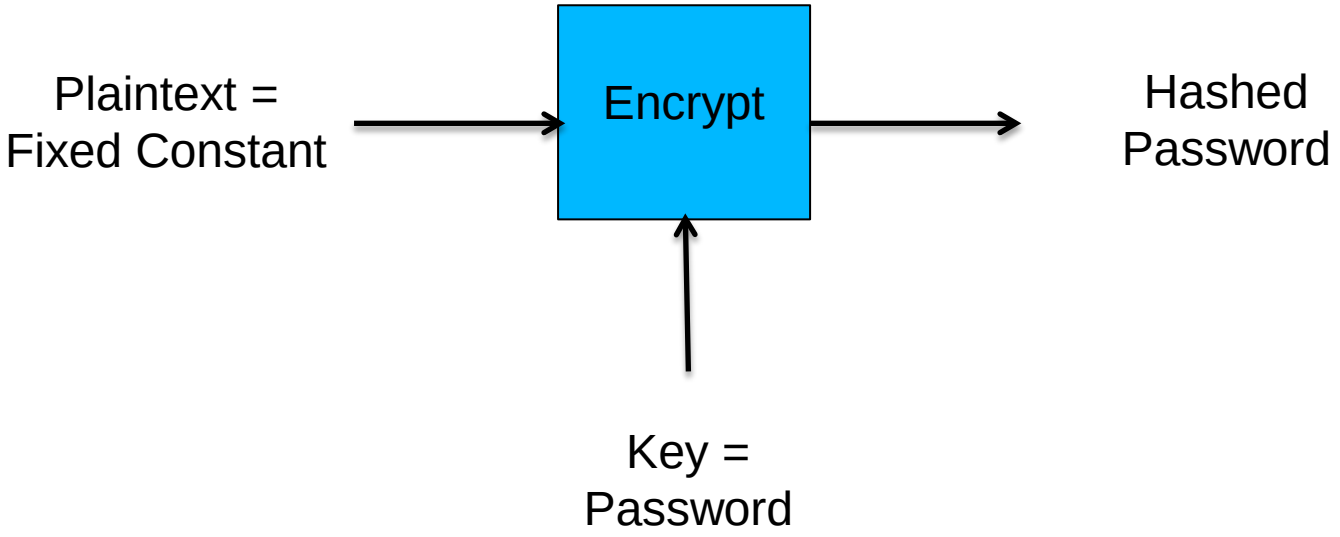
- Store passwords in a highly protected file
  - Single point of total failure
  - Easily copied by privileged users
  - Stored in plaintext on backups
  - Protection mechanisms are imperfect
- Store hashed passwords



Morris-Thomson 1979

Evolution of UNIX password mechanism

- Store hashed passwords



- Invention of dictionary attack rather than inversion attack
- In the initial enthusiasm hashed passwords were put in a world readable file!!

Cheswick 2013

- DoD Green Book requirement 1985:
  - The goal is to resist a year's worth of dictionary attacks with a cracking probability of 10^{-6} (or 10^{-20} for sensitive systems).
- Cheswick Table 2, page 42
  - Trying to meet this requirement by changing passwords regularly is rather hopeless

Narayanan-Shmatikov 2005

- "We demonstrate that as long as passwords remain human-memorable, they are vulnerable to "smart-dictionary" attacks even when the space of potential passwords is large."

- It's not just human-memorable it is also human-enterable.