User Authentication

Beyond Passwords (1)

Budi Arief

b.arief@kent.ac.uk

Based on slides by Shujun Li

Outline

- Recap and Context
  - Textual and Graphical Passwords
  - Usability Issues
- Knowledge-Based Authentication
- Password Recovery
- Beyond “What You Know”:
  - “What You Possess/Have”
- Summary

Recap and Context

University of Kent

- Textual passwords are still the dominant way of authenticating users
- However, (weak) textual passwords can be easily compromised
  - Various password cracking attacks
- Graphical passwords are mooted as a possible way to address this issue
  - They provide an alternative, but they have their own issues
- We looked at these issues in the last lecture

Outline

University of Kent

- Recap and Context
  - Textual and Graphical Passwords
  - Usability Issues
- Knowledge-Based Authentication
- Password Recovery
- Beyond “What You Know”:
  - “What You Possess/Have”
- Summary

Usability Issues

- Trade-off: memorability vs. security
  - Often users are forced to choose a password that is “strong” but difficult to memorise
- Question: what could be the consequences of enforcing a complicated password policy?

Usability Issues (contd.)

- Sometimes experts got it wrong too!

The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!

Bill Burr's 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error

By Robert McMillan

Aug. 7, 2017 12:41 p.m. ET

The man who wrote the book on password management has a confession to make: He blew it.

Back in 2003, as a midlevel manager at the National Institute of Standards and Technology, Bill Burr was the author of "NIST Special Publication 800-63. Appendix A." The 8-page primer advised people to protect their accounts by inventing awkward new words rife with obscure characters, capital letters and numbers—and to change them regularly.

Recommended Videos

1. Take a Tour of an Artist's Stunning New York Townhouse

2. What Latest Feuding Means for Trump and GOP

The Wall Street Journal: https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118

Outline

- Recap and Context
  - Textual and Graphical Passwords
  - Usability Issues
- Knowledge-Based Authentication
- Password Recovery
- Beyond “What You Know”:
  - “What You Possess/Have”
- Summary

Knowledge-Based Authentication

- There are ways (other than textual passwords) to authenticate users based on their knowledge
  - Keyboard patterns
  - Emojis
  - Other secrets
  - A real-world example: Pass∞

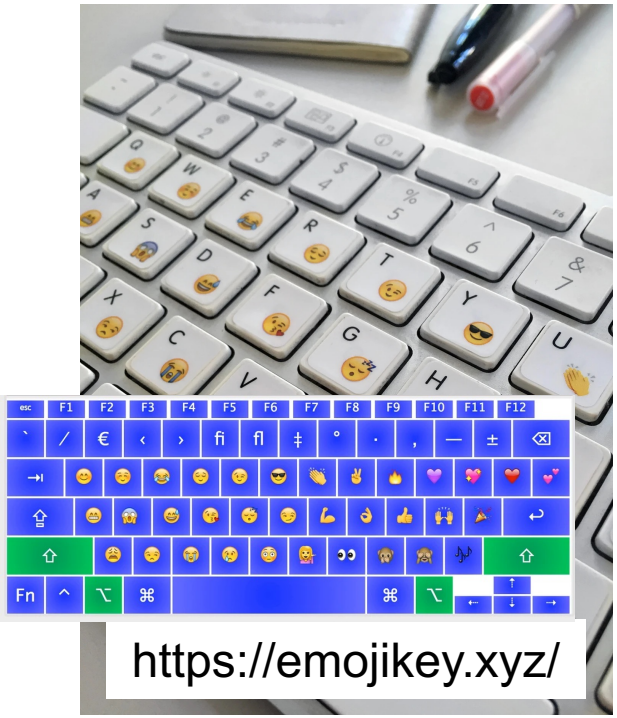
Passwords with keyboard patterns

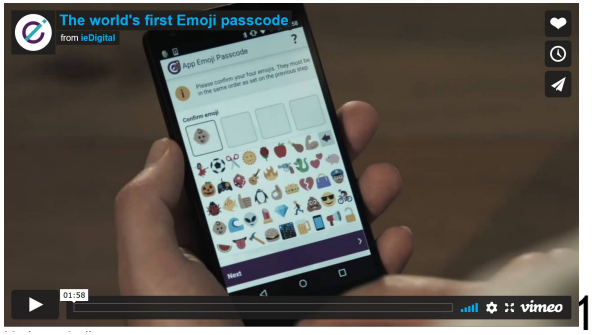
- Keyboards have a “graphical” pattern!
  - ⇒ You can draw your “password” (or part of it) on the keyboard!
  - What you remember: a graphical pattern (or part of it)
  - What the server receives: a normal-looking textual password
- Are they more secure?
  - You can still build a dictionary!
  - Most password cracking tools have considered such patterns!

- Dino Schweitzer, Jeff Boleng, Colin Hughes and Louis Murphy, “Visualizing Keyboard Pattern Passwords,” VizSec 2009, IEEE
- Makl Ndrix, "KeyWalking: pattern based passwords," blog article (GitHub)

Passwords with emojis

- Emoji keyboard stickers
  - Emoji stickers ⇒ Characters
  - What you remember: a list of emojis
  - What the server receives: a list of ASCII characters
- Directly typing emojis
  - Emoji keyboard layouts
  - What you remember: a list of emojis
  - What the server receives: a list of ASCII / Unicode characters or images
- Using special software
  - What you remember: a list of emojis
  - What the server receives: a list of ASCII / Unicode characters or images



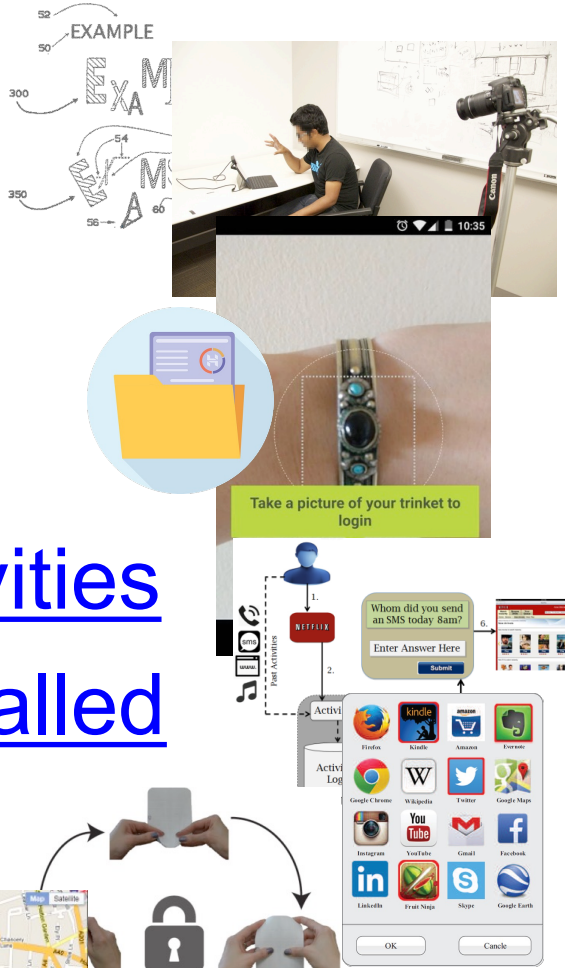


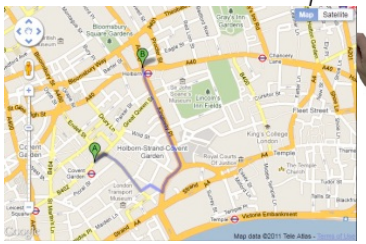
Much more secrets than textual (and graphical) passwords!

University of Kent

- Secret attributes of characters
- Secret gestures
- Secret music / songs
- Secret files / objects
- Secret knowledge of your activities
- Secret knowledge of apps installed
- How you interact with sensors
- Secret info on a map
- …

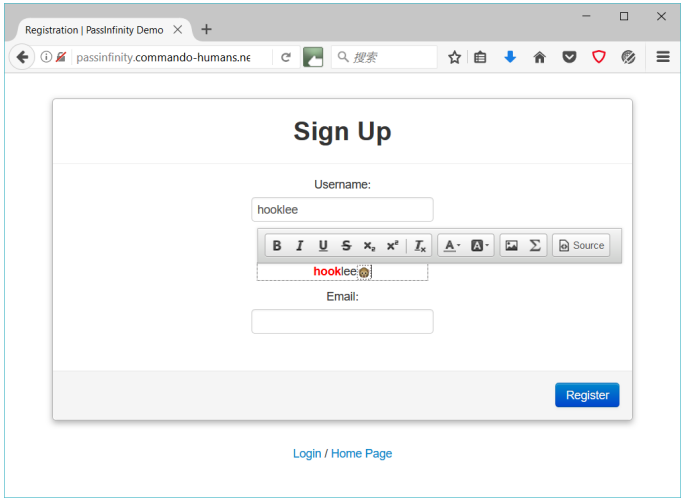
Click each of the blue links above for a research paper or a patent.



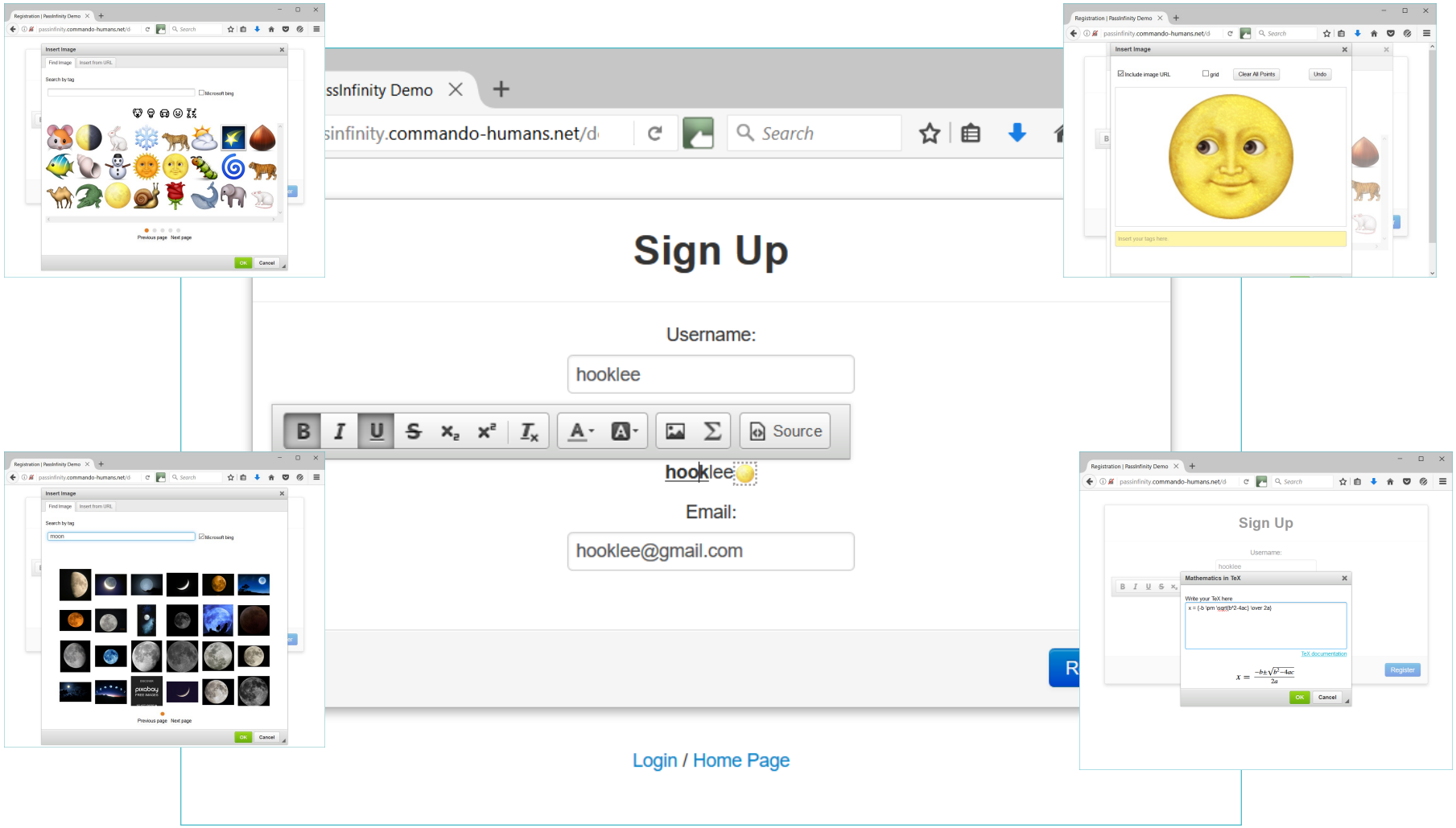


Passwords as anything or accessorising your passwords: Pass∞ (PassInfinity)

- A new technology proposed by Shujun Li and his former PhD student Nouf Aljaffan at the University of Surrey
- It allows **user-centric** combinations of **diverse authentication actions** (across **different factors**), while keeping **backward compatibility** with textual passwords
- Early work has been published as part of Nouf Aljaffan's PhD thesis and as a patent application



A web-based prototype of Pass∞

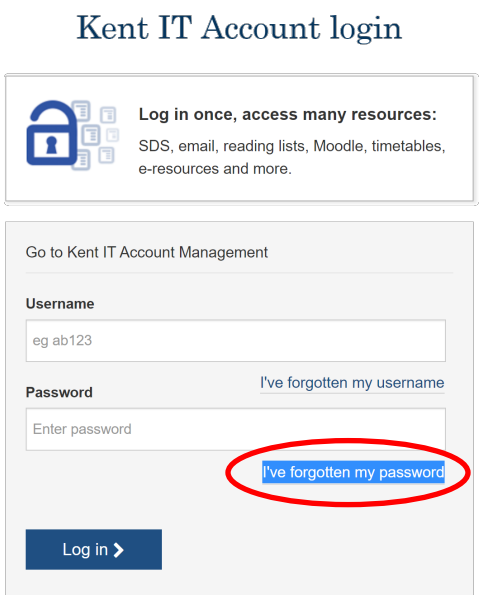


Outline

- Recap and Context
  - Textual and Graphical Passwords
  - Usability Issues
- Knowledge-Based Authentication
- Password Recovery
- Beyond “What You Know”:
  - “What You Possess/Have”
- Summary

Fallback/recovery/emergency authentication

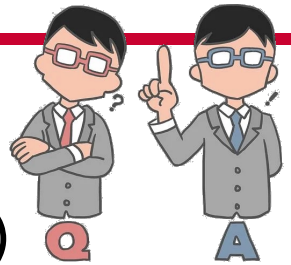
- What you know = What you (have to) remember
  - ⇒ You can forget it
  - ⇒ You will need a way to recover from forgetting it
  - ⇒ Password reset is necessary from time to time!
- Possible methods
  - Password reset via email
  - Secret questions and answers
  - Social authentication
    - Who you know
  - Physical authentication
    - Not always possible!



Password reset via email?

- Two common methods
  - Good: A password reset link sent to your registered email address
  - Bad (why?): Sent your password **in clear** to your registered email address
- What is it really about?
  - User authentication of a system ⇒ User authentication of your email system
  - ⇒ If someone hacks into your email, he/she can reset all your passwords of other systems!
  - ⇒ A single point of failure!

Secret questions and answers?



- Questions can be chosen by you.
  - Not part of the actual secret (shown to anyone!)
  - They can be chosen to make answers harder to guess
- Normally more than one question-answer pair
- Are they more secure than passwords?
  - It depends!

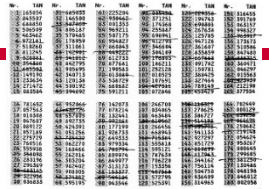
What is your pet's name?

- Can hashing and salting still be applied?
  - Yes for answers + No for questions (why no?)
- What user authentication factor?
  - What you know / What you (have to) remember!
  - $\Rightarrow$ A "password" to recover another "password"!

Outline

- Recap and Context
  - Textual and Graphical Passwords
  - Usability Issues
- Knowledge-Based Authentication
- Password Recovery
- Beyond “What You Know”:
  - “What You Possess/Have”
- Summary

What can you possess?



- Secret paper
- Smart cards (+ card reader)

- Connected security tokens
  - USB-based
  - Optical channel based

- Disconnected security tokens
  - One-time password generators
  - Transaction signers

- Mobile phones
  - Software versions of all the above

- …

How do they work?

- One-time passwords
  - Printed on a piece of paper (often with an index for each password)
  - Generated by a dedicated hardware device
  - Generated by a mobile app

- Digital certificates (for end users)
  - Stored on a USB key or the user's mobile phone (normally protected by a password!)
- Challenge-response protocols
  - A dedicated security device (the prover) responds to a challenge from the server (the verifier)
  - Advanced crypto (e.g., digital signature) is normally used
- Industrial standards
  - Universal 2nd Factor (U2F) by FIDO Alliance
  - …

Drawbacks of security tokens

- Usability issues
  - You need to bring it with you!
  - Additional costs (especially if you need to have many!)
- Loss and theft
  - Normally require a PIN to protect against such issues
  - ⇒ **Security reduced to the first authentication factor ("what you know")!**
- Man-in-the-middle attacks
  - Some security tokens are insecure against such attacks
- Insecure implementations
  - Predictable pseudo-randomness
  - Extraction of secret keys
  - Insecure mobile phones (e.g., mobile malware)
  - …

Outline

- Recap and Context
  - Textual and Graphical Passwords
  - Usability Issues
- Knowledge-Based Authentication
- Password Recovery
- Beyond “What You Know”:
  - “What You Possess/Have”
- Summary

Summary

- There are usability and security issues with textual and graphical passwords for authenticating users
- Researchers have been looking for ways to deal with these issues, for example:
  - Knowledge based password
  - Password reset
  - Other factors of “What You Know”, e.g., secret questions
  - Using “What You Have”, e.g., OTP, tokens, phone-based
- Next lecture:
  - We will continue with “Who You Are”, i.e., biometrics