INFOSECURITY
WITH
PLYMOUTH
UNIVERSITY

INFOSECURITY
WITH
PLYMOUTH
UNIVERSITY

FROM PASSWORDS TO BIOMETRICS
IN PURSUIT OF A PANACEA

Prof. Steven Furnell
Centre for Security, Communications & Network Research
Plymouth University
United Kingdom

Session Content

Scene setting

Traditional Passwords

The rise of alternative approaches

Active authentication (and beyond)

Conclusions

Introduction

- User authentication traditionally dominated by traditional PINs and passwords
  - Tokens and biometrics tended to remain the preserve of larger organisations
- Today's situation is rather more diverse
  - Lay users are far more likely to encounter things beyond the traditional secrets
  - Alternative and multi-factor approaches may now have been directly *experienced* rather than just heard about

Driving the change

- The increased security needs of certain online services, raising user expectations to see protection beyond the baseline
  - e.g. Internet banking
- The new opportunities afforded by our devices
  - e.g. touchscreens allow gesture-based secrets, while other sensors allow biometric inputs

Introducing Passwords!

- An aspect of security that we all tend to encounter
- Traditional methods are often regarded as very usable
  - Easy to understand the idea
  - Familiar across different systems
  - high degree of cross-device applicability
  - Perceived to be low cost
- Ease of use is often because users have not been made to use them properly

Authentication evolved?

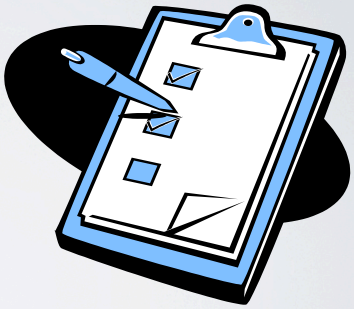
- For all the concerns over passwords, little has happened
  - all that has changed is what we are typing them on!
- Advanced technology but age-old methods

Usability challenges

- Practically every aspect of good password practice makes them more difficult to use
  - Enforcing selection criteria (length and character composition)
  - Changing them regularly
  - Avoiding password reuse
  - Avoiding a written record
- The need to use passwords across multiple systems amplifies the challenge
- Password management tools overcome some of the constraints but complicate the process of retrieving and using the passwords

Security amongst today's users

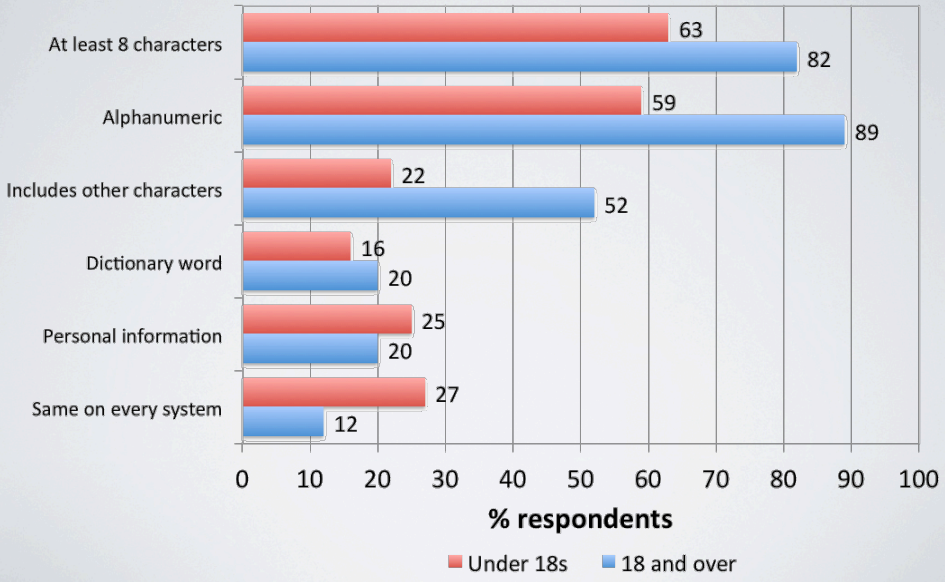
- Surveyed the behaviours of over 400 UK respondents
  - 290 respondents aged 18 and over
  - 129 respondents under 18
  - broad contrast to be drawn between those currently in the workplace and those in the next generation



Password Usage

Number of password-protected systems or devices	Under 18s	18 and over
1-5	38%	10%
6-10	35%	32%
11-15	15%	23%
16+	12%	36%

Password Practices



Predictably Popular

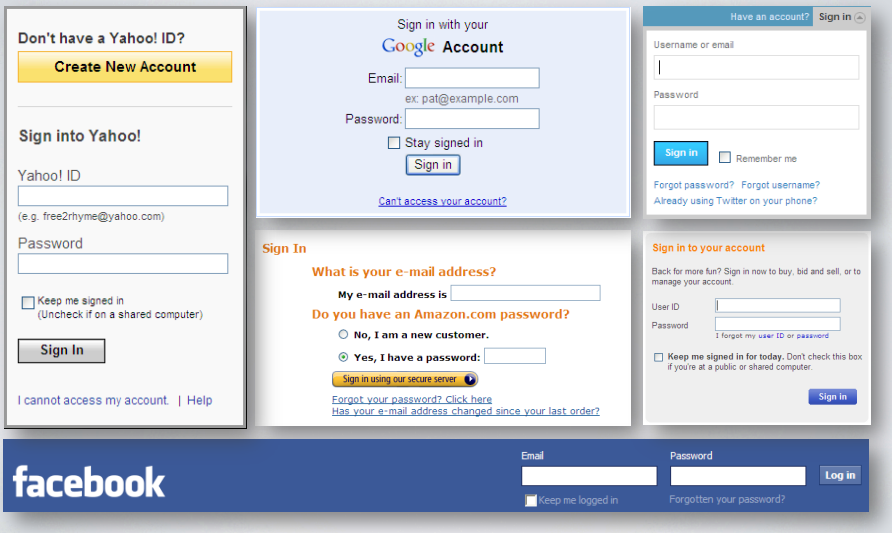
	2011	2012	2013	2014
1	password	password	123456	123456
2	123456	123456	password	password
3	12345678	12345678	12345678	12345
4	qwerty	abc123	qwerty	12345678
5	abc123	qwerty	abc123	qwerty
6	monkey	monkey	123456789	123456789
7	1234567	letmein	111111	1234
8	letmein	dragon	1234567	baseball
9	trustno1	111111	iloveyou	dragon
10	dragon	baseball	adobe123	football

Source: SplashData

From EU H2020 Digital Security Work Programme

- **DS-2-2014: Access Control**
- Specific challenge: Security includes granting access only to the people that are entitled to it. Currently the most widespread approach relies on passwords. Managing the passwords has its limits and poses a challenge to the user, which adds vulnerabilities. Common practice is to use the same or similar password, which increases significantly the risk should the password be broken.

Website Passwords



An analysis of website password practices

- Examination of ten leading websites
  - Selected from within the top 25 entries in the Alexa Global Top 500 websites in August 2014
  - represent popular online services used by the general public, rather than targeting a technical audience
- Captures a number of the leading and most recognised online brands
  - password practices likely to influence the largest proportion of end-users
  - potentially used as a baseline to be followed by other sites

Provision of password guidance

Site	Guidance Provided?		
	Sign-up	Password Change	Password Reset
Amazon	×	×	✓
Facebook	×	×	✓
Google	✓	✓	✓
LinkedIn	×	✓	✓
Microsoft Live	×	×	×
Pinterest	×	×	×
Twitter	×	×	✓
Wikipedia	×	×	×
WordPress	✓	×	✓
Yahoo!	×	×	×

Enforcement of password restrictions

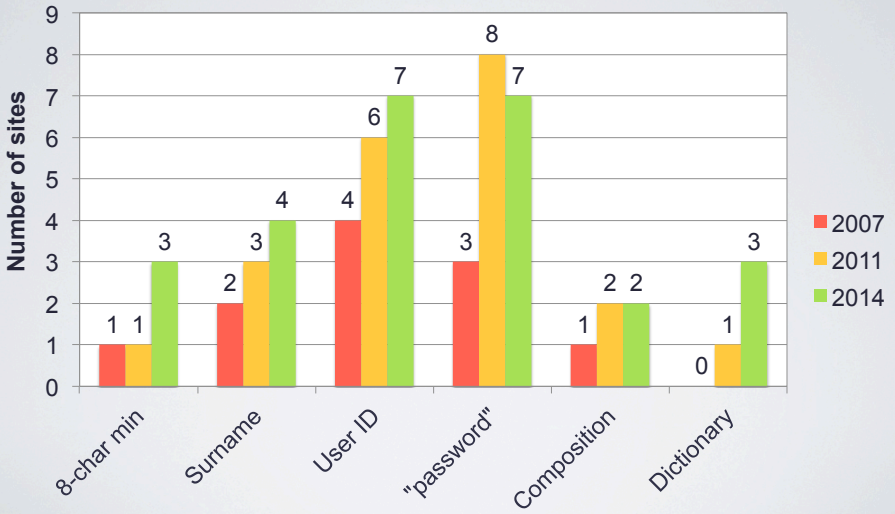
(at initial registration to website)

Site	Restrictions at sign-up						Other support		
	Length	Surname	User ID	Password	Compo-sition	Dictionary	Meter	Extra prot.	Prevents reuse
Amazon	6	×	×	×	×	×	×	×	×
Facebook	6	✓	×	×	×	×	Ratings	✓	×
Google	8	✓	✓	✓	×	✓	✓	✓	✓
LinkedIn	6	×	×	✓	×	~	×	×	×
Microsoft Live	8	✓	✓	✓	✓	×	×	✓	✓
Pinterest	6	×	✓	✓	×	×	×	×	✓
Twitter	6	×	✓	✓	×	~	✓	✓	×
Wikipedia	×	×	✓	×	×	×	×	×	×
WordPress	6	×	✓	✓	~	✓	×	×	✓
Yahoo!	8	✓	✓	✓	✓	✓	×	×	✓

Observations

- Password length enforcement was variable
  - Most enforced a minimum of 6 characters (Google, Microsoft and Yahoo! were 8)
  - Some sites enforced a maximum length (e.g. 32 for Yahoo!)
  - Wikipedia allowed a 1 character password
- Other viable checks were often excluded
  - Although some sites did *inform*, they did not *enforce*
- Some sites might argue that the checks are commensurate with the data at risk
  - Overlooks the potential for users to use the same password elsewhere
  - Better to help contribute towards raising the general security culture

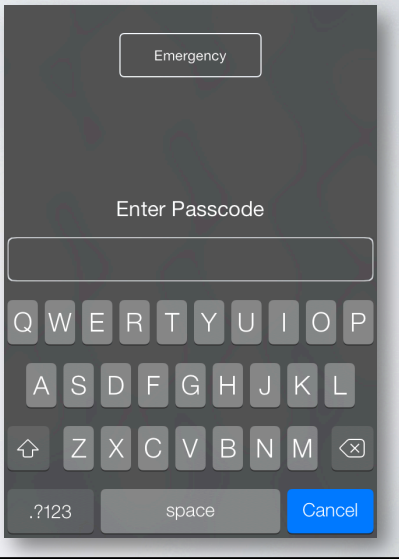
Evolving Enforcement



Evolving Enforcement

Site	Year	Restrictions at sign-up					
		Length	Surname	User ID	Password	Compo-sition	Dictionary
Amazon	2007	×	×	×	×	×	×
	2014	6	×	×	×	×	×
Facebook	2007	6	✓	×	✓	×	×
	2014	6	✓	×	×	×	×
Google	2007	8	×	✓	✓	×	×
	2014	8	✓	✓	✓	×	✓
Microsoft Live	2007	6	×	✓	×	×	×
	2014	8	✓	✓	✓	✓	×
Yahoo!	2007	6	×	✓	×	×	×
	2014	8	✓	✓	✓	✓	✓

Authentication
The traditional options



Protected or Neglected?
Smartphone Authentication

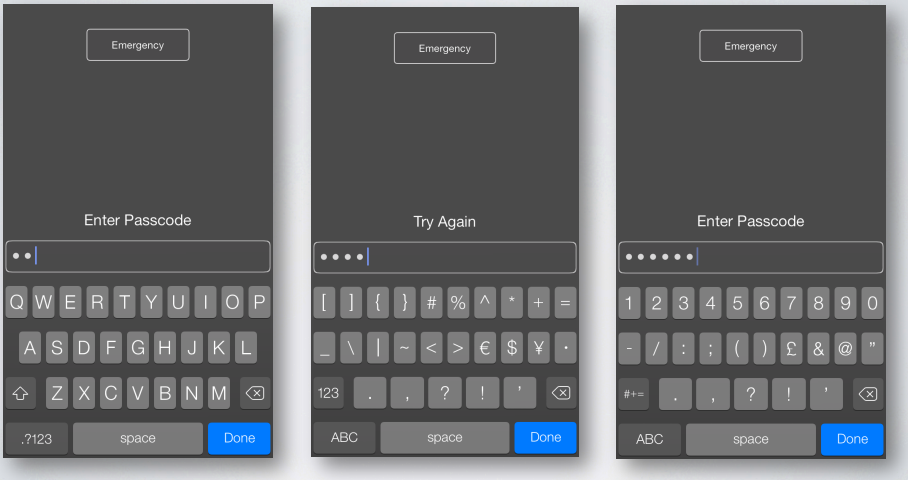
Authentication method	Respondents
PIN	47%
Password	23%
Pattern Lock	28%
None	17%

From 290 users surveyed
by Plymouth University in Sept/Oct 2013

The usability challenge

- Entering standard passwords on mobile devices can be awkward
- Time-consuming for a device that is frequently in and out of use for short bursts
- Awkward to enter, particularly if you use multiple character types
  - Let's see the effort to enter an 8 character string with letters, numbers and symbols on an iPhone …

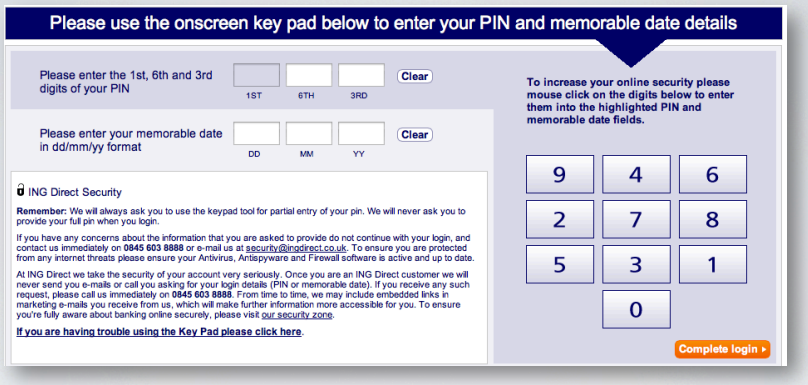
The challenge of entering Pa$$C0de



The compromise?

Ease of use at the expense of security

Online Banking



- Identification and authentication demands:
  - A personal banking number
  - Customer surname
  - Selected digits from security number
  - A memorable date

Challenging the legitimate user?

- More time-consuming and require more cognitive effort than passwords:
  - the authentication challenge will not be the same each time (i.e. different digits requested)
  - the user can no longer rely on reflex response of typing a normal PIN/password
  - the digits of the PIN are not requested in sequential order
  - the position of the digits on the graphical keypad varies on each occasion

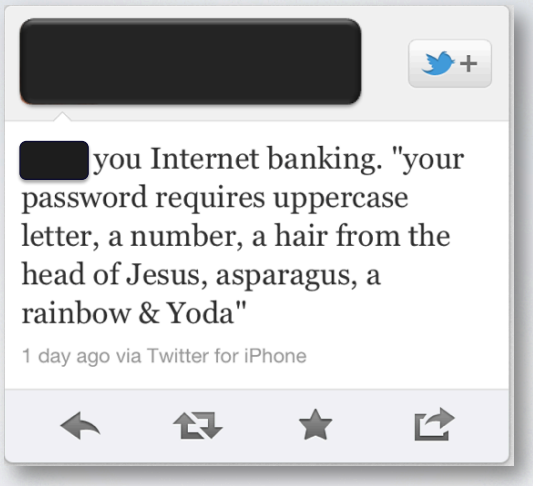
Online Banking

- HSBC Secure Key introduces a multi-stage process for each login:
  - User needs to enter their Banking ID
  - Then answer a security question defined when they set up the account
  - Then enter a 4-digit PIN code on the Secure Key device
  - Then enter the 6-digit code generated by the device into the web page

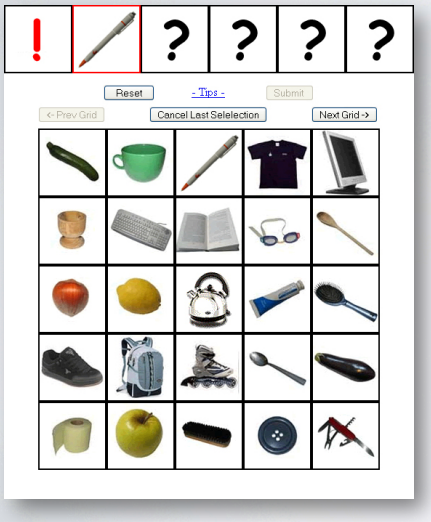
Acceptable trade-off?

- Users may not object in a banking context
  - they realise their money is at stake
- Such approaches would not work for website authentication in general
  - would not scale up well as having a variety of numbers to remember for different accounts would quickly become unmanageable for the user

The user's viewpoint?

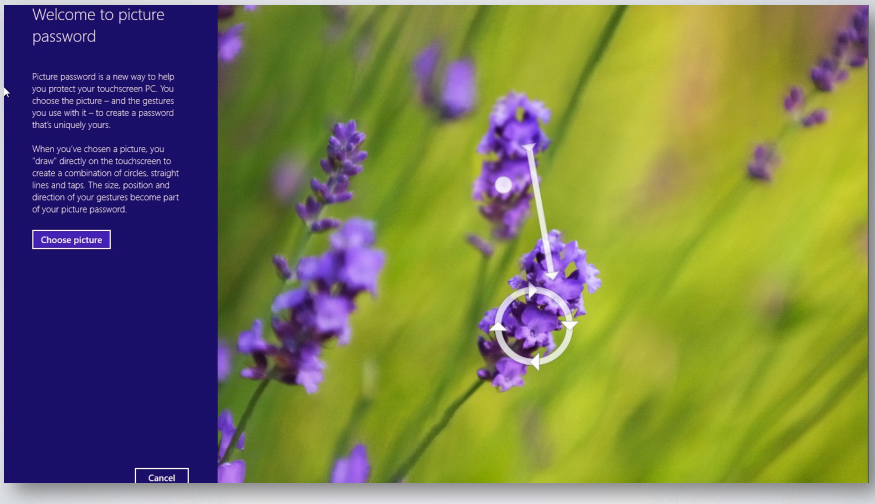


Alternative Secrets



- Alternatives based around graphical secrets
  - potentially easier to remember due to visual characteristics
- Plymouth studies include:
  - recall of everyday objects
  - combination with secret hotspots within images
- Some positive findings, but acceptance is not universal
  - still a PoE-only mechanism

Windows 8 Picture Password



Android Pattern Unlock

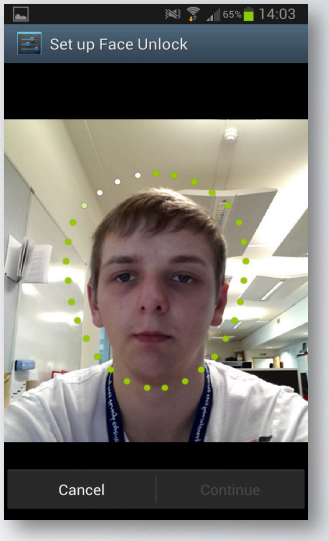
- Clearly suited to touch screen devices
- Complex patterns hard to remember?
- More observable than PINs
- Potential clues from greasy fingers
  - choose patterns that double-back …
  - … or clean the screen!

Trading security for usability?

- Both of the leading smartphone platforms now offer biometric alternatives to traditional PINs or passwords
  - Android has Face Unlock (2011)
  - iOS has Touch ID (2013)
- Having alternatives may be potentially valuable for mobile/pocket devices:
  - many users don't enable traditional techniques as they are too inconvenient
  - frequent, 'short burst' uses of the device can make PINs and passwords awkward in practice

Biometric options
Android Face Unlock

- Unlocks the phone in response to seeing the correct face
- Very quick and easy under the right conditions

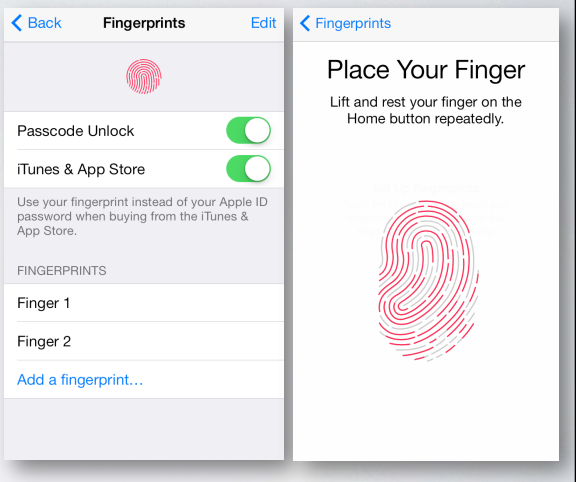


Biometric options
iOS Touch ID

- Introduces an RF-Capacitive Sensor into the Home Button
- Capacitive sensor is activated by the slight electrical charge that runs through the skin
  - means that a dead finger will not work

Biometric options
iOS Touch ID

- Can be used to unlock the device and confirm iTunes purchases
- The user can register up to five fingers
  - either all their own or also other users that they may wish to grant access to



The rationale for Biometrics
Usability over Security?

"You check your iPhone dozens and dozens of times a day, probably more. Entering a passcode each time just slows you down"

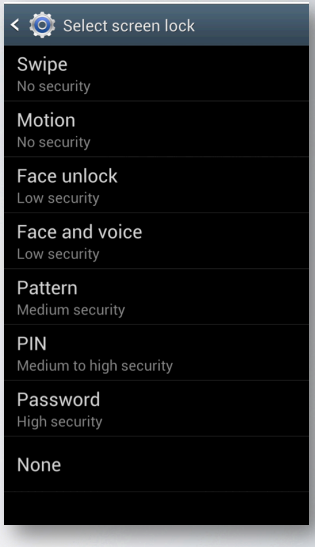
From Apple's promotional text for Touch ID

"making each person's device even more personal"

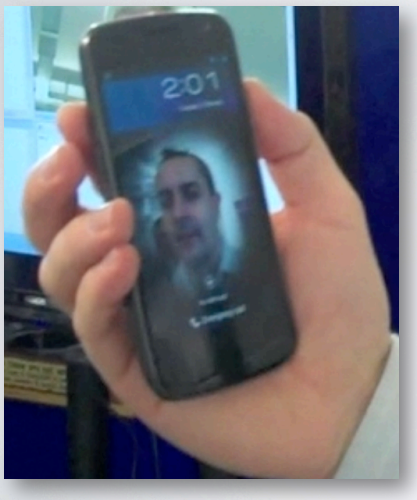
The advertising of Android Face Unlock

Ranking the protection

- Face Unlock is ranked as the *least* secure of the available options
  - the description explicitly cites it as *less* secure than any of the secret-based approaches (i.e. pattern, PIN or password)



Facial Flaws?



- Not a universal solution
  - reverts to PIN/password entry in low light conditions
- Questionable security
  - original version could be fooled by static photo of the legitimate user
  - limited Liveness detection (blink checking) introduced in mid-2012, but can still be fooled by edited photo

Fingerprint Fallbacks

Initial failure allows further attempts

After third consecutive failure, reverts to Passcode interface

Passcode required after five consecutive failures

The Primacy of the Passcode

- Users cannot actually use Touch ID without having set a passcode beforehand
- The passcode is also needed if:
  - the user wishes to change any of the authentication settings
  - the handset is fully reset
  - more than 48 hours have passed since the device was last unlocked
- Then relying upon a passcode that is less frequently used
  - arguably less likely to be remembered without being written down

Not always usable …

- There are some circumstances in which Touch ID stops working
- Notable cases:
  - Moisture
    - Sweaty hands
    - Rain!
  - Dirty fingers
  - Gloves
  - Skin damage
    - e.g. my wife's thumb

Not always usable …

- There are some circumstances in which Touch ID stops working
- Notable cases:
  - Moisture
    - Sweaty hands
    - Rain!
  - Dirty fingers
  - Gloves
  - Skin damage
    - e.g. my wife's thumb

One size fits all?

- Traditional authentication tends to deliver full access in one go
  - secondary authentication sometimes required for specific applications or services
- Potentially desirable to differentiate the requirement based upon the nature of the device/system, data, or level of access concerned but to manage it *transparently* wherever possible

Transparent, Non-intrusive authentication

- Relevant to consider how to bring authentication strength and convenience together in a more effective manner
- Non-intrusive methods aim to maintain tolerability while offering opportunity beyond Point of Entry
  - ability to obtain a continuous (or periodic) measure of authentication
  - leveraging natural user interactions as a basis for collecting authentication data

Active Authentication

- “The current standard method for validating a user’s identity for authentication on an information system requires humans to do something that is inherently unnatural: create, remember, and manage long, complex passwords”
- “The Active Authentication program seeks to address this problem by developing novel ways of validating the identity of the person at the console that focus on the unique aspects of the individual through the use of software based biometrics ... This program focuses on the behavioral traits that can be observed through how we interact with the world.”

(DARPA, January 2012)

Requirements

- Reduce the authentication burden upon the user
- Improve the level of security being provided
- More closely link authentication of the user with the subsequent request for access
- Ensure that the approach is commensurate with the needs of the access request
- Provide a more effective measure of identity confidence that goes beyond a simple Boolean decision

Non-intrusive mobile authentication

Signature Recognition

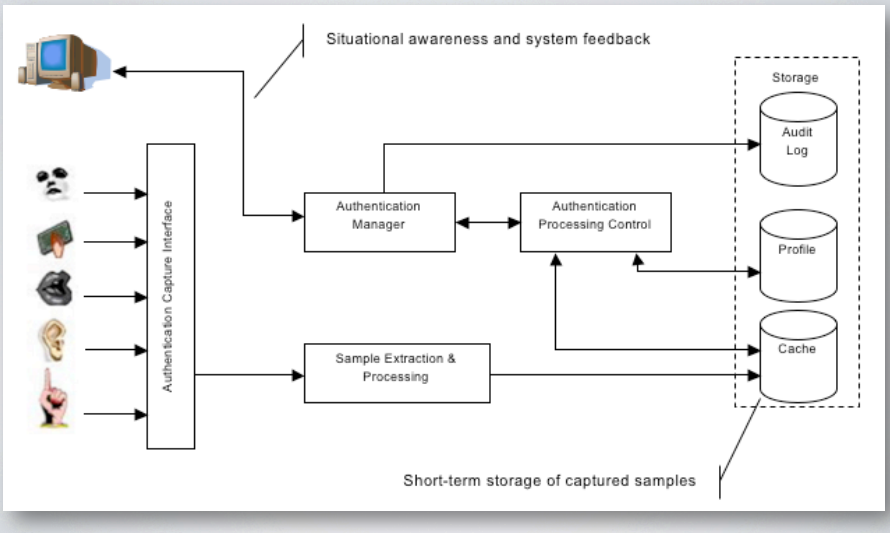
Service Utilisation

Voice Verification

Facial Recognition

Keystroke Dynamics

A generic transparent authentication framework



Framework Components

- Five key elements:
  - Capture of authentication samples
  - Processing of authentication samples
  - Short- and long-term data repositories
  - Authentication Manager
  - Response
- Enables continuous transparent capture of authentication samples by the underlying system

Authentication Aura

- Improving the experience for multi-device users
  - recent authentication on one personal device reduces the need for explicit authentication on other devices in close proximity
- Aura level affected by strength of authentication method and how recent
  - can be maintained by non-intrusive monitoring and boosted by further explicit authentication actions
  - dissipates over time without further authentications
- Devices (and data) accessible based upon their sensitivity and current Aura level

Authentication Aura

John authenticates himself using pattern unlock on his tablet

Authentication Aura

Establishes a resulting Authentication Aura of a certain level

Authentication Aura

John is in close physical proximity to several other of his devices

Authentication Aura

Medium value asset (Partial access)

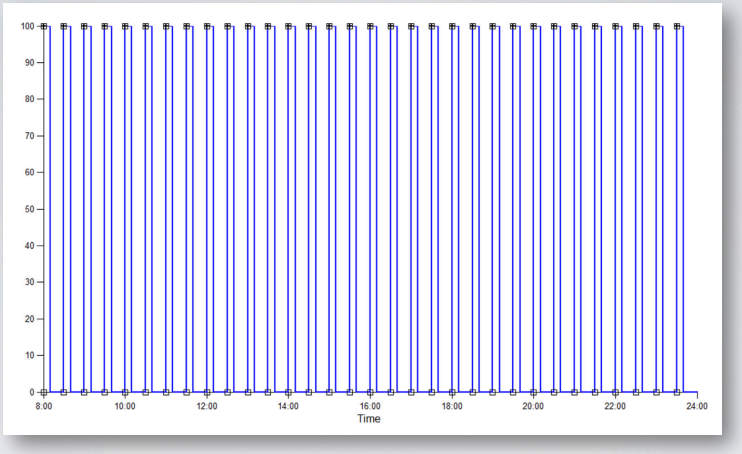
High value asset (Aura not strong enough, No access)

Low value asset (Full access)

The strength of his Aura permits access to some devices but not others

Simulating the Aura effect

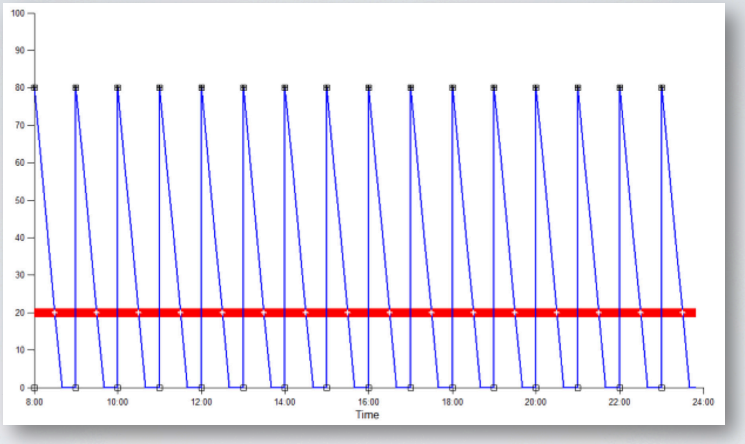
Reference scenario – A day in the life …



Plot of the ‘Authentication confidence’ on a device used every 30 mins, with 10-min inactivity lock

Simulating the Aura effect

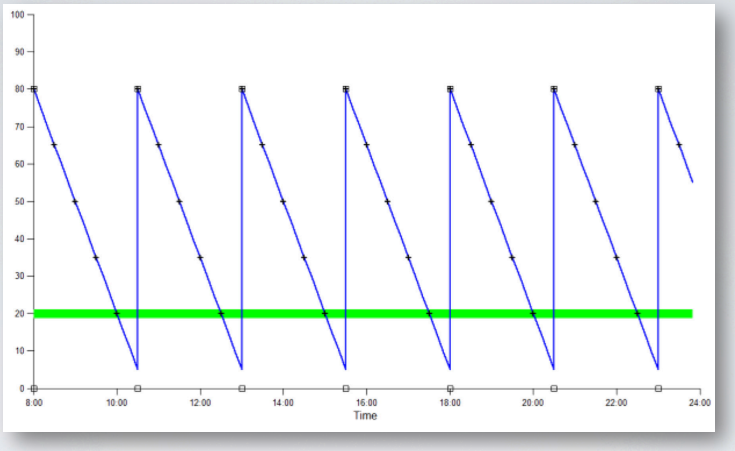
Progressive reduction of confidence



Confidence degrades over time, until a fresh authentication occurs

Simulating the Aura effect

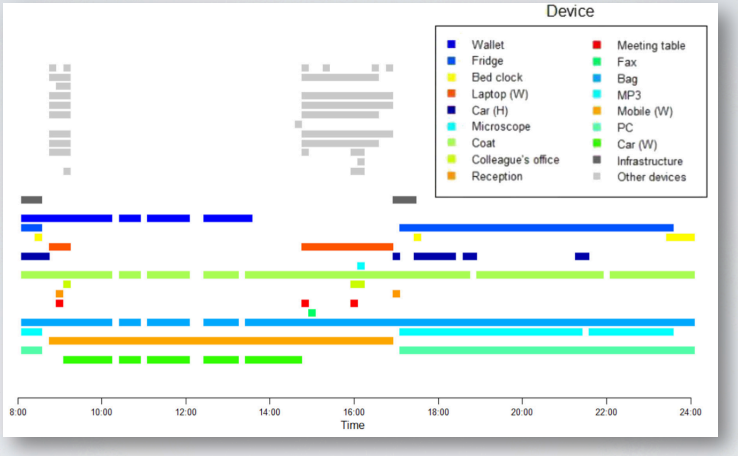
Progressive reduction of confidence



May configure to degrade less quickly in a familiar physical environment (e.g. at home)

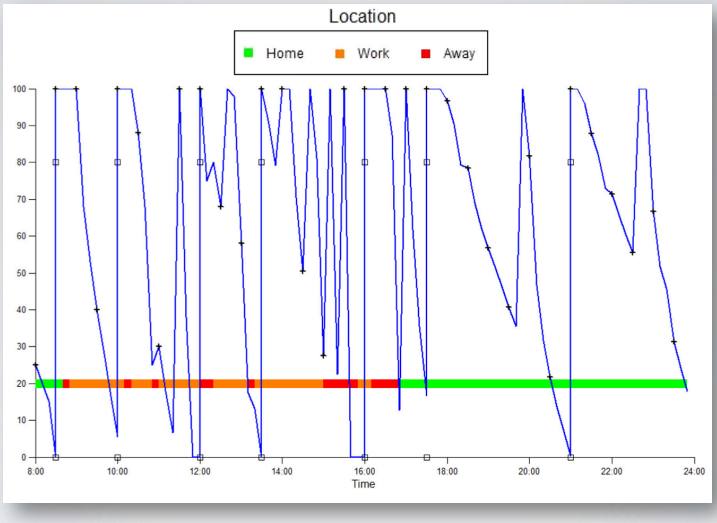
Simulating the Aura effect

Tracking device location and things around it



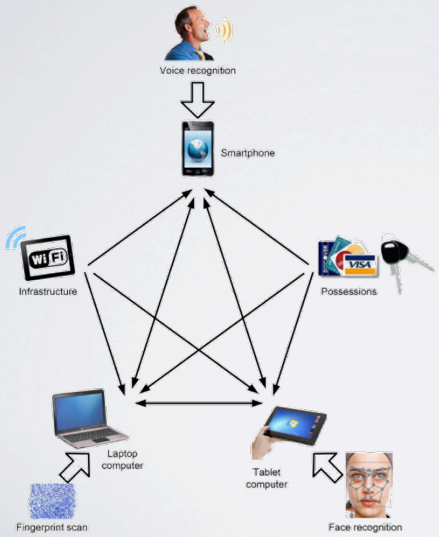
Actual device observations from one of our 20 trialists during one of their days

Simulating the Aura effect



Using other devices and location to affect the level

Authentication Aura Overall Results



20 participants for 14-days each

Each user RFID tagged 15 objects within home and work environments

Simulation based upon 1.23 million samples suggest a 75% reduction in explicit authentication requests

Conclusions

Conclusions

- The range of authentication options has grown
  - still no single solution that us universally applicable and effective
- Predictions:
  - passwords will be with us for some time yet
  - other approaches (particularly biometrics) will become more commonplace

Conclusions

- Passwords are familiar but nonetheless not used effectively
  - show no immediate signs of going away
  - required in more and more IT contexts, often without sufficient guidance
- The managability problem remains, but this exists in different forms for other secrets and for tokens
  - Biometrics introduce their own concerns

Conclusions

- Taking authentication beyond traditional methods and beyond PoE has usability benefits
- Use of a composite approach within an intelligent framework can strengthen protection
- Ongoing research is tackling the approach to authentication transparency within and between devices

Related Reading

"Co-operative user identity verification using an Authentication Aura"

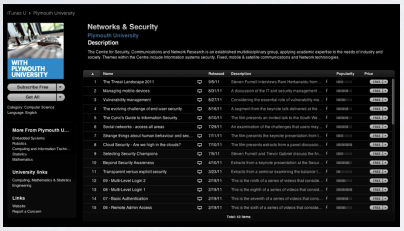
C.Hocking, S.Furnell, N.Clarke and P.Reynolds

Computers & Security

Vol. 39 (2013), pp486-502

Security Podcasts on iTunes U

LECTURES, DISCUSSIONS, INTERVIEWS, TUTORIALS, INDUSTRY INSIGHTS ...



www.cscan.org/podcasts

INFOSECURITY WITH PLYMOUTH UNIVERSITY

Prof. Steven Furnell
sfurnell@plymouth.ac.uk
@smfurnell

Centre for Security, Communications & Network Research
www.plymouth.ac.uk/cscan