Welcome to the NHS Identity and Access Management Summit!

9th October 2024
15 Hatfields Conference Centre,
London SE1 8DJ

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Chair Opening Address

Bharat Thakrar
CISO - CyberBTX

Keynote Presentation

Steven Furnell
Professor of Cyber Security
University of Nottingham

University of Nottingham
UK | CHINA | MALAYSIA

User authentication and access

Supporting staff to succeed?

Prof. Steven Furnell

School of Computer Science

Introduction

- User authentication is the frontline face of cyber security for millions of users
  - we all have to identify and authenticate ourselves somewhere
- Has become progressively more significant as there is more we want and need to protect
  - applies more often and to an ever-widening range of participants
- Mechanisms available to us have not necessarily evolved to keep pace

Authentication everywhere

- Multiple devices
  - e.g. we routinely authenticate ourselves on desktops, laptops, phones, tablets, etc
- Multiple services
  - e.g. applications and online services require us to have accounts
- Greater threats to identity
  - as online identity grows in value more must be done to safeguard it

The burden of proof?

- IAM starts with having to prove to the computer what we already know – i.e. who we are
  - I'm always sure that I am me - what varies is what I'm willing and able to do to prove it
- What will users tolerate?
  - depends upon the device, the context and what they are trying to protect
  - e.g. in time-pressured and urgent situations
- Same security, varying context
  - relatively easy to type a strong password when sat at a desktop or laptop PC
  - harder to do it when travelling with a phone

Inconsistent identity?

- In many cases, we lack facilities to support anything beyond password/PIN approaches
- Potential for significant variation
  - some service providers make specific provision for stronger approaches
  - some sites persist with basic and poorly considered approaches, which do not promote or reinforce good practice
- We end up encountering fundamentally different requirements:
  - our identity is validated to different degrees, but often links back to the same types of access and sensitive information

Preventing progress?

- Going beyond basic passwords requires additional technologies
  - biometrics
  - tokens
  - (authenticator apps)
- Needs the service to support and/or supply them
  - even then some technologies will not work on all devices
- Upshot is that we have generally relied upon methods that only need a keyboard

NHS - A Naturally Helpful Situation?

- The NHS context should work to the *advantage* of security
- Less need to convince of users of the *need* for authentication
  - they recognise sensitivity of data and the requirement to protect it etc
- Cyber security more generally aligns with the duty of care

Getting the basics right?

- Despite various alternatives and enhancements, our authentication experience is still dominated by passwords
- Despite being around for decades, we still haven't mastered it and passwords are still used badly
- The blame is commonly laid at users
  - but perhaps some responsibility perhaps rests with those requiring passwords to be used

Can you spot your password?

	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
1	123456	123456	123456	123456	123456	123456	123456	123456	123456	password	123456
2	password	password	password	password	password	password	123456789	123456789	123456789	123456	admin
3	12345678	12345	12345678	12345	12345678	123456789	qwerty	picture1	12345	123456789	12345678
4	qwerty	12345678	qwerty	12345678	qwerty	12345678	password	password	qwerty	guest	123456789
5	abc123	qwerty	12345	football	12345	12345	1234567	12345678	password	qwerty	1234
6	123456789	123456789	123456789	qwerty	123456789	111111	12345678	111111	12345678	12345678	12345
7	111111	1234	football	1234567890	letmein	1234567	12345	123123	111111	111111	password
8	1234567	baseball	1234	1234567	1234567	sunshine	iloveyou	12345	123123	12345	123
9	iloveyou	dragon	1234567	princess	football	qwerty	111111	1234567890	1234567890	col123456	Aa123456
10	adobe123	football	baseball	1234	iloveyou	iloveyou	123123	senha	1234567	123123	1234567890

(Sources: SplashData 2013-19; NordPass 2020-23)

So, let's vote … why do poor passwords persist?

- Is it because:

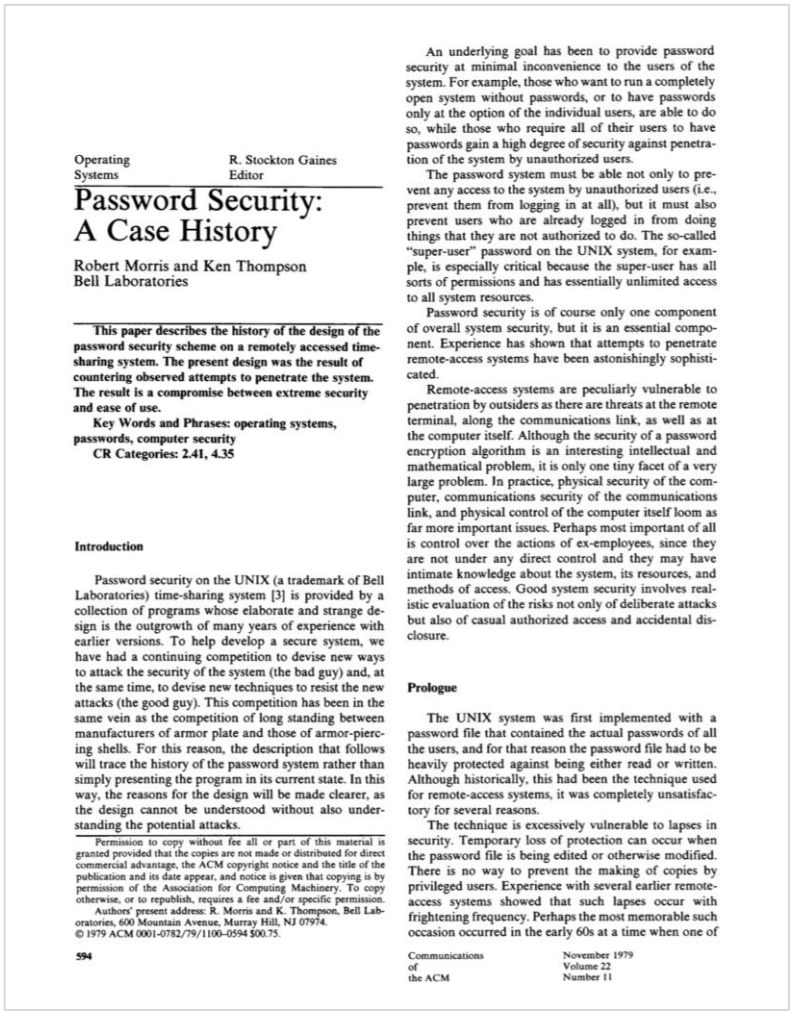
(a) People are stupid

(b) Passwords are flawed

(c) We allow them to be chosen

'123456' was the most common choice for 10 of the last 11 years … *perhaps* we could block it?

Not a new issue …



Operating Systems — R. Stockton Gaines, Editor

Password Security: A Case History

Robert Morris and Ken Thompson
Bell Laboratories

This paper describes the history of the design of the password security scheme on a remotely accessed time-sharing system. The present design was the result of countering observed attempts to penetrate the system. The result is a compromise between extreme security and ease of use.

Key Words and Phrases: operating systems, passwords, computer security
CR Categories: 2.41, 4.35

Introduction

Password security on the UNIX (a trademark of Bell Laboratories) time-sharing system [3] is provided by a collection of programs whose elaborate and strange design is the outgrowth of many years of experience with earlier versions. To help develop a secure system, we have had a continuing competition to devise new ways to attack the security of the system (the bad guy) and, at the same time, to devise new techniques to resist the new attacks (the good guy). This competition has been in the same vein as the competition of long standing between manufacturers of armor plate and those of armor-piercing shells. For this reason, the description that follows will trace the history of the password system rather than simply presenting the program in its current state. In this way, the reasons for the design will be made clearer, as the design cannot be understood without also understanding the potential attacks.

Authors' present address: R. Morris and K. Thompson, Bell Laboratories, 600 Mountain Avenue, Murray Hill, NJ 07974.

An underlying goal has been to provide password security at minimal inconvenience to the users of the system. For example, those who want to run a completely open system without passwords, or to have passwords only at the option of the individual users, are able to do so, while those who require all of their users to have passwords gain a high degree of security against penetration of the system by unauthorized users.

The password system must be able not only to prevent any access to the system by unauthorized users (i.e., prevent them from logging in at all), but it must also prevent users who are already logged in from doing things that they are not authorized to do. The so-called "super-user" password on the UNIX system, for example, is especially critical because the super-user has all sorts of permissions and has essentially unlimited access to all system resources.

Password security is of course only one component of overall system security, but it is an essential component. Experience has shown that attempts to penetrate remote-access systems have been astonishingly sophisticated.

Remote-access systems are peculiarly vulnerable to penetration by outsiders as there are threats at the remote terminal, along the communications link, as well as at the computer itself. Although the security of a password encryption algorithm is an interesting intellectual and mathematical problem, it is only one tiny facet of a very large problem. In practice, physical security of the computer, communications security of the communications link, and physical control of the computer itself loom as far more important issues. Perhaps most important of all is control over the actions of ex-employees, since they are not under any direct control and they may have intimate knowledge about the system, its resources, and methods of access. Good system security involves realistic evaluation of the risks not only of deliberate attacks but also of casual authorized access and accidental disclosure.

Prologue

The UNIX system was first implemented with a password file that contained the actual passwords of all the users, and for that reason the password file had to be heavily protected against being either read or written. Although historically, this had been the technique used for remote-access systems, it was completely unsatisfactory for several reasons.

The technique is excessively vulnerable to lapses in security. Temporary loss of protection can occur when the password file is being edited or otherwise modified. There is no way to prevent the making of copies by privileged users. Experience with several earlier remote-access systems showed that such lapses occur with frightening frequency. Perhaps the most memorable such occasion occurred in the early 60s at a time when one of

- An assessment of almost 3300 passwords
- Revealed various bad practices
  - short passwords
  - choices that would be found in dictionaries and name lists
- Introduced feedback to encourage users to make more secure choices

Some realisations …

Passwords are a broken mechanism

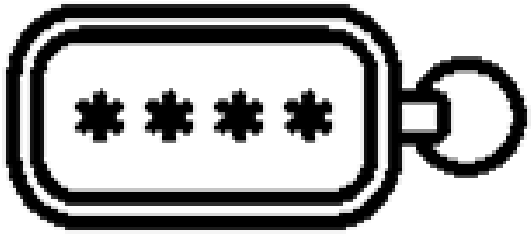
The *method* itself doesn't naturally improve over time

User *behaviour* won't naturally improve either

Change the method or support people better

Changing the method …?

Biometrics



Tokens

Authenticator Apps

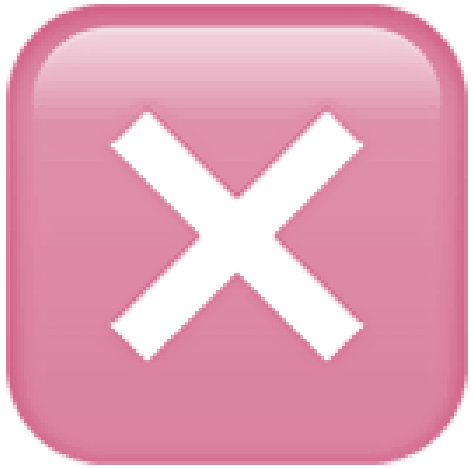
Any panacea here?

Providing support … ?

- Expecting us to use any method assumes we know *how* to do so
- But
  - Will users know how to do it?
  - What support do we provide to help them get it right?
- Support ought to cover:
  - Setting it up
  - General use
  - Handling problems

What are the problems with passwords?

- **Poor choices**
  - e.g. too short, common words, personal information etc.; vulnerable to cracking and social engineering
- **Written down**
  - risking discovery by other people
- **Retained for long periods**
  - increasing opportunity for an impostor if discovered (or previously shared)
- **The same on multiple systems**
  - a breach on one potentially renders the others vulnerable



And which of these problems are *avoidable*?

- **Poor choices**
  - e.g. too short, common words, personal information etc.; vulnerable to cracking and social engineering
- **Written down**
  - risking discovery by other people
- **Retained for long periods**
  - Increasing opportunity for an impostor if discovered (or previously shared)
- **The same on multiple systems**
  - a breach on one potentially renders the others vulnerable

How supportive is the NHS?

From the NHSmail Password policy:

Passwords are valid for 365 days and all users will receive reminders to change their password via email 18, 10, 5, 2 and 1 day(s) before it's expiry date.

All passwords must follow the following criteria:

- They must be 10 characters or more in length without spaces;
- They must not match the previous 4 passwords used;
- Must not contain the users First Name or Last Name within the password;
- Not detected as a common password, for example Password123, Winter2018;
- Not detected as a breached password (a password used for an account that has previously been compromised or identified as having been breached according to an internet-based breach database).

https://support.nhs.net/knowledge-base/nhsmail-password-policy/

How supportive is the NHS?

Top tip

A good way to create a strong and memorable password is to use three random words. Users should be creative and use words that are memorable to only them, so that people cannot guess their password.

https://support.nhs.net/knowledge-base/nhsmail-password-policy/

How supportive is the NHS?

Important note

We know that common passwords are currently used on the NHSmail service by a number of users. In the future, users who do not meet the above criteria will receive a failure message when changing their password.

https://support.nhs.net/knowledge-base/nhsmail-password-policy/

How supportive is the NHS?

Some reminders to help users keep their NHSmail account active and get the best experience from their account:

- **Record a UK mobile number and set a user account secret to their profile –** this will allow a user to reset their password via their local IT or NHSmail Helpdesk.
- **Register at least one authentication method on their account –** this will allow users to reset their password online at any time without contacting your local IT or NHSmail Helpdesk
- **Change password on all devices –** to prevent their account from becoming locked, users will need to update their password on all the devices (including personal devices) that they use to access NHSmail, for example mobile phone, Outlook desktop, tablet etc.

https://support.nhs.net/knowledge-base/nhsmail-password-policy/

Authenticating your authentication …

Additional Note:

Please note that only the below 3 authentication methods are supported to use SSPR:

- Authenticator App.
- Mobile Phone (SMS).
- Mobile Phone (Voice).

https://support.nhs.net/knowledge-base/getting-ready-to-use-self-service-password-reset-and-unlock/

Looking at the wider context

Computers & Security 120 (2022) 102790

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Assessing website password practices – Unchanged after fifteen years?

Steven Furnell

School of Computer Science, University of Nottingham, Nottingham, UK

ARTICLE INFO

Article history:
Received 16 April 2022
Revised 27 May 2022
Accepted 3 June 2022
Available online 5 June 2022

Keywords:
Passwords
Authentication
Websites
User awareness
Usability

ABSTRACT

Passwords continue to occupy an interesting position in cyber security, being both widely used and widely criticised at the same time. In many cases the criticism is levelled at users, who are routinely judged to be at fault for making weak choices. However, such judgements frequently tend to overlook that fact that users were ultimately permitted to make such choices, and often guided to do no better. This paper presents the fifth in a series of studies that have been conducted every 3-4 years since 2007 and examines the extent to which leading websites guide and support users in making appropriate password choices. Following the same core approach as the prior investigations, it examines the password practices of ten leading websites, with the aim of examining the level of guidance provided to users before and during the password selection process, as well as examining the nature of the passwords that users are then permitted to choose. The findings reveal that while there have been some marginal improvements in some areas (e.g. for the first time all of the sites under test were found to enforce a minimum password length), there are still numerous shortcomings and omissions in areas that would arguably support users in improving both their password practices and their resultant protection. Most sites present no upfront information on what good passwords should look like, and many offer ambiguous feedback in response to choices that are not permitted. Moreover, when it comes to filtering and preventing the use of weak passwords, there are a range of surprising omissions, with some sites readily permitting common passwords that others block for being too obvious. The findings demonstrate that users can remain unguided on good practice and unchallenged on bad decisions, which continues to be a disappointing outcome in an area of cyber security that is used so often.

1. Introduction

Despite being routinely criticised and frequently exposed in practice, passwords remain our most common form of user authentication. There are certainly situations where we now see less of them, most notably when authenticating via devices that have biometric capabilities. However, in many cases these other methods are simply acting as a usability layer and the password is still sitting underneath. Alongside all this, our ability to choose and use passwords appropriately remains inconsistent at best. Each year sees the release of a list of the most common passwords, and each year many of the same poor choices top the list. For example, in 2021, the top five spots were '123,456', '123,456,789', '12,345', 'qwerty' and 'password' (Cerniauskaite, 2021). None of these can claim to be good choices, and yet they are routinely in the running. Indeed, '123,456' has been topping the list since 2013. At the same time, the release of such findings also tends to prompt the same commentary – users are making bad choices and ought to do better to protect themselves and their data. So, we essentially get a yearly re-run of the same news and the same analysis. Moreover, the same issues around common choices and the resulting vulnerability of passwords are also highlighted in other studies based on other data sources (Kanta et al., 2021).

Of course, none of this is new. We can find studies evidencing the weakness of users' password behaviour as far back as the late 1970s, with Morris and Thompson's assessment of almost 3300 passwords revealing various bad practices (e.g. short passwords and choices that would be found in dictionaries and name lists) (Morris and Thompson, 1979). Given that such evidence was at hand over 40 years ago, one might have hoped that today's systems would be robust against preventing poor password choices. There has, after all, been a reasonable amount of time in which to improve things. Instead, it seems that any improvements are somewhat marginal, and many sites and services are still missing the opportunity to encourage and enforce better cyber hygiene.

To evidence the point, this paper examines the password practices observed within leading websites. It considers how users are supported in making good password choices when creating new accounts, looking at the level of guidance provided and the extent to which selection rules are enforced to prevent poor passwords from being used. It follows on from four earlier investigations, pub-

E-mail address: steven.furnell@nottingham.ac.uk

https://doi.org/10.1016/j.cose.2022.102790
0167-4048/

- Shouldn't all this password stuff be second nature by now?
- Shouldn't we already know 'good practice' from elsewhere?
- What support do we get in wider contexts?
- What sort of passwords are we able to 'get away with'?
- Let's look at some findings …

Giving good guidance?

Site	Information prior to password attempt	Tangible guidance prior to password attempt	Feedback during attempt	Post-attempt feedback
Amazon	✓	✗	✗	✓
Facebook	✗	✗	✗	✓
Google	✓	✗	✗	✓
Instagram	✗	✗	✓ (via Next button)	✓
LinkedIn	✓	✗	✗	✓
Microsoft Live	✗	✗	✗	✓
Reddit	✗	✗	✓ (via a meter)	✓
Twitter	✓	✗	✓ (via messages)	-
Wikipedia	✓	✗	✓ (via messages)	-
Yahoo!	✗	✗	✓ (via messages)	-

Post-attempt feedback examples

Please choose a more secure password. It should be longer than 6 characters, unique to you and difficult for others to guess.

Facebook

Please choose a stronger password. Try a mix of letters, numbers, and symbols.

Google

Please enter a more secure password.

LinkedIn

PASSWORD

••••••••

That password is unacceptable

Reddit

Preventing poor practices?

Site	Min length	Prevents surname	Prevents user ID	Prevents password	Prevents Password1!	Prevents dictionary words	Enforces composi-tion	Allows 3 random words	Allows browser-generated	Extra protection (available as options)
Amazon	6	✗	✗	✗	✗	✗	✗	✓	✓	2-step verification
Facebook	6	✓	✓	✓	✗	✗	✗	✓	✓	2-factor authentication
Google	8	✓	✓	✓	✓	~	~	✓	✓	2-step verification
Instagram	6	✗	✓	✓	✗	✓	✗	✓	✓	Two-factor authentication (via SMS codes or third-party app)
LinkedIn	6	✗	✗	✓	✗	~	✗	✓	✓	Two-step verification
Microsoft Live	8	✗	✓	✓	✗	~	✓	✗	✓	2-step verification Microsoft Authenticator App
Reddit	8	✗	✓	✓	✗	✗	✗	✓	✓	Connect to Apple, Google, Twitter. 2-factor authentication
Twitter	8	✗	✗	✓	✗	~	✗	✓	✓	Two-factor authentication (via a code, app, or physical key)
Wikipedia	8	✗	✓	✓	✗	~	✗	✓	✓	✗
Yahoo!	7-9	✓	✓	✓	✓	✓	~	✓	✓	2-step verification

Illustrating broader concerns?

- Findings with passwords are arguably illustrative of two broader issues:
  - Users are often expected to use security without a sufficient degree of guidance and support
  - Our use of security methods can remain fairly static while our use of wider technologies changes dramatically
- Both factors can potentially leave us more exposed to a growing range of threats

Conclusions

- IAM depends upon effective user authentication
  - effectiveness is the *security* and *usability* of the method
- Passwords can be poor in both respects
  - highlights the need for effective support as well
- Other forms of authentication can address some of the issues, but introduce others
  - … and still don’t remove the need for support
- Other aspects of user-facing cyber security have similar considerations
  - we shouldn’t blame users if we’ve not supported them

University of Nottingham
UK | CHINA | MALAYSIA

Prof. Steven Furnell

steven.furnell@nottingham.ac.uk

@smfurnell

Navigating Security Challenges in NHS Identity and Access Management Panel Discussion

Steven Furnell
Professor of Cyber Security - University of Nottingham

Sally Berrill
Head of Data Security and Protection - University Hospitals of Northamptonshire

CONVENZIS

Main Sponsor

CROWDSTRIKE

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Main Sponsor

James Burchell
Sales Engineer Manager
CrowdStrike

Refreshments & Networking

Chair Morning Reflection

Bharat Thakrar
CISO - CyberBTX


NHS IDENTITY AND ACCESS MANAGEMENT SUMMIT
Manage Identities and safeguard patient information

Case Study

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Case Study

BlueFort Security

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Case Study

Josh Neame
CTO - BlueFort Security

Peter Batchelor
Regional Sales Director - Silverfort

Fireside Interview

Barry Richardson
Head of Cyber Security and Information Security - NHS Blood and Transplant

Case Study

CYBERARK®
The Identity Security Company™

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Case Study

David Higgins
Field CTO - CyberArk

Lunch & Networking

Chair Afternoon Address

Bharat Thakrar
CISO - CyberBTX


NHS IDENTITY AND ACCESS MANAGEMENT SUMMIT
Manage Identities and safeguard patient information

Case Study

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Case Study

James Millington
VP - Product Marketing

Fireside Chat

atlasidentity
AN INTRAGEN GROUP COMPANY

okta

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Identity is a crucial role in delivering the NHS priorities

Stephen Williams
Founder of Atlas Identity

atlasidentity
AN INTRAGEN GROUP COMPANY

Justin Woolen
Public Sector Director, Okta

okta

Case Study

Mr Julian Fisher
Author and Intelligence Consultant
Africa Integrity Services Ltd

Drinks and Networking

CONVENZIS

CROWDSTRIKE

Scan here to claim your CPD Certificate...

9th October 2024
15 Hatfields Conference Centre,
London SE1 8DJ