ASSESSMENT 1: PROTOTYPE ACTIVITY REPORT

CYB6014.2 CYBER PROJECT 3

Name: Ray Parker

Student ID: 10532682

Unit Coordinator: BAZLUR RASHID

School of Science – Computing and Security

Edith Cowan University, Joodalup Campus

Table of **Contents**

[Executive Summary 2](#_Toc99127488)

[Objective 2](#_Toc99127489)

[Scope 4](#_Toc99127490)

[Methodology 4](#_Toc99127491)

[Testing /Revision Log 6](#_Toc99127492)

[Next Steps 7](#_Toc99127493)

[References 7](#_Toc99127494)

## Executive Summary

Text-based passwords alone are subject to dictionary attacks as users tend to choose weak passwords in favor of memorability, as well as phishing attacks. Many recognition-based graphical password schemes alone, in order to offer sufficient security, require a number of rounds of verification, introducing usability issues. A hybrid user authentication approach combining text passwords, recognition-based graphical passwords, and a two-step process involving a pin generated dongle, to provide increased security with fewer rounds than such graphical passwords alone. A variation of this two-step authentication method, which we have implemented and deployed, is in use in the real world (Method & Passwords, 2009).

In recent years, computer technology has dramatically changed the way we access information. And for no group is this more dramatic than for those with disabilities. With the support of assistive technology, people with all types of disabilities will be better equipped to enter the mainstream of information access. A person without the use of their hands can enter text by talking to a computer. A person with severe hearing loss can freely use the telephone. A person without sight can instruct a computer to read aloud everything on the screen. A young child with no voice can communicate through a talking computer. In the evolution of technology, this is a critical time in our society for people with disabilities who have so much to gain by accessing emerging technologies – and so much to lose if access is denied. According to the Alliance for Technology Access, while the incidence of disability in the general population is 20%, it is even higher in communities of mixed ethnicity and economically disadvantaged and in rural communities. Research indicates that 67% of all adults with disabilities are unemployed. Disability (seen or unseen) is a part of every community and it is critical that everyone have equal opportunity to move toward a more accessible environment. (Alliance for Technology Access: tasc.ataccess.org) There are several types of assistive technology available to improve accessibility when using comp uters: Screen enlargers and screen magnifiers work like a magnifying glass by enlarging a portion of the screen as the user moves the focus. Voice input aids or speech recognition assist people who have difficulty using a mouse or keyboard. These aids allow users to control computers with their voice instead of a mouse or keyboard. Screen reviewers and screen readers make on-screen information available as synthesized speech or a refreshable Braille display. Generally, they can only translate information that is text. Graphics can be translated if there is alternative text describing the visual images. An on-screen keyboard can help those unable to use a standard keyboard select keys using a pointing method such as pointing devices, switches, or Morse-code input systems. Keyboard enhancement utilities help those with trouble typing--including increasing typing speed. Assistive technology can compensate for erratic motion, tremors, slow response time, and other related conditions. Word prediction utilities offer other types of keyboard filters including typing aids. Alternative input devices allow individuals to control their computers beyond the standard keyboard or mouse with eye-gaze pointing devices, sip-and-puff systems controlled by breathing, and non-standard keyboards. (Microsoft Corporation, www.microsoft.com/) Until recently, these enhancements required the user to obtain specialized software that provided the desired feature. With performance improvements in computers, accessibility features are being gradually incorporated into the operating system and are able to address the following types of impairments: Vision Hearing Mobility Cognitive Language 317 From negligible to extreme, the range of impairments is broad. Symptoms of low vision include dimness, haziness, extreme far-sightedness or near-sightedness, color blindness, and tunnel vision. Those with hearing impairments may be able to hear some sound, but may not be able to distinguish words. Others may not hear any sound. For those with hearing impairments, computer prompts such as beeps and spoken messages can be problematic. Users with hearing impairments need visual signals for all information otherwise conveyed by sound. Mobility impairments can be caused by a wide range of illnesses and accidents such as arthritis, stroke, cerebral palsy, Parkinson's disease, multiple sclerosis, loss of limbs or digits, repetitive stress injury, etc. Poor muscle control or weakness can make using standard keyboards and mouse devices difficult. Some people are unable to type two keys simultaneously, while others may hit multiple keys or repeat keys when pressing or releasing them. Those with use of only one hand experience difficulties with certain keyboard and mouse tasks. (Microsoft Corporation, www.microsoft.com/) Cognitive and language impairments ranging from dyslexia to difficulties remembering, solving problems, or perceiving sensory information to problems comprehending and using language can make using computers more difficult. A language translator could prove beneficial to people with any of these disabilities (Camen Lamboy, 2002).

Objective

The results of this prototype test is to facilitate a positive login result from the 2 step authentication process that will be utilised network wide across the entire company

Text passwords have been widely used for user authentication, e.g., by almost all websites on the Internet. However, it is well-known that text passwords are insecure for a variety of reasons. For example, users tend to choose simple passwords in favour of memorability, making them subject to dictionary attacks; and text passwords can be stolen by malicious software (e.g., keystroke loggers) when being entered from keyboards. Phishing is another serious threat to text passwords, by which, a user could be persuaded to visit a forged website and enter their passwords. Such an attack is made possible in part due to the fact that text passwords do not allow users to authenticate a server; by design they provide only one-way user authentication, and server authentication is not a design objective of text passwords alone (Method & Passwords, 2009). We propose a two-step authentication method to strengthen text passwords by combining them with pin generated dongle. In this approach, called Twostep Authentication, users continue to use text passwords as a first step, but then must also enter a pin number generated from a dongle, providing the following advantages: (1) users’ current sign-in experience is largely preserved; (2) a text password alone which is stolen (e.g., by phishing) does not compromise an account; (3) users can be alerted if not seeing the graphical password cueing image after providing their text passwords, implicitly providing server authentication; and (4) it can be implemented in software alone, increasing the potential for large-scale adoption on the Internet (Method & Passwords, 2009).

## Scope

2SAS Two Step Authentication Solution: Passwords with access to organizational systems and networks are vulnerable and open to hackers and compromise the network system. Many organizations fail to secure or implement strong passwords for users. To harden the computer network in the organization we plan to introduce a simple one button press token to generate a pin number to use with the user password to gain access to the system. The use of a sms solution requires all users to have their phone with them at login. This presents a problem when you consider many government and military organisations prohibit the use of mobile phones in the office or in some cases the building.

Manage the password authentication process to harden the computer system to protect from attacks and hackers gaining access to the network system.

## Methodology

To prepare a virtual lab consisting of 2 servers running Microsoft Server 2022 and 5 client machines running Microsoft Windows 11 mentioned in the preceding table 1. Evaluation ISO images (Windows Server 2022 (Insider Preview) and Windows 11\_English) from the Microsoft Evaluation download centre. VM Ware Workstation software was provided by ECU university, downloaded and installed on the host machine (Dell 9010 SSF workstation). The first virtual machine which will be the first Domain Controller (DC01) was created in VMWare. Installation was performed by an autounattend.xml file. Once installed this server was promoted as a Domain Controller in the widget LLC forest with Active Directory services installed. The second Domain Controller (DC02) was then installed in Vmware and promoted to the widget LLC domain (K.G.Mark, 2016).

|  |  |  |
| --- | --- | --- |
| **S.No.** | **VM Name** | **Operating System** |
| 1 | DC01 | Windows Server 2022 |
| 2 | DC02 | Windows Server 2022 |
| 3 | Client01 | Windows 11 Pro |
| 4 | Client02 | Windows 11 Pro |
| 5 | Client03 | Windows 11 Pro |
| 6 | Client04 | Windows 11 Pro |
| 7 | Client05 | Windows 11 Pro |

*Table 1.*

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **VM Name** | **IP Address** | **Role** |
|  | DC01 | 10.10.10.101  Netmask :255.0.0.255  DNS: 10.10.10.100 | Domain Controller of widgetllc.internal domain. |
| 2 | DC02 | 10.10.10.102  Netmask :255.0.0.255  DNS: 10.10.10.100 | Member sever of widgetllc.internal domain. |
| 3 | Client01 | 10.10.10.103  Netmask :255.0.0.255  DNS: 10.10.10.100 | Client machine of widgetllc domain |
| 4 | Client02 | 10.10.10.104  Netmask :255.0.0.255  DNS: 10.10.10.100 | Client machine of widgetllc domain |
| 5 | Client03 | 10.10.10.105  Netmask :255.0.0.255  DNS: 10.10.10.100 | Client machine of widgetllc domain |
| 6 | Client04 | 10.10.10.106  Netmask :255.0.0.255  DNS: 10.10.10.100 | Client machine of widgetllc domain |
| 7 | Client05 | 10.10.10.107  Netmask :255.0.0.255  DNS: 10.10.10.100 | Client machine of widgetllc domain |

*Table 2.*

Restart and sign in to the system with the Administrator account. After some time, the Server Manager console will display. 4. Open the Run dialog box, type ncpa.cpl, and then press Enter. 5. Select and right-click the active network adapter, and then select Properties. 6. Set the following TCP/IP settings: IP address: 10.0.0.100. Subnet mask: 255.0.0.0. Default gateway: 10.0.0.1. Preferred DNS server: 10.0.0.100The following features are proposed:

* The stakeholders require a more secure login system to prevent attacks from internal and external actors.
* Users will provide a password along with a pin generated by the dongle to login to the network system.
* This solution will harden the network system and help protect assets and intellectual property from attacks.
* Users will not be impacted except for an extra 5 seconds to input the pin to login.
* The only cost incurred by the stakeholders will be the purchase of the dongle
* This solution will only require existing IT personnel to implement the change necessary on the server side to include the scripting to allow authentication for user logins.

## This project will be implemented over a period of 18 weeks from January 10 2022 and is expected to be completed by 26 June 2022 (Parker, 2022).

The resources required to complete this project include the purchasing of the dongle to be used and supplied to all users of the system. An inventory system will be integrated into the current asset inventory system to allocate the dongles to users of the network.

Current IT department employees will be provided by the company eliminating any new costs to the project.

A video presentation will be created in order to show the stakeholders how the new system will operate and the new login process will only add around 5 seconds to the current login time.

Training users will only include a short explanation of how to use the new dongle to generate the pin which expires in 5 seconds and a new pin is generated to operate in sync with the authentication server.

## 

## Testing/Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Action** | **Steps performed** | **Results (If any)** |
| 1 | Install Windows Server 2022 in VM Ware as Domain Controller 1(DC01) | Opened VM ware on Host Dell 9010 | VM workstation initialised |
| 2 | Promote Server DC01 with Active Directory Services | Promote DC01 primary DC in widgetllc forest | IP address: 10.10.10.101 Subnet mask: 255.0.0.0   DNS: 10.10.10.100 |
| 3 | Install Windows Server 2022 in VM Ware as Domain Controller 2 (DC02) | Promote DC02 into the widgetllc forest | IP address: 10.10.10.102 Subnet mask: 255.0.0.0   DNS: 10.10.10.100 |

(Zhang et al., 2018)

## Next Steps we need to define this part of the doc

## References

Camen Lamboy, M. S. (2002). Microsoft Windows XP Accessibility Features

K.G.Mark. (2016). Installing and Configuring Windows Server 2016 (Hands-on Guide).

Method, T. A. A., & Passwords, C. T. a. G. (2009). TwoStep An Authentication Method.

Parker, R. (2022). *CYB6013\_Prototype Activity Report*.

Zhang, J., Tan, X., Wang, X., Yan, A., & Qin, Z. (2018). T2FA: Transparent Two-Factor Authentication. *IEEE Access, 6*, 32677-32686. <https://doi.org/10.1109/access.2018.2844548>