Assignment 6

# Access Control

Nathan Ketterlinus

Fisher College of Science and Mathematics

Towson University

Towson, United States

[nketter1@students.towson.edu](mailto:nketter1@students.towson.edu)

1. Open the article <https://www.androidauthority.com/show-hidden-passwords-1010049/> and follow the steps to reveal at least three of your passwords. List which apps you were able to find your passwords.

I have passwords for 97 websites stored on my chrome account, including passwords for websites such as chess.com, ea.com, and funimation.com

1. Complete the following lab and Submit the certificate on blackboard.

<http://cis1.towson.edu/~cyber4all/modules/nanomodules/Computer_Literacy-Passwords.html>

A screen shot of a computer program

Description automatically generated

1. Read three recent news articles about passwords and write a brief summary. Include a reference to each article. (One full page minimum)
2. The first article I read refers to a recent side channel attack in IOS and MacOS devices with A- and M- series CPUs. The attack, labeled “iLeakage”, allows attackers to reconstruct data from any website an affected system has loaded in memory, including “YouTube viewing history, the content of a Gmail inbox—when a target is logged in—and a password as it’s being autofilled by a credential manager” [1]. The rate at which the attack recovers and reconstructs data is around 512 bits per 30 seconds [1]. While this is relatively small, the fact that any data can be scraped at all is what is concerning.
3. The second article I read essentially restates a lot of the best practices of creating and managing secure passwords. The tips listed include enforcing a minimum password length of eight characters, including uppercase, lowercase, numerical, and special characters, and not using easily guessable phrases, like names or birthdays. In addition, the article suggests changing passwords every “90 to 180 days” [2]. Finally, the article suggests various alternatives that can be used to replace or in conjunction with passwords, such as 2FA, MFA, biometrics, tokens, OTPs, and social logins [2].
4. The third article I read relates to Netflix’s ongoing pursuit to stop its customer base from sharing passwords. The way that they appear to be implementing their solution is to require all paying subscribers to set a primary location. Any device that Netflix deems doesn’t belong to that network/ falls outside of acceptable use will add an extra charge to the paying subscriber’s bill. The criteria for what constitutes acceptable use seems a bit vague, but Netflix is quoted as saying that devices on a primary network will be determined “’using information such as IP addresses, device IDs, and account activity from devices signed into the Netflix account’” [3].
5. Read three recent news articles about Biometrics and write a brief summary. Include a reference to each article. (One full page minimum)
6. The first article I read outlines the Customs and Border Protection’s implementation of facial biometrics at all international airports. Based on authorization granted by the 9/11 commission report, the CBP has begun using facial comparison software to “record the arrivals and departures of visitors at all air, sea and land ports of entry” [4]. Specifically, all travelers that are scanned have their face scans sent to a cloud-based facial matching service, where they are compared to templates from passenger travel documents [4]. While this service is being used to speed up the customs process at airports, having such a massive database of PII is a bit alarming. The value of that collection is astronomical, and every measure must be taken to use and protect that data responsibly.
7. The second article I read covers the basics of what biometrics are, as well as the advantages and disadvantages of using them. The primary listed benefit is the added convenience of things like fingerprint and face scans, achieved with an accuracy of around 99.9% [5]. It allows users to add security to their devices in a way that is easily accepted and adapted to by new users [5]. Using biometrics as a primary authenticator with a pin or passcode as a backup also allows for the backup codes to be more complex, as they will not have to be entered every time. However, the article also addresses concerns of biometric attacks, such as presentation attacks, replay attacks, the needed security of fallback authenticators, and privacy issues [5].
8. The final article I read defines biometrics, but also goes in-depth on the differences between behavioral biometrics, such as keystroke recognition and signature recognition, and physiological biometrics, such as fingerprint recognition and iris recognition [6]. The article then lists biometric data breaches, misinterpretation bias, and the selling of biometric data as inherent risks of biometric data [6]. The article then shills Norton 360 with LifeLock Select as a way to protect your biometric data [6].
9. Research the Bell-La Padula Security Model and complete the second table.
   * Suppose you have a secure system with two subjects and two objects. Notation H is High security level, and L is Low security level.

|  |  |  |
| --- | --- | --- |
| **Type** | **Name** | **Level** |
| Object | Obj1 | L |
|  | Obj2 | H |
| Subject | Subj1 | H |
|  | Subj2 | L |

* + You wish to implement a Bell and LaPadula model of security for this system. Fill in the access rights (R and/or W) permitted by the model for each subject/object pair in the access matrix below.

|  |  |  |
| --- | --- | --- |
|  | **Obj1** | **Obj2** |
| Subj1 | R | RW |
| Subj2 | RW | W |

# Resources

[https://courses.cs.vt.edu/~cs5204/fall99/protection/harsh/#:~:text=The%20Bell%2DLapadula%](https://courses.cs.vt.edu/~cs5204/fall99/protection/harsh/#%3A~%3Atext%3DThe%20Bell%2DLapadula%20model%20supplements%2Caccess%20control%20and%20information%20flow.%26text%3DBell%20and%20Lapadula%20modeled%20the%2Cthe%20security%20of%20the%20system) [20model%20supplements,access%20control%20and%20information%20flow.&text=Bell%20an](https://courses.cs.vt.edu/~cs5204/fall99/protection/harsh/#%3A~%3Atext%3DThe%20Bell%2DLapadula%20model%20supplements%2Caccess%20control%20and%20information%20flow.%26text%3DBell%20and%20Lapadula%20modeled%20the%2Cthe%20security%20of%20the%20system) [d%20Lapadula%20modeled%20the,the%20security%20of%20the%20system](https://courses.cs.vt.edu/~cs5204/fall99/protection/harsh/#%3A~%3Atext%3DThe%20Bell%2DLapadula%20model%20supplements%2Caccess%20control%20and%20information%20flow.%26text%3DBell%20and%20Lapadula%20modeled%20the%2Cthe%20security%20of%20the%20system).

[https://www.vokke.com.au/blog/2021/03/15/permission-systems-and-access-controls-the-](https://www.vokke.com.au/blog/2021/03/15/permission-systems-and-access-controls-the-bell-lapadula-model/) [bell-lapadula-model/](https://www.vokke.com.au/blog/2021/03/15/permission-systems-and-access-controls-the-bell-lapadula-model/)

[https://www.cs.purdue.edu/homes/ninghui/courses/526\_Fall14/handouts/14\_526\_topic17.pd](https://www.cs.purdue.edu/homes/ninghui/courses/526_Fall14/handouts/14_526_topic17.pdf) [f](https://www.cs.purdue.edu/homes/ninghui/courses/526_Fall14/handouts/14_526_topic17.pdf)

References

[1] D. Goodin, “Hackers Can Force IOS and macos browsers to divulge passwords and much more,” Ars Technica, <https://arstechnica.com/security/2023/10/hackers-can-force-ios-and-macos-browsers-to-divulge-passwords-and-a-whole-lot-more/> (accessed Oct. 26, 2023).

[2] M. Bacon, “What is a password?,” Security, <https://www.techtarget.com/searchsecurity/definition/password> (accessed Oct. 28, 2023).

[3] Nerdist, “Netflix’s password sharing crackdown has officially arrived in the US,” Nerdist, <https://nerdist.com/article/netflix-stopping-password-sharing-with-price-increases/> (accessed Oct. 28, 2023).

[4] Customs and Border Patrol, “Biometrics,” U.S. Customs and Border Protection, <https://www.cbp.gov/travel/biometrics> (accessed Oct. 28, 2023).

[5] National Cyber Security Centre, “Using biometrics,” NCSC, <https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/using-biometrics> (accessed Oct. 28, 2023).

[6] C. Stouffer, “What is biometrics + is it safe? - Norton,” United States, <https://us.norton.com/blog/iot/what-is-biometrics> (accessed Oct. 28, 2023).