Unit 3 Authentication Mapping

**Corey Crooks**

**Purdue University Global**

**IT484—Cybersecurity Policies**

**Preston Rich**

**December 27, 2023**

**Part 1**

There are many key considerations when using a “defense in depth” strategy. Primarily among them are security controls. Security controls are particularly important to prevent malicious actors from entering an organization's network either physically or digitally to secure the data contained within. These controls act as either physical or digital barriers against these malicious actors and have their unique style of Prevention mentioned within the control categories (Franco, n.d.). These controls come in many forms, but they typically fit into three categories. First and foremost there are administrative controls. Administrative controls deal with the management of the platform that an organization is trying to implement. These controls are particularly important for keeping operational efficiency at maximum while swapping out different modules that may be required by the cybersecurity team. This can help keep an organization running effectively while also mitigating the damage and downtime an organization may have during their operations in their daily functions. Secondly, there are physical controls. These controls determine how an individual may physically gain access to critical systems within an organization. Although these systems come in many different forms there are a few key components that they share. Physical controls may be something simple such as a lock on a door leading to a server room a physical badge that an employee is required to wear at all times for immediate identification, or even a key card that grants access to certain rooms but not all. All of these systems are essential For an organization to maintain heightened security while also not impeding employees in their ability to do their daily job functions. Finally, there are technical controls. Technical controls get a little bit more complicated as the disciplines required to operate them may expand or shrink depending on the complexity of the attack they are made to divert. These controls may come in the form of a simple firewall meant to screen Internet traffic to look for potential malicious actors as they pop up in real-time, or they may be more complex tools that allow an engineer to screen through various network traffic to route for suspicious patterns of malicious activity. All of these controls combined can help synergize the workplace in an organization to further increase the security value in organizations that employees may be able to add to it. Although each of the three of these security controls serves similar purposes, they are different enough to warrant stacking security layers on top of one another. Because of this careful consideration must be put into exactly how an organization is implementing each of these security protocols. It is important to look past the bare requirements of an organization to see what value each security control may give to the organization to bolster the security as a whole. It is also possible that the security controls may be able to synergize with one another to further help security effectiveness. For instance, certain technical controls may be able to have utilization with certain physical controls to increase the effectiveness of the other simultaneously.

**Part 2**

**What are the pros and cons of three different biometric identification authentication systems?**

* Biometric identification comes in many forms. One such form would be a fingerprint scanner. This scanner takes a user’s fingerprint and stores it within the scanner's database to prevent entry to any fingerprint that doesn’t match physically with entries stored in its database (Atherton, 2022). Historically this biometric identification method may come at a low cost and simple installation. It is additionally simple to use and is widely available in the technological industry. This does come with a drawback, however. Fingerprint scanning can become unreliable for certain users. Users who are trying to identify themselves in the rain may have warped fingerprints that may produce an unreliable scan and create false negatives. Additionally, if the user’s fingerprints become damaged from physical injuries such as cuts, the fingerprint scanner may become unable to read them. A second low-cost biometric identification system comes in the form of voice recognition. This technology is widely available for machines of very little computing capacity. This can make this particular technology optimal for organizations of a higher scale due to the low cost of implementation. However, this system may be particularly easy for a false positive. Technologies such as deep fakes allow malicious actors to synthesize a voice that sounds identical to a target. This will allow malicious actors easy entry into the facility despite not being approved before their entry. A third example of biometric identification would be facial recognition. This identification method is widely popular due to the intricacies of the design of the concept. This identification method gives you a more easily recognized user. However, this identification method can be very easily subverted. Using concepts like videos or photos of a target, a tanker can easily gain access to the facility by simply holding up the photo or video in front of a camera. There are concepts such as three-dimensional depth mapping which makes this style of attack much harder to perpetrate By enforcing that a face must exist within a three-dimensional space. However, even for non-malicious actors, this identification method may be unrealistic. For users that undergo frequent visual changes such as shaving a beard Or wearing a different hat, this system may have a difficult time storing their unique signature within the system’s database. This will in turn prevent authorized users from entering the site simply due to a false negative.

**What security controls would you use to make credit cards more secure?**

* Several security controls already exist to help bolster the security of credit cards in today’s society. Such controls may take the form of technical controls, which run several diagnostic systems to ensure that the user is physically capable of making such a transaction. I would expand further on this situation to make sure that a user is probable to make such a transaction. I believe that further communication could be done on a user’s part to inform a bank of plans such as traveling abroad That could be combined with such systems to create a data map of a user’s habits. This behavioral pattern could be essential to providing a more secure experience to a user's credit card needs. Specifically, I would implement a solution in which a user would not be able to make purchases across state lines, or similar geographic areas, which they may be perfectly capable of should advanced transit such as planes or trains be available to them. Instead, the habitual map of the user’s purchases would serve as data points to whether or not they would be statistically inclined to make purchases from that area. Should a user not have a record of purchasing from that area, or making such purchases outside of their typical scope before, communication would be established to ensure that that purchase is indeed made by that user in question. This may in turn create false negatives, but I believe additional false negatives may be worth reducing the risk of false positives that could be much more costly for both the user and the bank associated with them.

**What is authentication, and what are three different ways to accomplish it?**

* Authentication details several different cybersecurity disciplines. Specifically, the concept of authentication details whether or not a subject can access what they are trying to access. One such way to accomplish this would be a simple credential combination (Boston University, n.d.). This method is particularly popular Online where a user may need a user account that keeps track of user data to streamline processes such as purchases or recommendations. In this situation, they would commonly use a username provided by them in conjunction with a password provided by them. Upon entry of The correct username and password combination, the user will then be able to log in to their specific user account. Another authentication method would be Significantly more involved. This method details two-factor authentication. In this, a user still has a password and user name combination, but they would also stack an additional layer of security on top of that by providing a second means of authentication such as a code from a text they received to their cell phone, or an email to the address provided (Rochester, n.d.). This doubles the security of the accounting question by making it much more difficult to succeed in malicious attacks by needing a degree more account information to bypass security protocols. A third authentication method would be that of biometrics. Biometrics aims to gather the physical descriptors of a user to utilize those as a unique identification for the user and their security permissions. This can take the form of a fingerprint, an ocular scan, or even a user’s voice. This hyper-specific method of authentication can seem particularly personal to a user and may be much more difficult to bypass compared to standard username and password combinations.

# **References**

Atherton, K. (2022, February 9). *The Enduring Risk Posed by Biometric Identification Systems*. Retrieved from Brookings.edu: https://www.brookings.edu/articles/the-enduring-risks-posed-by-biometric-identification-systems/

Boston University. (n.d.). *Understanding Authentication, Authorization, and Encryption*. Retrieved from bu.edu: https://www.bu.edu/tech/about/security-resources/bestpractice/auth/

Franco, J. (n.d.). *Cyber Defense Overview*. Retrieved from The University of Cincinnati: http://gauss.ececs.uc.edu/Courses/c6055/pdf/defense-in-depth.pdf

Rochester, T. U. (n.d.). *Standard Security Controls*. Retrieved from rochester.edu: https://tech.rochester.edu/policies/standard-security-controls/