COMP1002

Assessment 1: Set Exercises

Contents

Authentication Report

The current standard for authenticating ATM clients is 4-digit PINs. In light of the bank's concerns with the security of PIN authorisation, this report will discuss a variety of alternative methods, and promote the best fitting solution(s).

As for what makes an authentication method applicable, depends on these four following attributes (Thorpe et al., 2005):

- Changeability
- Resistance to shoulder surfing
- Theft protection
- User non-compliance protection

PIN authentication itself is not widely regarded as a highly secure method because, although it can be easily changed if compromised, a client's PIN does not offer the three latter points. Clients must actively be cautious when entering PINs to prevent shoulder surfing attacks. Likewise, clients have to actively engage in not sharing PINs (De Luca et al., 2010), which in the cases of blackmail or social engineering, can leave the client vulnerable. Finally, as with passwords, PINs can be cracked via brute force techniques due to their limited entropy (PINs are of limited size and often restricted to being numerical).

Whilst increasing the length of the PIN would surely increase the entropy, it would also impact the advantages that a PIN provides, such as: conveniency and memorability. Also, compared to other authentication methods PINs are undeniably cheaper to implement on a widespread scale.

Another method (although not used practically) is EEG-based authentication which uses Brain-Computer Interface technology to both authenticate and uniquely identify clients (Khalifa et al., 2012; Thorpe et al., 2005; Saulynas et al., 2017) via brain waves. Studies into this form of biometric authentication point towards a future in which authentication is 'hands-free' (Saulynas et al., 2017) and in instances where clients have disabilities, BCI make ATMs more inclusive. BCI is invulnerable to shoulder surfing, unobservable to third parties, access cannot be shared, and the access criteria can be changed. However, as research has shown, BCI authorisation requires training (Saulynas et al., 2017); the hardware is also costly to deploy in comparison to PIN.

The bank may also opt for another form of biometric authentication, such as fingerprint scanning. However, these applications are vulnerable to attacks such as fake biometric readers. Physiological biometrics are advantageous because of their uniqueness between different individuals; however, many of these biometric applications are reliant upon unchanging characteristics (Thorpe et al., 2005), which can negatively impact accessibility to ATMs in certain contexts, such as injury. Also, if stolen by an attacker, a client's biometric, because unchangeable, can be indefinitely compromised.

This report's final proposal is to implement One-Time Passwords, which relieves the issue of shoulder surfing (Kaspersky Lab, 2016). OTPs themselves may not be best fit as a single factor approach, but if combined with at least one other factor (2FA), a strong authentication (Kaspersky Lab, 2016) system can be created, therefore leading the report to conclude with three hypotheses:

1. Keep using PIN authentication because it is the current standard, is cheap and provides the most conveniency to clients as it is the fastest method.

2. In the context of securing high value assets, implement the new EEG biometric authorisation methods, as it is theoretically the most secure method.
3. Employ a 2FA system, such as the combination of a biometric and an OTP, to make it harder for attackers to fraudulently access an ATM as they need both factors simultaneously.

Ultimately, of these solutions the most advisable solution is the third - it provides multi-layered access control. 2FA provides attackers with a greater challenge when attempting to commit crime – there is high entropy and if one factor is compromised, the other remains confidential as the factors themselves are ideally 'mutually independent' (Kaspersky Lab, 2016). Whilst sacrificing some conveniency, this approach still increases the complexity of the security, in comparison to PIN.

Authentication Reference List

De Luca, A., Hertz, K. and Hussman, H., 2010. ColorPIN: Securing PIN Entry through Indirect Input. In: CHI '10: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. New York, NY, USA: Association for Computing Machinery, pp.1103-1106.

Kaspersky Lab, 2016. Future attack scenarios against ATM authentication systems. Kaspersky, pp.3-27.

Khalifa, W., Salem, A., Roushdy, M. and Revett, K., 2012. A survey of EEG based user authentication schemes. In: 8th International Conference on Informatics and Systems (INFOS). IEEE, pp.55-60.

Saulynas, S., Lechner, C. and Kuber, R., 2017. Towards the Use of Brain–Computer Interface and Gestural Technologies as a Potential Alternative to PIN Authentication. International Journal of Human–Computer Interaction, 34(5), pp.433-444.

Thorpe, J., van Oorschot, P. and Somayaji, A., 2005. Pass-thoughts: authenticating with our minds. In: Proceedings of the 2005 workshop on New security paradigms. New York, NY, USA: Association for Computing Machinery, pp.45-56.

Network Design Report

Flat networks are not ideally suited for complex networks, of which the bank is most likely to have as there will generally be multiple departments and each would require different services to each other. To force this type of network onto the bank would create a lot of issues and potential vulnerabilities.

Firstly, if a technical issue arises within the network, the inflexible, integrated flat network design would make it harder for technicians to locate and identify faults. Secondly, the three CIA principles (Confidentiality, Integrity, Availability) may be breached as its harder to prevent certain clients from accessing material that they are not permitted to view – such as janitors viewing personal information about the bank's customers. Therefore, these disadvantages indicate a need for a modular and segmented network.

This report will continue on to outline an alternative network structure whilst providing and evidencing the logic as to why the proposed design considerations will benefit the security of the bank. Viewing the bank's network as a whole, the reader will be shown a high-level view of the best network practices and drawn upon why a flat network is not suitable for the bank.

A hierarchal network is an industry accepted network architecture and has many advantages, such as having a modular design. Other advantages include (Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design, 2021):

- Scalable and flexibly
- Manageable
- Resilient

By abstracting the design of the network into three layers (Core, Distribution, Access) it ensures that the network can be easily restructured (such as when increasing the network's size). Within this design, traffic is local to its layer can be controlled much easier – meaning that the network is easier to moderate as suspicious activity can be filtered or recognised. The access layer can also be used to identify and provide specific clients with different permissions – guests connecting to guest Wi-Fi will not be given the same level of access as other clients, such as IT staff.

However, the network can be provided with more security via modularity by adapting the Enterprise model, which expands upon the hierarchal structure (Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design, 2021). Aside from the Core, Access and Distribution layers, network modules can be connected via the core to provide greater functionality – such as services, and remote access. A modular approach allows for greater access control and management and therefore improves the security of the entire network. By having a modular data centre, the bank can store all of their high asset data (confidential data, personal information etc.) offsite and mitigate the risk of losing it all due to physical hazards like floods or fires.

Finally, through the use of VLANs, even greater control of which clients can access what material on the network can be exercised. The network would ideally create a VLAN for each department within the bank, also including guests, and then provide these VLANs with access to their required resources.

In conclusion, this report ultimately suggests that the bank adopt an Enterprise network architecture to provide modularity to each section of the network, and then use VLANs to segment the clients connecting to the network via the Access layer. Through separating resources and clients, access can be limited to only what the user needs, and the network can maintain the Integrity and Confidentiality of all data.

Network Design Reference List

Ciscopress.com. 2021. Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design. [online] Available at: <https://www.ciscopress.com/articles/article.asp?p=2202410> [Accessed 17 April 2021].