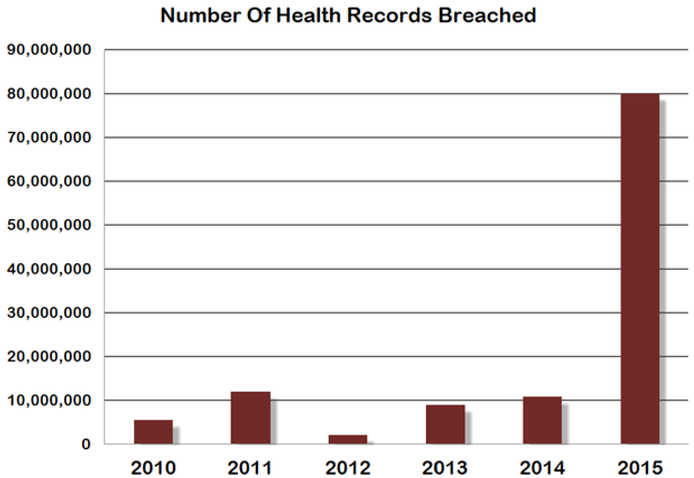
Designing a Secure e-Health Network Architecture

Gabriel De Luca, Morgan Brattstrom - Dr. Patricia Morreale (Advisor)

Department of Computer Science, Kean University, Union, NJ

Abstract

Healthcare data breaches are a growing issue, with healthcare security incidents increasing more than 900% in the last 2 years. This research proposes an improved e-Health network security architecture which will significantly reduce the risk of data breaches and data theft, with minimal additional cost or network delay. This architecture is reliant on the application client and ensures authorized access to health records through the use of a secure client and a 2-step authentication process. The proposed network design will reduce instances of compromised networks, phishing attacks, or unwanted remote access, while improving authenticity of credentials.



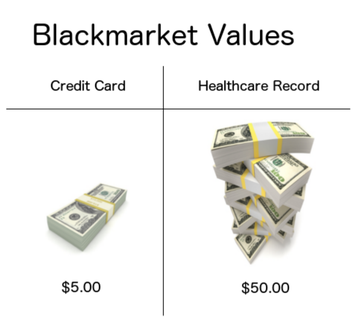
Methods

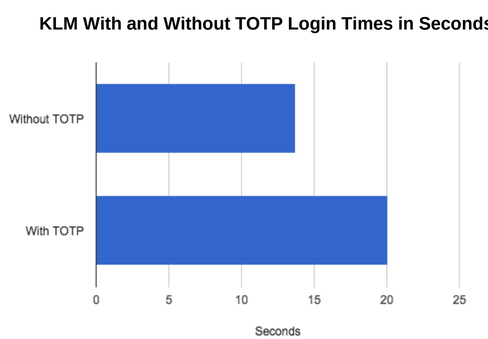
While researching healthcare breaches , a list of vulnerable elements within healthcare networks was compiled. The most frequently targeted vulnerability was phishing of employee login information. Methods to increase user authentication and improve security when logging on add additional time to the login process. We examined the tradeoff of additional login time against the benefit of increased security provided by enhanced user authentication . We also spoke with healthcare workers in several departments to determine the impact an additional 6.35 seconds of login time for improved security would have on their work.

	e-Health Network Architecture Practices	
	Most Secure Practice	***Most Realistic Practice***
Rate-limiting	all access to EHR DB	On-site only
Phishing	Detect and flag all emails	
TOTP	Implement on all systems	
Records	All encrypted	
Off-site	Access disabled	Very restrictive access
IT EHR access	Restricted, only to repair corrupted data	
Process	Pre-encrypt all records on the server; when accessed they are downloaded to the secure client. The secure client is then given a key which allows only the client to be able to decrypt the records for viewing.	
Internet access	Restrict EHR devices	Block personal email
Passwords	Change frequently	
Off-site access		TOTP + credentials
Secure Client access		Secure direct tunnel to network (i.e. VPN)

Results

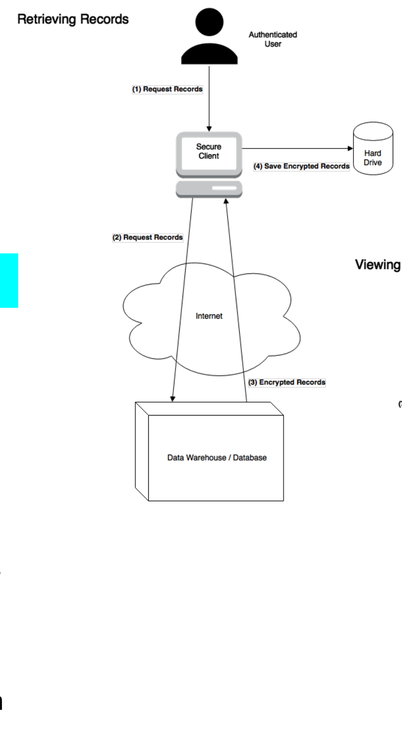
Healthcare data breaches include patient names, medical history, dates of birth, social security numbers, home addresses, phone numbers, email addresses, incomes, and employment information. This type of information almost never changes, or is very hard and expensive to modify. Theft of this information causes victims to be vulnerable to identity fraud years later. Healthcare networks which contain this information become huge targets. We found that a Time based One Time Password (TOTP) added only 6.35 seconds to the amount of time required to authenticate a user into a system. We established that offsite access of patient information was far too easy for something so important. Adding offsite encryption and tunnels to and from the network, effectively forcing all patient information to be encrypted at every point including while not being used, improves data security while adding zero additional time to the them needed to access patient information which does not hinder a healthcare professional's quality of service.





Conclusions

The addition of Time Based One Time Passwords which are used by companies like Google, Facebook, Dropbox, Microsoft, Github, and many others as part of a 2-Step Authentication process greatly increases the security of healthcare systems while only adding 6.35 seconds to the login process.



References

1. Verizon Data Breach Investigation Report 2015.
2. T. Murphy and B. Bailey, "Hackers mine for gold in medical records", Assoc. Press, Feb. 6, 2015.
3. K. Westin, "Encryption wouldn't have stopped Anthem's data breach", MIT Tech Feb 10, 2015.
4. NBC News, "US healthcare system has $5.6 billion security problem", March 12, 2014.
5. R. Rauscher and R. Acharya, "A Network Security Architecture to Reduce the Risk of Data Leakage for Health Care Organizations", Proceedings of the IEEE 16th International Conference on e-Health Networking, Applications, and Services (IEEE HealthCom 2014), 2014, pp. 231-236.
6. C. Pereira, S. Frade, P. Brandao, R. Correia, and A. Aguiar, "Integrating Data and Network Standards into a Interoperable E-Health Solution", Proceedings of the 2nd International Workshop on Service Science for e-Health (IEEE SSH 2014), 2014, pp. 99-104.
7. U.S. Dept. of HHS, "Is the use of encryption mandatory in the Security Rule?", 201.
8. S. Sutner, "Ransomware program fuels health data extortionists", Tech Target, July 10, 2014.

G. Deluca, M Brattstrom, and P. Morreale, "Designing a Secure e-Health Network System", *Proceedings of the 10th IEEE International Systems Conf.*, Orlando, FL, April 18-21, 2016.