Sheri L. Wilson

Capella University

TS8535 - System and Application Security Advances

November 29, 2023

Assignment 8: Assignment Draft and Analysis

Leveraged Identity Authentication

1. Research Topic Definition: Leveraged Identity Authentication (LIA) is the concept of using security products developed by a third party, accessible using an Application Protocol Interface (API). The use of LIA enables centralized and simplified account creation and management. There are more than three options that increase the complexity of the management task and each of the three options have different management features.

2. Use Cases:

A client wants a secure E-Commerce Site that handles secure credit card transactions for the exchange of goods and services. It does not want to manage user accounts or be responsible for maintaining user data, but it wants users to be able to securely make purchases from their online store. The recommended solution is the "Sign in With" feature, offering three options. The selected privacy and account management in this study is the "Google One-Tap Sign In" which enables the sharing of secure account information for the transaction. Although it requires more than one tap to register a new account, this method leverages an existing account managed by a primary provider: Google, Inc. Because security is managed by a third party, the individual online retailer lowers its risk and responsibility and users can shop, socialize, and do business online with a lower responsibility of information security management, thus lowering risk and responsibility in two places because of leverage. Google offers a centralized data privacy center that enables users to view and manage accounts in one place through data use authorizations.

3. The System and Application Security Issue(s): Not all systems offer leveraged account information (LIA). An Individually managed duplicative structure is still used. Duplicating account increases the possibility of variation and is more difficult to manage because information is contained in multiple locations, requiring each location to be accessed to change the same data. It does not follow a relational shared data structure. This creates inconsistency problems

and non-standardization of security practices across the internet, limiting the ability to *efficiently* authenticate computerized accounts and activity. Efficiency measurements must be established to determine what fits the criteria. Proof of the theory of causal increase using correlation statistics with a scalable formula for application data management will show greater advantages and lowered risk using the leveraged account information compared to the individualized account management system. Does the Federal Risk Management Framework apply to using leveraged account information coding security system?

4. Research Problem:

Account Management that requires human data duplication requires maintenance in an unknown number of locations with no centralized management system. Account Management and Identity authentication have historically been developed individually for desktop applications that are closely designed similarly to the Operating System's authentication procedure, requiring the creation of an account to use the system. The purpose of identity management and ownership of data is for tracking and authentication in multiple areas, such as business, finance, location, and personalization. New privacy control and disclosure mechanisms have recently been developed to help give people who access online applications and services greater power over their personal information and how it is used, as well as to increase transparency and accountability for organizations that collect and process this information (Balash, 2023). This once meant every Internet Site required the creation and maintenance of single account profiles, for each site, with individually managed site security – proven by a small lock image in the browser address bar, implemented by trained security experts and created by new account holders. It was a security structure with roles and responsibilities split into based on two or more parts: The Company, A Third Party, Sites Security Implementer, and the Account Holder/User. The assumption or

understanding was that each technology provider would create or procure a standard security solution, using multiple languages designed to meet general security requirements of various levels. Although information management is standardized using 'profile' and 'account maintenance' for each Internet Site and users are willing to create multiple accounts using duplicative manual typing processes to set them up, industry is lagging in the implementation of an efficient shared data architecture.

Since architecture refers to both hardware and software designs, it is necessary to understand both sides of the network operation from more than just one side, therefore test cases and use case scenarios are created to prove the hypotheses. A research design and proof must start with an individual user and then be tested with a larger group to prove, even though it can be proven with one single human user who maintains multiple accounts. The use case is designed to prove efficiency in data and privacy management using Leveraged Account Information (LIA). It is unknown if the use of Google's Sign in With code feature is reliant or affected by low-quality security of the information site it is used on, or if security functionality and risk is transferred. It is also unknown what information is transferred and stored in Google, Inc's possession, maintained in their system and for how long, thus transfer of risk and data responsibility remains only a partially understood and partially managed problem. "All of our products are guided by three important principles: With one of the world's most advanced security infrastructures, our products are secure by default. We strictly uphold responsible data practices so every product we build is private by design. And we create easy to use privacy and security settings so you're in control." (Pichai, Google I/O 2021).

5. Limitations of the Study

One of the important limitations of the study is that it can only be tested as a user and not as an information security network manager of leveraged account development and management because it requires the use of third-party technology or another account, where insight is limited. In a limited capacity, it can prove ease of use for developers using LIA Products via an API as a recommended security solution, but to reduce complexity, LIA and API must be both generally explained and studied in detail to prove the theory that lower number of accounts in central locations (or the reuse of existing data) results in lower risk that simplifies the complex 'risk management' design created by previous security assessors.

Since the success of Internet Applications and Mobile Technologies, security protocols have been standardized and followed, requiring identity authentication for every Internet application, with additional and separate security for networks, internet connectivity, and now merchant accounts, as well as other popular Internet applications categorized as social media and now even account management for interactive internet sites. Security breaches, including data hacking, monetary and identity theft, and social engineering, continue to be reported to be on the rise. Because of the invention and popularity of "Artificial Intelligence" and "Information Assurance," the necessity for real authenticated data in online transactions is critical, but so is centralized user managed data security. Sharing of data amongst service providers, commerce, and social systems is considered the most efficient, which is why technologists are now willing to work together to leverage what used to be individually developed 'code' for account management creation and security. Not all e-commerce and online profile systems leverage existing account authentication and management methods, which causes more work and variation that seems like it cannot be statistically evaluated because of the vastness of the Internet and the high number of business and social transactions or sites that are managed by account.

6. Problem Simplification:

A security architecture of interconnectedness that leverages secure account management is vital, which requires a change to more than just a security policy, awareness, press releases or media, technical code, database management, threat-based monitoring, and developer choice. It is unknown if using Google's security functionality by adding code, or connecting through an API is dependent upon the internet site that the code runs on and to what extent. Re-clarification of the scope of security must also be explained and correctly applied to the correct management system. Rather than teaching users how to create secure accounts for each merchant or internet site, and using awareness as a user responsibility, a change to security processes from one side is required, with implementation across the Internet to change how Internet Sites (and possibly more) are created and managed. The result guarantees a benefit that can be seen as a change to the improper transfer and balance of risk and responsibility. Currently, security risks are spread out and by bringing them together, they can then begin to be understood and effectively managed, but first risk must be separated from trust and roles and responsibilities must be well understood, standardized, and proof of improvement to even begin a system security evaluation from a two-part perspective.

7. Background

Security awareness is an educational endeavor, and by doing this, security risk has been transferred to the users, with developers and site owners assuming people can and should manage device and application security on multiple levels, in multiple places, and with many different

companies, processes, and details of promise or service. This has created a security problem that raises the question of whether there is a better architecture or some solution that could centralize and standardize security. The main problem is internet shopping, socializing, and doing business which has resulted in a high number of accounts, and is unnecessarily duplicative, which is hypothesized to increase error and time, increasing the rate of problems, resulting in future mismanagement and possible misfortune. This is expected to become an even greater problem as humans age. It has also resulted in bad publicity in the security sector and lowered consumer confidence, of which there does not seem to be standard protocol or study available for how these critical problems are measured and solved.

Risk and crime are not the only problems, even though they are major. Because of the freedom the internet offers and because of automation, the botnets and hackers have creatively engaged in regular criminal activity online, including cyber-bullying, and theft, and have extended into fake intelligence or the creation and spread of false information, all proving to cause significant damage to people and businesses across the world. Individual training and awareness placed a burden on every user. Fake media is also on the rise, leaving consumers fearful, yet communicative and somewhat knowledgeable about what is happening in computer security.

The idea of creating a single security suite to manage security profiles that can organize all critical information in a centralized location is viewed as a great risk if compromised or misused, thus several efforts, such as individual security accounts with manual organization, multi-factor authentication, and some cyber security practices have been implemented. The theory is that if everything is in one place, then everything can compromise, causing greater damage and the alternate theory is that if everything is maintained using one security profile, then simplification increases security because of the lower number of places to manage necessary change for multiple

events, enabling faster resolution and improved management. The multiple events are changes to personal details, emergency account changes, accessibility, and other information management tasks. Centralized security is of great benefit for efficiency and information management purposes if it is secure and reduces the risk of theft or misuse. It is also hypothesized that an increase in the variation of security options adds to the conceptual risk profile because of individualized approaches which becomes an unmanageable problem. Although risk is often spoken of, it is believed that if there are individualized non-standard security approaches to application account management, then there are also non-standardized risk assessment procedures, making security appear to be professionally management, with varied informal and inconsistent processes, which is what a disorganized criminal or a member of organized crime benefits from. Complexity and decentralization make it more difficult to manage.

There are two problems to solve: the data architecture and user management, which both have direct causal relations to economics, crime, and longevity. Because of the long list of benefits of a centralized system, it must be carefully examined before investment. If developers continue to create varied security solutions, then they cannot solve existing problems, so a stop-work process must be created and placed on all development resources across the world since it poses the greatest risk. If people and management don't view it as a problem, then work continues as usual until the problem is formally presented and proven to cause or increase risk or reduce complexity and meet efficiency criteria for improved use.

8. Significance of the Study

Establishing software product efficiency criteria can be an adopted standard applied to all software, not just security. Specific risk criteria and benefits can also be applied for consideration of other products. The metrics used to evaluate software enable informed selection, which

improves user and/or consumer confidence. The study can be applied to other software systems to show where efficiencies can be gained by using a leveraged approach to functionality.

Reviewing the number and functionality variations of security products is a heavy task, as is understanding and explaining overall security problems with the current process when viewing the entire internet user population, therefore a security developer single-user study is presented. Before the research can be applied to others, levels of experience must also be gathered and evaluated. Without empirical data to show the effectiveness of such practices, efforts continue to strengthen the security system of the Internet as it expands access to other devices including mobile and the development of the Internet of Things. As the Internet grows, risk grows, as do security problems, and the industry adapts through changes like improved security practices in code development, the use of biometrics, online security awareness, and new approaches such as the Federated Identity Model and leveraged Authentication. If the number of accounts grows and increases security risk and results in mismanagement and can be proven, then it can also be believed that as the number of security options and variations grow, the risk also increases to a point of unmanageability and terms or processes can no longer support the design, therefore it must evolve. The “Risk Management Framework” requires reconsideration of the ways in which security is viewed to look beyond a single application and single user view into much higher numbers to understand, prove, and accept the theory. The Risk Management Framework (RMF) provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations (NIST, RMF, 2023).

There is a greater focus now on user experience, with much effort and attention on security. With an enterprise identity management system, rather than having separate credentials for each system, a user can employ a single digital identity to access all resources to which the user is entitled (Barton, et. al, 2019). Even though organizations implement and follow strong security standards and the ISO 27000 Series has 60 standards covering a broad spectrum of information security issues (Kirvan & Granamann, 2023), few engineers have concluded that the security architecture is not the best fit for advanced cyber-evolution and have only slowly taken on an integrated and centralized approach to security. To effectively convey the security problem, it is necessary to understand the burden and risk placed on its users, with better efforts to engineer a solution that solves the problem. Rather than transfer risk and responsibility to the user with varied complexities in many locations and expecting security procedures to be learned and followed by every security company, developer, and user, its lower risk to centralize the design. The research study must follow the quantitative scientific research method to prove its theory, this means the theory must be defined, with double hypothesis testing using the standard method of statistical analysis.

9. Research Method: Quantitative and Qualitative Research using a survey questionnaire and statistical analysis to compare the average number of online accounts per user, number of leveraged accounts, and management time. It must also review a small sample of password reset frequency, along comparison of two security products. Qualitatively, it will review existing broad published research on security breaches for online accounts and processes for small organizations to monitor or evaluate security policies. The questionnaire will also collect a sample on the use of security management suites and the consideration of using a centralized security management suite

for personal online accounts to evaluate two variables comparatively and statistically: leveraged security and individual security profile management. It is possible more variables will be added.

10. Research Questions

Is the existing individualized security account management system functional for a single user? What is more efficient and simplified: LIA or IAM? Is it of lower risk and benefit for a centralized account management system with a more organized and integrated authentication system? Which side of the two- or three-part of security responsibility benefits most? To what extent does a sample population use leveraged security and what is their perceived risk or benefit in doing so? How is the Risk Management Framework applied or changed by choosing a different method? Is offering multiple security options adding more complication to security management and what is the most professional security strategy for new and existing accounts? What are both security processes and why is one better than the other? Is a single-user research study sufficient to create efficiency and risk standards to change the current security practice industry-wide, or do other solutions need to be evaluated for product comparison?

11. Data Collection

Data will be collected and analyzed to show differences between leveraged user accounts and individual accounts. Statistical analysis of the data collected will show time and process variations for both methods and will qualitatively present comparative risk management metrics. A second data collection phase might be conducted using survey data from random participants in a small community, as well as random online participants. The questions will be designed following the qualitative research standards model of survey questionnaires, adhering to ethics, and the survey should include a variety of question types that aim to obtain quantitative data with some qualitative responses from open-ended questions. Ethical Considerations. Confidentiality is important and

ensuring safe handling of information and protection of personal data. Specific informed consent will be explained in detail as to the extent of the survey and voluntary participation. Anonymity will be an option for survey participants and published results will not include personal information.

12. Definitions

Individual User Account: An individual user account is a single profile completed on an internet site or internet site application where a username and password are required, along with personal profile details. These are managed site by site. It is a similar, but not exactly the same standard login process for each site and requires users to 'retype' the same profile information, and allows variation in username, passwords, and personal information.

Leveraged User Account: A leveraged user account uses an existing account, such as Google, Facebook, or AppleId to manage its personal account information. It uses a management console that enables users to control access to other merchants or providers of Internet goods and services. It is a three or four-step login process with no typing required.

Risk Management Terms: Acceptance, Avoidance, Transfer, Mitigation. These are terms used in the Risk Management Framework for Security of Applications. Risk is considered accepted by the users when setting up a profile, and risk is considered transferred by the Technology community, along with information management responsibility. Risk increases when data mismanagement opportunities and inconsistency exist. Perceived risk is a non-proven risk of trusting only one company or application with personal privacy data management. Risk is considered mitigated by users who utilize a centralized password vault, paper process, or third-party application to manage multiple security profiles used in many places. Risk terms from a

developer perspective is also transferred to the provider of security application code implementation using LIA and risk responsibility are uncommunicated mitigation actions completed by security product providers, and data users which encompasses more than a single person, including those who require, use, share, sell, and store the personal data. Risk responsibility is critical to clarify roles and actions required to change media alerts, and viral scare tactics, and to manage security efforts properly for more than just the consumer/user.

Single User Account Data

The table below will be used to collect data to summarize and statistically present once the data has been collected and analyzed using JASP, a statistics calculator. Process comparisons of LIA and IAM will also be presented in the dissertation project.

Individual vs. Leveraged Accounts	
Total Number of Individual Accounts	
Profile Setup Time/Steps	
Login Time/Steps	
Reset Time/Steps	
Total Number of Leveraged Accounts	
Profile Setup Time/Steps	
Login Time/Steps	
Reset Time/Steps	
Data Analysis	
What is the average amount of time spent on Profile Setup	
What is the total average login time for Individual Profiles	
What is the total average login time for Leveraged Accounts	
What is the total average time for Personal Detail Change Leveraged	
The difference between the averages	
Number of possible variations of account information	
Number of actual variations of account information - leveraged	

Account Management Console	
Leveraged Google Accounts	36
Individual Accounts (managed by Human Memory)	
Newsletter Subscription Management	
Individual	
Managed by Google	
Total Number of Subscriptions	

13. Qualitative and Quantitative Research

Depending upon the quality of data and meeting the goals and objectives of single user study of data privacy account management methods, the research project may include a second phase of research that is interview-based, sample of qualified technology professionals for more specific results, which is to be determined after examination. The sample frame for written mailed and online surveys is general internet users with an evaluation of formal technology education and position to perform correlation analysis and independent t-tests on specific variables.

14. Rules, Policy, Regulations, Law

The Privacy Act of 1974 establishes a code of fair information practices that govern the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies (Privacy Act of 1974, 5 U.S.C. § 552a, 1974). The Freedom of Information Act applies only to federal agencies and not to records held by Congress, the courts, or state or local government agencies. Each state has its own public access laws (The Freedom of Information Act, 5 U.S.C. § 552). The Digital Millennium Copyright Act is a 1998 United States copyright law that implements two 1996 treaties of the World Intellectual Property

Organization, criminalizing the production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works (Digital Millennium Copyright Act, Pub. L. No. 105-304,1998).

The availability of information, from personal information to public information, is made all the easier today due to technological changes in computers, digitized networks, internet access, and the creation of new information products. The E-Government Act of 2002 recognized that these advances also have important ramifications for the protection of personal information contained in government records and systems (DOJ, 2019). Privacy Impact Assessments (PIAs) are required for Federal Agencies that develop or procure new information technology involving collection, maintenance, and dissemination of information in identifiable form or that makes substantial changes to an existing system (E-Government Act of 2002, Pub. L. No. 107-347, 2002). Local and state laws vary regarding rules of use of personal information; the state of Virginia prohibits the processing of sensitive data without obtaining consumer consent (Va. Code § 59.1-578). The processing of sensitive data also triggers the obligation to conduct and document a data protection assessment (Va. Code § 59.1-580). The state of California's Consumer Protection law is much more specific in delineating consumer rights of personal information protection (CA DOJ, CCPA, 2023). The Virginia Consumer Data Protection Act (VCDPA) clearly defines whose personal data is covered, describing consumers as Virginia residents "acting only in an individual or household context." It further clarifies that consumers are not those acting in a "commercial or employment context." Unlike California, where the now-expired B2B and employee exclusions have been the subject of several statutory amendments, Virginia has chosen not to leave those potential compliance hurdles up in the air (Bloomberg Law, 2023).

If specific laws that govern the protection of personal information are state by state, then another problem exists in security protections, as are the procedures for remedy when the laws are violated. Therefore, the responsibility for the security of personal information must be clarified and added to the argument that a single provider of security products for consumer use is beneficial for more than just efficiency, but legal purposes.

Literature Review

1. Federated Identity is a service provided by a third party that enables participating organizations to leverage home organizations' digital identities to access partner resources by implementing a common standard for technical interoperation**.**

Barton, et. al, (2019), 7 Things You Should Know About Federated Identity, EDUCAUSE Publications accessed via the Internet at https://library.educause.edu/resources/2019/1/7-things-you-should-know-about-federated-identity

Informative Article

2. If technology can help bridge the design gaps we have, and perform tasks that are mind-numbingly repetitive, why not let it? This article discusses the human condition and evolution with technological assistance.

Kandala, K. (2018), Digital Paranoia: Modern Form of Existential Crisis, accessed via the Internet at https://medium.com/swlh/digital-paranoia-a-case-of-existential-crisis-d2a53ec977c1 on October 17, 2023

Informative Article

3. This is where IT security frameworks and standards are helpful. Knowledge of regulations, standards, and frameworks are essential for all infosec and cybersecurity professionals. Compliance with these frameworks and standards is important from an audit perspective, too.

Kirvan, P. & Granneman, J., (2023), Top 10 IT security frameworks and standards explained *Tech Targets,* accessed via the Internet at https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one on October 17, 2023

Informative Article

4. There is an assumption based upon brand recognition that a user's sense of security correlates with their knowledge of the popularity and success of technology business names. This is a study about brand recognition theory using psychology methods, attempting to apply it to Big Technology names and user's perception of security and trust in software.

The Role of Big Tech in Providing Cybersecurity to End Users: A Qualitative Case Study, Morgan, J.M (2023), Northcentral School of Business, San Diego

Methodology: Qualitative Case Study

5. The Digital Forensics Framework, which is still in its infancy, makes the requirement for hybrid solutions, and creates a conflict or proves delay between law enforcement and technology, increasing security risk.

Quick, Martini, B., Choo, K.-K. R., & Shavers, B. (2014). Cloud storage forensics (1st edition). Elsevier.

6. Copyright and intellectual laws, along with privacy and legal issues as it relates to cloud computing is reviewed. There is no specific "theory" used to articulate the challenges, nor does it suggest how moving to the cloud reduces risk or changes laws. Ownership of data, sharing and other legal issues are still possible, and potentially even greater due to an open programming model that enables a wide variety of security options at the discretion, and control of businesses, and users.

Cheung, A. S. Y., & Weber, R. H. (Eds.). (2015). Privacy and legal issues in cloud computing. Edward Elgar Publishing Limited.

7. Consumer Privacy Legislation by State; privacy-related laws; how do they stay current with cloud computing evolution? Consumer protection acts and do not sell my information remains on the forefront, as does state by state legislation issues with jurisdictional boundaries often crossed in dealing with E-Commerce and information transactions, increasing the need for digital forensics. Consumer awareness studies and a framework for empirical data reviews are also missing.

2022 Consumer Privacy Legislation, National Conference of State Legislature, accessed via the Internet at https://www.ncsl.org/about-state-legislatures/2022-consumer-privacy-legislation on Oct 30, 2023

8. Cognitive Information Processing Theory as it relates to career and adult development. A well-known theory applied to human development not correlated to security systems, or medical device tracking. I attempted to find a study that related the human design of psychology as it correlates with computer processing in information management, with overlaps in terminology, but was unable to find anything.

Osborn, D. S., Hayden, S. C. W., & Brown, C. (2020). Chapter 1: Cognitive Information Processing Theory: International Applications. Career Planning and Adult Development Journal, 35(4), 4-16. Http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Ftrade-journals%2Fchapter-1-cognitive-information-processing-theory%2Fdocview%2F2573517889%2Fse-2%3Faccountid%3D27965

Scholarly Journal

9. Wearable in ear device for Electroencephalography Based System for Biometric Authentication. EEG's brain wave scan ability for use as security biometrics, suggesting brain scan devices worn in the ears can be used for biometric authentication.

Hwidi, J. (2023). *Wearable In-Ear Electroencephalography Based System for Biometric Authentication* (Order No. 30770766). Available from ProQuest Dissertations & Theses Global. (2873028071). http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Fwearable-ear-electroencephalography-based-system%2Fdocview%2F2873028071%2Fse-2%3Faccountid%3D27965

Dissertation, Quantitative Study

10. Direct Brain to Device Connections, review of documented technology and possible security problems and solutions. Advanced authentication, perhaps the best form of biometrics, and additional knowledge management functionality, it appears solutions are added to the long list of possible authentication methods, going from brain scan to wearable technologies, when the

technology itself requires a standard authentication method, integrated with other systems, but with possible sensor technology.

Ortega, A. (2023). *Wearable Brain Computer Interfaces with Near Infrared Spectroscopy* (Order No. 30242215). Available from ProQuest Dissertations & Theses Global. (2769193628). http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Fwearable-brain-computer-interfaces-with-near%2Fdocview%2F2769193628%2Fse-2%3Faccountid%3D27965

Dissertation, Qualitative Study

11. Relationship between Self-Identity Confusion and Internet Addiction among College Students: The Mediating Effects of Psychological Inflexibility and Experiential Avoidance. Are there any related studies or field research on the correlation of technology identity and personal identity problems, and solutions? Identity authentication is varied in computer systems, offering several options, left at company or developer discretion, requiring a high number (non-quantified) and duplicative tasks, proving a non-integrated authentication architecture in Internet or Cloud Systems.

Hsieh, K. Y., Hsiao, R. C., Yang, Y. H., Lee, K. H., & Yen, C. F. (2019). Relationship between Self-Identity Confusion and Internet Addiction among College Students: The Mediating Effects of Psychological Inflexibility and Experiential Avoidance. International journal of environmental research and public health, 16(17), 3225. https://doi.org/10.3390/ijerph16173225

Scholarly Journal

12. Your Head is in the Clouds is an old saying. Since Cloud Computing is new, research is required on using brain imaging technology and cloud computing systems beyond medical information, as well as a higher level of security. It's necessary to review the similarities published by the American Psychological Association to what is being done, said, and referred to in Technology.

How to Keep Your Head in the Clouds: Cloud computing concepts are giving developers freedom and flexibility in application deployments. (2009). *Information Management, 19*(3), 18. http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fhow-keep-your-head-clouds%2Fdocview%2F214668988%2Fse-2%3Faccountid%3D27965

Scholarly Journal

13. Half A Century In CT: How Computed Tomography Has Evolved. The CT-Scan has evolved with the introduction of cloud computing. Medical imaging and radiation therapy professionals need more education in CT technology, including potential laser therapies, and research into information transfer in both digital and physical matter; a combined physics and computer science endeavor would advance the technology, but requires a controlled test in confined spaces.

Half A Century In CT: How Computed Tomography Has Evolved, International Society for Computer Tomography, CT Evolution, Oct 2016 accessed via the Internet at https://www.isct.org/computed-tomography-blog/2017/2/10/half-a-century-in-ct-how-computed-tomography-has-evolved#:~:text=In%201967%20Sir%20Godfrey%20Hounsfield,Laboratories%20using%20x%2

Dray%20technology.&text=In%201971%20the%20first%20patient,publicized%20until%20a%20year%20later. On Oct 30, 2023

Methodology: Qualitative Informative Study

14. Security Awareness Studies on Single Sign-On Solutions of Students

Pratama AR, Firmansyah FM, Rahma F. Security awareness of single sign-on account in the academic community: the roles of demographics, privacy concerns, and Big-Five personality. PeerJ Comput Sci. 2022 Mar 11;8:e918. doi: 10.7717/peerj-cs.918. PMID: 35494842; PMCID: PMC9044249.

Methodology: Quantitative Research

15. User Behaviors and Attitudes towards password expiration policies.

Hana Habib, Pardis Emami Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. User Behaviors and Attitudes Under Password Expiration Policies. Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), Baltimore, MD, pp. 13-20.

Methodology: Quantitative Analysis of Survey Research

16. Diversifying Passwords to Survive: A two-part online study to examine how participants create and use passwords under two adaptive password policies in multiple configurations.

Sean Segreti, William Melicher, Saranga Komanduri, Darya Melicher, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Cranor, and Michelle Mazurek. Diversify to Survive: Making Passwords Stronger with Adaptive Policies. SOUPS 2017, Santa Clara, CA, July 12-14, 2017.

Leveraged Identity Authentication

Methodology: Quantitative Analysis of Survey Research

17. According to Verizon's 2022 Data Breaches Investigations Report, 82% of data breaches involve a human element. In today's volatile cyberattack landscape, every business in every industry is at risk of a cyberattack. That means that every business needs to make sure that it's taking a strong defensive posture with the right solutions in place to reduce risk. One of those solutions should be a robust security awareness training program.

ID Agent: These 10 Facts About the Benefits of Security Awareness Training Are Game-Changers accessed via the Internet at https://www.idagent.com/blog/10-facts-about-the-benefits-of-security-awareness-training/.

Article Review of Verizon Study Methodology: Quantitative Survey

18. Cybercriminals were quick to exploit vulnerabilities. Organizations reported a dramatic increase in malware attacks. The 2020 FBI Internet Crime Report collated data from 791,790 complaints -- a jump of more than 300,000 from the prior year. These victims claimed losses of more than $4.2 billion.

Tech Target, DeCarlo, A., What are the elements of modern network security architecture, July 2023 accessed via the Internet at https://www.techtarget.com/searchnetworking/tip/What-are-the-elements-of-modern-network-security-architecture

Article of Quantitative Study

19. This generic qualitative study explored the factors that influence the state of information security governance in modern non-IT organizations across North America. The study was

framed within the general deterrence theory and used two research questions as a guide. The first research question was what factors influence the effectiveness of ISG policies in non-IT organizations? The second research question was what strategies do non-IT organizations employ to enforce policy compliance?

Kamaziwe, D. W. (2023). *Information Security Governance Shortfalls in Non-IT Organizations: A Generic Qualitative Inquiry* (Order No. 30494236). Available from Dissertations & Theses @ Capella University. (2818503049). http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Finformation-security-governance-shortfalls-non%2Fdocview%2F2818503049%2Fse-2%3Faccountid%3D27965

Capella Dissertation: Qualitative Study

20. This study focused on cybersecurity risk management for the residential real estate industry. The residential real estate industry is an ongoing target for hackers given its information-rich transactional data. The study research question was Which cybersecurity risk management policies do experts in real estate cybersecurity recommend that managers of residential real estate firms implement to prevent, detect, and respond to cybersecurity threats, vulnerabilities, and attacks?

Middleton, T. T. (2022). *Effective Cybersecurity Risk Management Policies for the Residential Real Estate Industry* (Order No. 29261271). Available from Dissertations & Theses @ Capella University. (2694989069). http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-

theses%2Feffective-cybersecurity-risk-management-policies%2Fdocview%2F2694989069%2Fse-2%3Faccountid%3D27965

Generic Qualitative Study

21. The usability and effectiveness of the new privacy control and disclosure mechanisms do not always align with expectations and in this dissertation, we identify and address the shortcomings of these mechanisms to enhance their performance and improve their outcomes.

Balash, D. G. (2023). *Usability of Privacy Control and Disclosure Mechanisms* (Order No. 30316226). Available from ProQuest Dissertations & Theses Global. (2792832069). http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Fusability-privacy-control-disclosure-mechanisms%2Fdocview%2F2792832069%2Fse-2%3Faccountid%3D27965

George Washington University Dissertation: Qualitative Study

22. The Privacy Act of 1974 is a federal statute; a code of fair information practices that governs collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. It is defined as a system or group of records under the control retrieved from an agency regarding an individual.

Privacy Act of 1974, as amended, 5 U.S.C. § 552a, accessed via the Internet at https://www.justice.gov/opcl/privacy-act-1974

Professional Review of Legal Statute

23. The Freedom of Information Act covers public access rights to information records from any federal agency. Not all agencies follow the same procedure for fulfillment of an FOIA, in

fact, the term: records have even been defined to conform to this law in what agencies can provide upon formal request.

The Freedom of Information Act, 5 U.S.C. § 552, Department of Justice, accessed via the Internet at https://www.justice.gov/oip/freedom-information-act-5-usc-552

Federal Legal Statute

24. Since digital technology could allow for infinite numbers of exact copies of works to be made, the lawmakers agreed they had to extend copyright to include limits on devices and services that could be used for anti-circumvention in addition to acts of anti-circumvention. In establishing this, the lawmakers also recognized this would have a negative impact on fair use without exceptions, with electronic works potentially falling into the public domain but still locked beyond anti-circumvention measures, but they also needed to balance the rights of copyright holders. The DMCA as passed contained some basic fair use allowances such as for limited reverse engineering and for security research.

Digital Millennium Copyright Act, Pub. L. No. 105-304,1998, accessed via the Internet at https://www.copyright.gov/legislation/dmca.pdf on November 29, 2023

Federal Legal Statute

25. The California Consumer Privacy Act (CCPA) is a state law that covers consumers' protection rights to information, as well as their ability to limit change and gain access to notices explaining privacy practices. Some search engines require a Privacy Act disclosure statement on internet sites to produce an error-free internet search engine scan, but contents vary by state

because of state law variation. Compliance checks and automation might be possible but does not exist for all or small internet site developers.

State of California Department of Justice, California Consumer Privacy Act (CCPA), Attorney General's Office, California Civil Code § 1798.192 (2022) accessed via the Internet at https://oag.ca.gov/privacy/ccpa on November 28, 2023

Legal Statute: California Civil Code

26. Department of Justice, eGovernment Act of 2022 enacts the establishment of Personal Information Assessments (PIAs) for all government agencies and that the PIAs must be made publicly available upon request, unless it is considered a matter of national security.

EGovernment Privacy Information Assessments, Office of Privacy and Civil Liberties, Department of Justice, Feb 2019 accessed via the Internet at https://www.justice.gov/opcl/e-government-act-2002 on November 28, 2023

Federal Statute, Department of Justice

27. The Code of Virginia on Personal Data Assessments, responsibilities of the Controller and protection of the processing and sale of personal information.

VA code § 59.1-575, Ch. 53, Jan 2023, accessed via the Internet at https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/ on November 29, 2023

28. Bloomberg Law's Legal Interpretation of the Virginian Consumer Data Protection Act.

Leveraged Identity Authentication

Virginia Consumer Data Protection Act (VCDPA): Everything you need to know about Virginia's new comprehensive data privacy law, Bloomberg Law, accessed via the Internet at https://pro.bloomberglaw.com/brief/virginia-consumer-data-protection-act-vcdpa/ on November 28, 2023

Professional Law Review

29. Google's Safety and Privacy Promise; Google's Product Guiding Principles: 1) Secure Product by Default; 2) Responsible Data Practices; 3) Easy to Use Privacy and Security Settings "so you're in control."

Google, Safety Center, Privacy and Security, Pichai, S., 2023 accessed via the Internet at https://safety.google/security-privacy/ on November 29, 2023

Corporate Product Suite Guarantee

30. The Risk Management Framework: Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor. Not all security efforts match the Risk Framework; small developments using leveraged Code uses different processes, but similar to the RFM. he RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The RMF includes activities to prepare organizations to execute the framework at appropriate risk management levels.

National Institute of Standards Technology (NIST), Risk Management Framework (RMF), Nov 2023, accessed via the Internet at https://csrc.nist.gov/projects/risk-management/about-rmf on November 29, 2023

US Department of Commerce, Federal Guideline