Mandala 4:00
R9

Disclaimer: This paper partially fulfills a writing requirement for first year (freshman) engineering students at the University of Pittsburgh Swanson School of Engineering. *This paper is a **student paper, not a professional** paper.* This paper is based on publicly available information and may not provide complete analyses of all relevant data. If this paper is used for any purpose other than this author's partial fulfillment of a writing requirement for first year (freshman) engineering students at the University of Pittsburgh Swanson School of Engineering, users are doing so at their own risk.

SECURING DATA FOR THE FUTURE

Avery Peiffer (aep65@pitt.edu)

INTRODUCTION: LESSONS FROM EQUIFAX

On September 7th, 2017, the credit reporting agency Equifax revealed that "highly sensitive personal and financial information for around 143 million U.S. consumers was compromised in a security breach that began in late spring [2017]" [1]. With a seemingly infinite supply of credit card, drivers' license, and social security numbers now readily available to those possessing malicious intent, many Americans now find themselves at extreme risk of identity theft [1]. Equifax's response to this incident has been less than inspiring; CEO Richard F. Smith placed the blame for the entire cyberattack on one individual who failed to communicate the need to upload the company's software [2]. I find it very difficult to believe that the incompetence of one person can result in an attack of this significance. If this is the case, it speaks to Equifax's systemic ideology regarding the safety of its customers' data that the breach was allowed to happen.

That the personal information of hundreds of millions of Americans was entrusted to Equifax conferred upon the company an inherent responsibility to ensure the security of that information. Equifax failed to uphold this responsibility, but it is important to understand what that entails. Data security is most easily accomplished with a strong data encryption scheme, which is a way of converting information into a form that can only be decoded by those who are given permission to access it [3]. The Equifax breach occurred because the company failed to install security updates in its software, creating an exploitable vulnerability [4]. The data accessed should have been heavily encrypted and therefore protected from attackers. However, there is a strong consensus that the methods by which Equifax encrypted its data were ineffective at best, and nonexistent at worst [4].

Equifax's negligence should not detract from the importance of effective data security in the twenty-first century. It is critical to recognize that the strength of a single encryption scheme can be the difference between a secure nationwide network of personal information, and the constant fear of becoming a victim of identity theft, a fear with which 143 million Americans must now live their lives. The National Academy of Engineering lists data security as one of its "14 Grand Challenges for Engineering in the Twenty-First Century," stating that the industry has been hindered because cutting-edge research and development have only occurred after vulnerabilities have been exposed [5]. Given the number of people who depend on secure data for every facet of their daily lives, taking a proactive approach to inventing new methods of encryption is a necessity for the preservation of contemporary American society.

CURRENT METHODS AND QUANTUM COMPUTING

Unlike Equifax, most of the Internet uses encryption schemes to ensure the privacy of user data in transactions. The two types of encryption most widely used today are the Rivest-Shamir-Adelman cryptosystem (RSA) and the Diffie-Hellman key exchange [6]. Both methods are based on the idea that very large prime numbers are incredibly difficult for computers to use in performing calculations. However, it should be noted that the source of confidence in these methods is that no human has been able to develop separate algorithms capable of efficiently computing their solutions, which would render both methods ineffective [6]. Therefore, though RSA and Diffie-Hellman continue to be the industry standard, their viability as long-term solutions for data security is not guaranteed. [6].

Continued use of these standard methods of encryption is contingent on the status of the development of quantum computers. Whereas today's computers operate on a binary system of either true or false, quantum computing is based on probabilistic calculations, where every possible value is stored at once. This means that a quantum computer possesses the ability to make exponentially more calculations than a regular computer. In July of 2017, Mikhail Lukin, head of the Lukin Group of the Quantum Optics Laboratory at Harvard University, announced that he and his team had successfully built a 51-qubit quantum computer, the largest to date [7]. A regular computer with 51 bits is capable of storing 2^{51} (2 quadrillion) calculations one at a time; a quantum computer with 51 bits, however, can store 2 quadrillion

values simultaneously, demonstrating an exponential increase in computing power.

Since Peter Shor's proof in 1994, it has been known that a quantum computer with sufficient processing capabilities could shatter the RSA and Diffie-Hellman schemes with ease, simply because it would have the power to produce calculations necessary to break each system [8]. Such computational power poses a serious threat to the security of all sensitive data, from personal information to bank records to top-secret government documents [6]. A quantum computer would have no trouble breaking whatever encryption schemes are instituted to keep this information private. The NSA itself has formally stated that the Internet encryption schemes currently in place would be rendered useless by a quantum computer [6]. Innovation in data encryption is a serious necessity if security is to match the ever-increasing availability of computational power.

LATTICE-BASED CRYPTOGRAPHY

Lattice-based cryptography has recently emerged as a promising method of data encryption in a world of quantum computers. Lattices are collections of points organized into one or more sets of information [9]. The visual representation of related points, with connections drawn between them, resembles a lattice, like on a fence. I have included a visual example of a lattice in the Appendix for further understanding.

Lattice-based encryption is founded on the construction of a complex lattice, requiring that highly difficult problems be solved to decrypt a message. Difficult problems can be created with relative ease because lattices can become highly convoluted when represented visually. First developed in the 1980s, lattice-based encryption was initially too inefficient to act as a legitimate improvement in the field of data security [6]. Interest in lattices diminished, but various teams of researchers continued their attempts to develop improved lattice schemes [6]. In 2005, Oded Regev of New York University's Courant Institute of Mathematical Sciences eventually proved that an encryption scheme based on the most difficult lattice problems, known as learning with errors (LWE), is secure against quantum computers [10]. Just as quantum computers use probability to increase computing power, LWE requires a computer to solve a set of equations to a small error, using probability to determine all possible answers [10]. Complex lattice problems such as LWE are categorized as non-deterministic polynomial time (NP) hard, meaning there is no known method of determining how long it will take for even a quantum computer to solve them [10]. Thus, lattice problems constructed to be sufficiently difficult can secure data from any possible computing threat currently known.

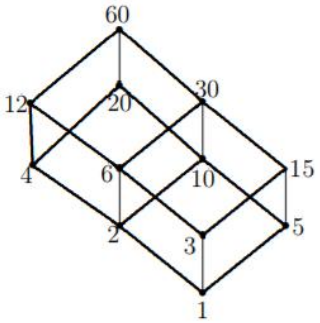
Innovations in lattice-based cryptography over the past twenty years have made it a viable security measure for the future. Security Innovation, a software security company that develops solutions for over one-third of Fortune 100 companies, now owns a lattice-based cryptography algorithm known as N^{th} degree truncated polynomial ring (NTRU) [12]. NTRU is described as "the most battle-tested and efficient quantum resistant algorithm available today" and has been labeled by the Institute of Electrical and Electronics Engineers (IEEE) as the standard method for encryption of financial systems [12]. While lattice-based algorithms such as NTRU do not yet have a large base of users, like the 30,000 companies using RSA, their limitless capabilities demonstrate that as computing, both regular and quantum, continues to progress, lattice-based cryptography will only become more prevalent in the data security community [13].

CONCLUSION: IMPORTANCE TO ME, AND EVERYONE ELSE

Most, if not all, people do not want their personal information to be stolen. It is unfortunate that an event the scale of the Equifax breach was necessary to conduct in-depth research into how personal and financial data is handled. I now see data security as an ever-present issue that we often dismiss as a foreign concept with which we do not have to concern ourselves. We falsely believe that threats to our personal information will be visible before they are executed, allowing a period of time for a response. We blanket ourselves with a false sense of security, and remain blissfully ignorant as mistakes are silently exposed. I suspect this attitude was widespread throughout the ranks of Equifax, and directly contributed to the exploitation of the vulnerabilities in its system.

Lattice-based encryption schemes have been presented as a solution which will hold strong with the development of quantum computing, but one satisfactory method of security does not ensure complete safety. The breach on Equifax was entirely preventable, but the fact that the data of all those affected was concentrated at a single point of failure means that the damage done was maximized [2]. It is necessary for the data security community to assume a preemptive approach to innovation of security measures so there is no possibility of exploiting a single point of failure. Besides developing and innovating new methods of encryption, professionals must make a greater effort to educate the public on the everyday actions we can take to secure our information. It may be too late for the 143 million people impacted by the Equifax breach, but improved education regarding data security is crucial in preventing an incident of this scale from affecting future generations of Americans.

APPENDIX



This is a lattice of integer divisors of 60, ordered by "divides." If one started at a different point in the lattice, it would represent the integer divisors of that number instead. 30, 20, and 12 are directly connected to 60 because those numbers are integer divisors of 60 that are not integer divisors of another number. The number 15 is not directly connected to 60 because it is also a divisor of 30 [14].

SOURCES

[1] G. White. "A Cybersecurity Breach at Equifax Left Pretty Much Everyone's Data Vulnerable." The Atlantic. 09.07.2017. Accessed 10.23.2017. https://www.theatlantic.com/business/archive/2017/09/equifax-cybersecurity-breach/539178/

[2] A. Jeffries. "It's worse than you think: The Equifax breach shows the dystopian gap between wealth and competence in America." The Outline. 10.03.2017. Accessed 10.29.2017. https://theoutline.com/post/2366/it-s-worse-than-you-think

[3] N. Lord. "What is Data Encryption?" Digital Guardian. 07.27.2017. Accessed 10.23.2017. https://digitalguardian.com/blog/what-data-encryption

[4] A. Woodie. "Following Equifax, Focus on Database Encryption." IT Jungle. 09.20.2017. Accessed 10.23.2017. https://www.itjungle.com/2017/09/20/following-equifax-focus-database-encryption/

[5] "Secure Cyberspace." National Academy of Engineering Grand Challenges for Engineering. Accessed 10.28.2017. http://www.engineeringchallenges.org/9042.aspx

[6] N. Wolchover. "The Tricky Encryption That Could Stump Quantum Computers." Wired Magazine. 09.19.15. Accessed 10.23.2017. https://www.wired.com/2015/09/tricky-encryption-stump-quantum-computers/

[7] P. Caughill. "A New Breakthrough in Quantum Computing Is Set to Transform Our World." Futurism. 07.28.2017. Accessed 10.27.2017. https://futurism.com/a-new-breakthrough-in-quantum-computing-is-set-to-transform-our-world/

[8] P. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20-22, 1994, IEEE Computer Society Press, pp. 124-134. Accessed 10.23.2017. https://arxiv.org/abs/quant-ph/9508027

[9] D. Micciancio, O. Regev. "Lattice-based Cryptography." Post-Quantum Cryptography. 07.22.2008. Accessed 10.29.2017. https://www.cims.nyu.edu/~regev/papers/pqc.pdf

[10] O. Regev. "The Learning with Errors Problem." Proceedings of the 2010 IEEE 25th Annual Conference on Computational Complexity. 06.09.2010. Accessed 10.28.2017. http://www.cims.nyu.edu/~regev/papers/lwesurvey.pdf

[12] "Security Innovation Announces Special Pricing on Quantum Resistant NTRU." Security Innovation. 05.06.2016. Accessed 10.29.2017. https://www.securityinnovation.com/company/news-and-events/press-releases/security-innovation-announces-special-pricing-on-quantum-resistant-ntru

[13] "RSA Customers." RSA. 2017. Accessed 10.29.2017. https://www.rsa.com/en-us/customers

[14] H. Reiter. "Just the Factors, Ma'am." University of North Carolina. 2007. Accessed 10.30.2017. http://math2.uncc.edu/~hbreiter/m6105/Divisors.pdf

ACKNOWLEDGEMENTS

This writing assignment, and many others, would not be possible without the fantastic editing of Avocet Greenwell. Her comments have helped me to become a more disciplined and well-rounded writer in addition to immediately improving the quality of my writing. I am extremely grateful for the time that she has spent revising my work.

I guess it is only appropriate to thank my terrible fantasy football teams for giving me the time to work on this writing assignment. By making me lose all desire to watch and enjoy football on Sundays, fantasy football has allowed me to commit longer periods of time to conducting detailed research and writing drafts for this assignment. Thank you, me from the past, for being embarrassingly awful at fantasy football.