December 9, 2016

Towards a Secure, Decentralized Future

Anthony Wittemann
University of Southern California
awittema@usc.edu

Abstract

In this paper, I focus on the current state of information security and the problems the security community faces today due to our reliance on centralized computer systems architecture, and the problems society will face in the near future due to the rapid development of quantum computers which can break the encryption upon which we rely daily. But fear not! I propose solutions to these two problems based on work done by prominent researchers. Finally, I will provide some practical recommendations for both small organizations and individuals, both now and going forward. The goal of this paper is to inform people, regardless of technical background, about the security of their data, and what can be done to protect it.

1. Introduction

1.1 Centralization vs decentralization

Paranoia and the fear of insecurity of any kind is omnipresent amongst people in Western Society. Currently we turn to authoritative figures to provide that security, be it Google and Facebook with our personal data, hospitals with our health data, banks with our money or the Government with its police force, military, TSA, NSA, etc. This is the data equivalent of putting all your eggs in one basket and trusting a single goose with guns to protect not only your eggs, but everyone else's eggs. Ignoring the potential for abuse of this power by these authorities, this trust in centralized authorities still poses a major security threat because data stored on a single server (nest of eggs) provides a single point of attack for malicious hackers who can take advantage of this for all sorts of malicious activity further described in the next section. The opposite of a centralized architecture is naturally a decentralized architecture in which responsibility for keeping data secure is handled by a large connected network of computers that all adhere to a common protocol. Decentralized computing and data storage solutions are beginning to rise in popularity due to the technological breakthrough called the blockchain introduced by

Bitcoin. Blockchain has generated a lot of interest due to the vast number of use cases including secure distributed file storage, secure sharing of electronic medical records, and of course cryptocurrencies, none of which require a central authority.

1.2 Encryption and quantum computing

Encryption was originally used for thousands of years to send messages between commanders in battle so in case the message was intercepted, the enemies would not be able to understand the contents of the message. Today as a society we rely on encryption, not only to reading private messages, but to prevent people from accessing a wide variety of private data on the internet and on computers including pictures of family, financial statements, company secrets, calendars, contacts and much more. Common encryption used today can be broken or significantly weakened by quantum computers. Quantum computers take advantage of a physical phenomenon called superposition to allow them to search through the entire possible space for any given problem and find the optimal solution instantly. This can be used to solve a number of computationally difficult problems such as predicting how proteins will fold, object recognition, running Monte Carlo simulations and solving a host of optimization problems[6]. For encryption, this means that asymmetric encryption (RSA) can be broken using Shor’s algorithm and symmetric encryption can be significantly weakened[7].

2. Problem

2.1 Today

All the centralized authorities mentioned in the introduction are susceptible to several kinds of attacks, including DDOS, which prevents the servers of these organizations from receiving and responding to requests from users. This means that if hackers target DNS providers, they could knock out internet access entirely, not just one site, like what happened in the Dyn hacks. This is not just a matter of huge inconvenience, but can also be a matter of life or death if hackers choose to target the centrally stored data and computers used by hospitals, militaries and utility providers.

Aside from the problems caused by centralized computing and data storage, another major data security problem today is the lack of encryption use and poor security practices of everyday people. For example, all text (SMS, MMS) messages are unencrypted. Additionally, 73% of online accounts are protected by a duplicate password and 95% of people share at least 6 passwords[9] (lots of them over unencrypted SMS!!).

What's even more concerning is that many forms of encryption broken by NSA today with their massive budget by using brute force on classical computers to calculate large prime numbers that would commonly be used by RSA and other encryption algorithms[1]. The NSA has also installed hardware backdoors on processors[8], routers and other hardware that not only allow them access, but anyone else access who can figure out how to get in. As if that's not enough, with their program XKeyscore, the NSA can collect nearly all data on users' online activity[2]. I won't delve too deep into the details of what the system is capable of, but some of the abilities are truly terrifying including the ability to track facebook messenger chats given a username and a time range, viewing all the content of emails sent to anyone as long as a "reason" is provided, and accessing all the websites a person has visited. Even if you aren't bothered by this activity and trust the NSA to be judicious with the power they are given, you should still be concerned because if they were to be hacked, everyone's data would be made available for anyone else to abuse. Here, we find a potential security vulnerability due not only to the potential for encryption being broken, but also due to the fact that the NSA stores all this data on centralized servers.

2.2 In the near future

Even assuming the NSA can't crack encryption today, there is still the unavoidable day upon which a quantum computer will fall into malevolent hands and used to break encryption en masse. How can this happen? As stated in the introduction, a sufficiently powerful quantum computer can use Shor's algorithm to break RSA and DSA Encryption, while weakening Symmetric encryption; namely, a quantum computer can search through a space of size 2^n in time $2^{n/2}$. This means that a 128-bit AES key would be demoted back to the strength of a 64-bit key. Similarly, a hash function with an output of n bits would resist preimages with strength $2^{n/2}$ and collisions up to $2^{n/3}$ (figures with classical computers being 2^n and $2^{n/2}$, respectively). SHA-256 would still be as strong against collisions as a 170-bit hash function nowadays, i.e. better than a "perfect SHA-1"[10].

Enough of the technical details. To reiterate some of the implications this has for everyday data available online: iMessages, emails, documents, credit card numbers, web connections, health records, financial statements, location history now can all be instantly accessed in seconds without permission. This will be the case unless all services that store consumer and corporate data upgrade to post-quantum encryption, which I will explain in greater detail in the Section 3.2. However, given historical precedent, I find it highly unlikely that all companies will take updating their encryption seriously as many businesses run on outdated software and are reluctant to incur extra operational costs on “just another upgrade”.

Before I get too carried away, you might ask how far away in the future is this quantum apocalypse? I believe this will happen within the next 15-20 years, and experts say within 15-30[4]. Quantum computing power increased 300,000 times over the course of 2 years when D-Wave went from a 128-bit architecture to a 512-bit architecture and the overall development in the space mirrors the exponential growth of Moore’s Law[5]. Quantum computers have already used Shor’s algorithm in practice to factor numbers up to 21[3]. This may seem quite tiny, but again, the progress in this space has been exponential.

Another trend that should be taken into consideration when evaluating the potential security threat quantum computers pose to data encrypted using today’s standards is that the amount of data being collected is also growing exponentially. Concretely, the amount of data being generated daily in 2020 is estimated to be 44 times what it was in 2009[11]. If that growth didn’t suprise you, perhaps the fact that 90% of the world’s digital data in 2013 was generated in 2012 and 2013 alone[12] and that trend has not slowed down at all in the past few years. Granted not all this data is being generated is labeled and clean, but progress is being made to obtain insights from unlabeled data as well like some of the work done by researchers at Carnegie Mellon to drastically reduce the error rate when analyzing unlabeled data[16]. All this means that not only will there be more data to secure, but also more demand for that data to be processed and analyzed, further incentivizing governments and corporations to develop quantum computers to tackle the mind boggling challenge of making sense of all this new data.

3. Solution

3.1 Decentralization

One of the major appeals of a distributed architecture is that the network becomes much more resistant to DDOS attacks, which spam the network with requests in an attempt to crash the servers. When data is stored on millions of nodes (computers) located all over the world, the effect of DDOS attacks becomes negligible even unnoticeable.

Moreover, decentralized networks also distribute authority across the population of people and organizations running the servers instead of all the authority resting with one or a few elite companies or government departments like the NSA or Google. A lot of the appeal of the internet was the democratization and rapid dissemination of information to people around the world. However, for this vision to be fully realized, the control of the data also need to be spread across the entire population. The advantages of decentralized systems can be demonstrated by the success of torrenting despite the efforts of media conglomerates and governments around the world to take down copyrighted material. Instead of all the pirated music being stored on Limewire, which was easily shut down, small parts of songs are stored on millions of computers around the world. This decentralized network is much more resilient to attacks and security breaches than its centralized counterparts.

Another instance of decentralized networks succeeding is cryptocurrency. Instead of the supply of a fiat currency being controlled by a secret, terrifyingly powerful, unelected centralized authority like the Fed, ECB or the People’s Bank of China, the supply of Bitcoin is predetermined by a protocol which has been adopted by millions of “miners” or nodes in the network who collectively contribute their computing power to validate transactions for which they are rewarded. The exponential growth of daily volume on cryptocurrency exchanges and accelerating adoption rate over the past 7 years indicate that Bitcoin and cryptocurrency is not just an experiment, but a definitive move towards decentralized control of a global internet money supply that is here to stay.

Despite the above advantages of the decentralized architecture used by blockchain technologies and cryptocurrencies, even they, in their current state are rendered insecure to the otherworldly capabilities of quantum computers (although bitcoin and other cryptocurrencies can easily be upgraded to protect against quantum computing attacks using Lamport signatures[13]). As stated earlier, any system that relies on RSA, DSA or elliptic curve encryption, including blockchain, fails in seconds against the astronomical computational power of quantum computers.

3.2 Post Quantum Cryptography

One solution would be to stop allowing your data to be stored online, or simply being more cognizant about what data you have online about you or your company. Unfortunately, there is still a lot of data stored online about companies and individuals without their explicit consent. This trend will only accelerate as more companies realize the huge competitive advantage of making data driven decisions based on insights provided by machine learning algorithms. Again, we should be reminded by the activity of our friends at the NSA about how insufficient the above proposed solution is. At this point, the security of data appears to be a lost cause, but hope remains thanks to the work of brilliant researchers developing post quantum encryption algorithms.

A few of the algorithms proposed by experts include AES-256 bit symmetric encryption, Public Key Encryption with McEliece with binary Goppa codes using length n = 6960, dimension k = 5413 and adding t = 119 errors, instead of RSA or ECC or Public Key Signatures using cryptographic hash functions such as SPHINCS-256[15]. All these options would offer 2^{128} post quantum security as opposed to the 2^{64} post quantum security example in section 2.2. These encryption schemes should not only be adopted by large corporations and governments, but also individuals because they are the most powerless in case of a mass security attack and cannot rely on large organizations to ensure the security of their data.

One might wonder why we should worry about switching to post quantum encryption when the threat of sufficiently powerful quantum computers is estimated to be at least 15 years away? Daniel Bernstein of the University of Illinois offers us 3 good reasons: “We need time to improve the efficiency of post-quantum cryptography, time to build confidence in post-quantum cryptography, and time to improve the usability of post-quantum cryptography.”[14] He argues that we simply aren’t ready to handle the threat of quantum computers yet and need time to develop and test these algorithms before they are needed.

4. Practical Recommendations

4.1 For small corporations and governments

Make sure employees are properly trained and understand the importance of security! It does no good to have the most advanced security system only to have it overridden by an impatient employee. If you are part of a large corporation, hire an expert to ensure your company follows security best practices. For small businesses that care about security, I have below a quick start guide of tools to use and practices to follow.

Phones:

- Blackphone 2 or Blackberry

Internet connection:

- VPN, one that does not log data such as IVPN
- Torbrowser for sensitive web search
- disable trackers, scripts (ghostery, HTTPS everywhere)

Messaging:

- Signal, NO SMS OR MMS

Two Factor Authentication:

- Authy or Google Authenticator

Password Manager:

- Store passwords and Keys Internally
- KeePassX or Encryptr

Email:

- Thunderbird, GnuPG, Enigmail
- Protonmail (auto destruct messages after some time)

Team communication, file sharing:

- Semaphor by Spideroak

Data Backup:

- SpideroakOne (you have the keys)

4.2 For individuals

For many individuals, the level of security used by corporations is either not something they can afford or simply don't have the time or motivation to inconvenience themselves. In order for many individuals to strongly protect their privacy, they would also need to conduct a massive overhaul in the services they use and their daily habits with how they share their data. That prospect is not appealing to the majority of people who would rather spend time doing something they enjoy. Since this is the case, the recommendations made in this paper will be targeted towards this larger demographic. People concerned about their privacy beyond a basic level can download the tor browser, connect to a vpn and have at it. For the rest of the folks, the below recommendations should take no more than an hour of your time to set up.

4.2.1 Everyday habits

- Don't share unecessary information, especially with parties you do not trust.
- *Think of your data as being naked when it is unencrypted*. Put some clothes on it and make sure it's encrypted.
- Use secure password managers like KeePassX

- Use encrypted messaging app like Signal, iMessages instead of SMS or MMS
- Set up 2 factor authentication
- Install HTTPS everywhere and adblock extensions
- Bug your local representation to dismantle the NSA and destroy all the data they've collected on American citizens

4.2.2 Things to be aware of in the future

- Before quantum computers start breaking encryption en masse:
    - When possible, secure offline copies of your data and delete the online copies
    - Upgrade encryption to proposed standards
- For decentralization:
    - Start utilizing services like IPFS (Interplanetary File System) to store and share large online files instead of Dropbox, Google Drive, etc
    - When possible, use secure, preferably anonymous (ZCash, Monero, Dash) cryptocurrencies instead of cash or credit card.

References

Articles:

[1]http://arstechnica.com/security/2015/10/how-the-nsa-can-break-trillions-of-encrypted-web-and-vpn-connections/

[2]https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

[3]http://arstechnica.com/security/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocolypse/

[4]http://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment

[5]https://gcn.com/articles/2013/09/10/dwave-quantum-computing.aspx

[6]http://www.dwavesys.com/quantum-computing/applications

[7]https://security.stackexchange.com/questions/48022/what-kinds-of-encryption-are-not-breakable-via-quantum-computers

[8]http://www.eteknix.com/expert-says-nsa-have-backdoors-built-into-intel-and-amd-processors/

[9]http://associationsnow.com/2016/02/study-95-percent-of-people-share-up-to-six-passwords/

[10]https://security.stackexchange.com/questions/48022/what-kinds-of-encryption-are-not-breakable-via-quantum-computers

[11]http://www.csc.com/insights/flxwd/78931-big_data_universe_beginning_to_explode

[12]https://www.sciencedaily.com/releases/2013/05/130522085217.htm

[13]https://en.bitcoin.it/wiki/Quantum_computing_and_Bitcoin

Papers:

[14] Introduction to post-quantum cryptography Daniel J. Bernstein 9783540887010

[15] Initial recommendations of long-term secure post-quantum systems Daniel Augot, Lejla Batina, Daniel J. Bernstein, Joppe Bos, Johannes Buchmann, Wouter Castryck, Orr Dunkelman, Tim Gu ̈neysu, Shay Gueron, Andreas Hu ̈lsing, Tanja Lange, Mohamed Saied Emam Mohamed, Christian Rechberger, Peter Schwabe, Nicolas Sendrier, Frederik Vercauteren, Bo-Yin Yang 7. September 2015 Revision 1

[16] Estimating Accuracy from Unlabeled Data Emmanouil Antonios Platanios, Avrim Blum, Tom Mitchell