7TUNNELS

PRIMER

7TUNNELS ENCRYPTION

THE BASICS

7TUNNELS®

Park City · Utah · USA info@7Tunnels.com

7TUNNELS PRIMER

7TUNNELS ENCRYPTION

$7.35M

The average cost of a data breach to U.S. companies per the Ponemon Institute [1]

53%

U.S. businesses that reported being hacked in 2017 [2]

$650B

2018 cybercrime profits from theft and trade of secrets, IP and data [3]

2018

7Tunnels develops working applications of its technology

2019

DuPont completes long-term testing of 7Tunnels systems and selects AG7s for its fleet of aircraft

Data Encryption: What's At Stake

For businesses today, cyberattacks aren't just a threat—they're an inevitability. For every widely publicized cyber breach like the 2014 Sony Pictures hack and the Equifax hack of 2017, there are hundreds—if not thousands—of devastating smaller-scale attacks yearly.

The results for targeted companies are distressingly familiar: irretrievable financial losses, stiff fines and penalties, and the damage to both customer trust and company value. Industry forecasts predict that the damage costs associated with cybercrime will reach $6 trillion annually by 2021,[4] a number that will dwarf the total worldwide profits of the illegal drug trade.

Moreover, companies are being held increasingly accountable for protecting the personal information of their customers and clients. Colorado and California have enacted strict privacy and cybersecurity laws, and Sen. Ron Wyden of Oregon's proposed Consumer Data Protection Act calls for prison sentences of up to 20 years for CEOs who fail to adequately secure their customers' private data.

"Cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world." **- Ginni Rommety, Pres. & CEO - IBM**

Current Standards and Future Flaws

The two main forms of digital encryption used today are symmetric (shared secret key) and asymmetric (public key). Most online communications involve a combination of the two: asymmetric encryption to securely share a secret key and symmetric encryption using that shared secret key to encode the data sent.

The Advanced Encryption Standard (AES) is a symmetric block cipher algorithm used as the standard by the U.S. Government. Rivest–Shamir–Adleman (RSA) is the primary asymmetric encryption standard. While the mathematical-based algorithms powering both AES and RSA are largely impervious to brute force attacks from classical computers, the rapid advent of quantum computers threatens the security of both standards.

Last year, China broke ground on the $11 billion National Laboratory for Quantum Information Sciences in the Anhui Province and began construction of a quantum fiber link that will eventually connect the cities of Beijing, Shanghai, Jinan and Hefei.

The Russian Quantum Center, which is a project of the private- and government-funded Skolkovo Institute in Moscow, has spearheaded research that has led to critical breakthroughs in general quantum computation and qubit entanglement.

It's too early to tell whether it will be China or the U.S. that comes out on top in the quantum arms race... But the money China is pouring into quantum research is a sign of how determined it is to take the lead. **- MIT Technology Review**

The U.S. is attempting to keep pace. Google, IBM and Intel have invested heavily in quantum research and are developing quantum technologies concurrently. In the public sector, the U.S. Department of Energy's 2019 budget request included $105M "to address the emerging urgency of building U.S. competency and competitiveness in the developing area of quantum information science." [5]

Meanwhile, cybercriminals and large state and non-state actors are already intercepting and stockpiling encrypted communications and the key exchanges used in encryption.[6] Once large-scale quantum computers become operable—and most experts agree it will happen within the next decade—that data will be decrypted and leveraged against its rightful owners.

***"Anyone that wants to make sure that their data is protected for longer than 10 years should move to alternate forms of encryption now."* - Arvind Krishna, Director of IBM Research.**

The 7Tunnels Encryption Solution

7Tunnels creates a secure, quantum-proof tunnel between users and exclusive endpoints hosted in U.S.-based cloud data centers through which communications can safely flow. The 7Tunnels technology doesn't simply encrypt the contents of emails, web browsing, streaming video, VOIP calls, file transfers, etc., but protects all of the above—and anything else flowing through the tunnel—by securing communications at the network packet level.

The 7Tunnels patented technology is, in its simplest form, a digital version of the one-time pad (OTP) system. Invented in 1882 and widely used during World War II, the OTP has been proven to be unbreakable when used correctly. The sender and receiver of a message use a pre-shared key to encrypt and decrypt the message, after which the key is destroyed. (During WWII, those keys were printed on actual paper pads, hence the name "one time pad").

Encryption Beyond Mathematics

While current digital encryption methods use difficult mathematical algorithms such as the factorization of the product of two large prime numbers or the algebraic structure of elliptic curves to create a secure method for sharing a secret key, 7Tunnels uses sequences of true random numbers (TRN) generated by unpredictable physical processes to create a provably secure encryption system. Those processes include photon behavior, zero-point energy in a vacuum, radioactive decay, transistor band gap noise and measurement of shot noise, each of which can be used to ensure absolute true random numbers with no pattern, algorithm or standard method of creation. Because the keys are truly random, the encryption is guaranteed to be secure.

7Tunnels key libraries are loaded onto 7Tunnels' proprietary devices, including the AG7 for aviation use, the PG7 for personal portable use and the OG7 for home office use, creating impenetrable communication tunnels between those devices and secure cloud endpoints, allowing secure communications with any desired recipient. Encryption keys are discarded after use, to ensure security, and the devices are replaced before key libraries are ever fully exhausted. 7Tunnels' unlimited data model allows users to communicate with no concern for added costs or limits on replacements.

Proven Solutions

7Tunnels products and technology have been successfully field tested and are currently being used for real-world applications by Fortune 50 companies. The devices pair seamlessly with existing wired or wireless Internet connections to create a new, easily identifiable and fully secure network. The information sent or received between a 7Tunnels device and the cloud-based endpoint is protected now and into the future. No software or app downloads are required, and no special clicks or settings are needed to encrypt or decrypt communications. The encryption and decryption processes run transparently in the background.

In a world of diminished expectations and lowered "good enough" standards for everything from food quality to technological performance, 7Tunnels' quantum-proof encryption is the only sensible choice for protecting critical and proprietary corporate data.

[1] Ponemon Institute: *2018 Cost of a Data Breach Study* https://www.ibm.com/downloads/cas/861MNWN2
[2] *Insurance Journal*, September 29, 2017 https://www.insurancejournal.com/news/national/2017/09/29/465954.htm
[3] *Hashed Out*, September 27, 2018 https://www.thesslstore.com/blog/2018-cybercrime-statistics/
[4] *Forbes*, July 13, 2017 https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#123794cf4947
[5] U.S. Department of Energy, February 12, 2018 https://www.energy.gov/sites/prod/files/2018/02/f48/DOE-FY2019-Budget-Fact-Sheet.pdf
[6] Official Website of Congressman Will Hurd, June 23, 2018 https://hurd.house.gov/media-center/in-the-news/best-piece-legislation-dc-about-quantum-computing