WHITE PAPER

Quantum Resilient Encryption Technology versus Ransomware

James Castle
Flavia Kenyon

Global Foundation For Cyber Studies And Research®

About the Authors

James Castle is the CEO/CISO/CSO of Terranova TCU Communications Incorporated, a manufacturer of commercial cybersecurity products in quantum resilient encryption, in microprocessor architecture and in secure communication solutions. The company is multi-sector specialized and offers direct services in cybersecurity, aerospace, maritime, defense, unmanned vehicles, and in communications.

James is also the Chairperson of the Cyber Security Global Alliance (CSGA), which operates alongside Terranova Defense NFP and explores the possibility of creating cybersecurity legislation for global systems with a team in nine countries worldwide. He is a Canadian Ambassador for an EU Commission think tank based in Brussels, representing over 30,000 high-profile technology and defense companies in 64-countries globally.

James has worked as a volunteer in business mentorship, has run recreational programs in his community over the last three years, and is currently involved as a volunteer taskforce member both in UAVs and First Responders with the Canadian Standards Association.

He started the Terranova Group of Companies in 2014, in public safety and emergency management. In 2018 and later, he was invited to speak as a Special Witness before the Standing Committee on Transport, Infrastructure and Communities (TRAN) at the House of Commons in Ottawa as an expert in unmanned vehicles and the future of drones in Canada.

Terranova Defense Solutions, one of the companies owned by James Castle, was elected as one of Canada's Top Defence Companies in both 2020 and 2021 by the Canadian Defence Review Magazine and over the years it has expanded into a conglomerate of corporations from defense systems to advanced cybersecurity manufacturing to innovation hub technologies, including cybersecurity managed services, cyber ranges and incident management, aerospace systems and in smart city developments for climate change initiatives.

Flavia Kenyon is a leading British barrister. She holds an impressive and varied portfolio of national and international financial crime cases.

Flavia advises start-ups, SMEs, and individuals on cyber fraud litigation and regulatory issues emerging from new technologies, such as blockchain, decentralised finance and crypto-currencies. She advises companies on how to respond to ransomware attacks, and advised the BBC on the future of cyber attacks on media organisations.

Flavia is frequently instructed to defend in complex, multi-handed fraud trials with an international dimension. She has defended in insolvency prosecutions, money laundering, cyber fraud, fraudulent dealing, international conspiracies to defraud financial institutions, and conspiracies to making articles to use in fraud, ponzi schemes, and fraud by misrepresentation.

She has developed a strong profile in government advisory and ambassadorial work, recently advising the Romanian Embassy in London on issues of state immunity and commercial property. Her advisory work also extends to non-governmental organizations, such as Transparency International, for whom she acted in an international case of bribery of public officials in the oil and gas industry in Senegal.

Flavia is the author of numerous legal articles and is a legal commentator. She was educated at Oxford University, and called to the Bar in 2005. She is fluent in English, French, and Romanian. Flavia is listed as a leading individual in both national directories of excellence, Chambers and Partners UK and The Legal 500.

About GFCyber

Global Foundation for Cyber Studies and Research is an independent, non-profit and non-partisan policy research think tank for Cybersecurity studies, located in the Washington D.C, USA.

Cover Design & Styling: Amanullah Quadri

Citation Style:

James C., and Flavia K. “Quantum Resilient Encryption Technology vs. Ransomware”, Global Foundation for Cyber Studies and Research, July 2021.

Quantum Resilient Encryption Technology vs. Ransomware

Introduction

In the digital era of increasing cyber-attacks, the Cyber Security Global Alliance has investigated real solutions. A super-cluster company in Canada has created possibly the first true answer to countermeasure ransomware. This countermeasure (which has been proven by a leading Canadian Polytechnic University in Saskatchewan) was designed and manufactured to be the world's first superior commercial-grade quantum resilient encryption software. Originally designed for the military and commercial drone communications, this technology was reconfigured into a Windows-based Enterprise technology that is compatible with Linux, Android, and Apple technologies.

This technology was manufactured, designed, and built by our Canadian business partners CEW Systems Canada and Terranova TCU Communications, who are working together in advanced manufacturing of cybersecurity products. As the world plummets into cyber and Ransomware attacks, the world needs a Superhero and that Superhero is CEW Systems Canada and its encryption tool - Bi-Symmetric handshake.

Terranova TCU Communications has already expanded into the unmanned and autonomous vehicle sector automobile industry, aerospace, and defense, and into future technologies such as hypersonic technologies and missile defense systems. Terranova TCU Communications is the future defender against electronic warfare and the next generation of quantum resilient cyber defense systems.

CEW encryption solutions is defined as a quantum resilient encryption algorithm designed to encrypt and decrypt data that is being transmitted via the Bi-Symmetric handshake. The solution is ideal for all unmanned as well as manned vehicle communication to prevent cyber-attacks from all computers, including supercomputers and upcoming quantum computers. These computers will soon be able to execute brute-force attacks against intercepted encrypted data. On December 3rd, 2020, in the journal Science, scientists from China built a photonic quantum computer that they claimed to be ~10^14 times more powerful than the third most powerful supercomputer in the world.

The integrated cybersecurity solution proposed within will include internal and external communication encryption using CEW Systems Canada's Bi-Symmetric Encryption software. It uses challenge and counter challenge codes to exchange public keys using private keys. This ensures listening parties (potential attackers) will be unable to read the contents of the encrypted data and/or to send unwanted commands designed to interrupt on-boards activities or systems.

Asymmetric Encryption is Vulnerable

In encryption, there is a little-known issue that both cryptographers and hackers know about but is almost never talked about. Asymmetric keys use public/private key pairs, which are heavily relied upon because one can easily send public keys which if intercepted/hacked can be used to encrypt data. Only the holder of the private keys can decrypt the data.

So let's think about this statement for a minute and its consequence in the context of a ransomware attack: anyone with a public key can encrypt data with it. Essentially, what this means is that anyone who intercepts a public key, can pretend to be another person, and spoof the receiving device or person. This is one of the main means hackers use to get into the backdoor of servers.

Let's consider an example to best illustrate this. In typical encryption descriptions, Farah, and John exchange secret information while Max tries to intercept the encrypted data. So, Farah sends John a public key, which John uses to encrypt his data, but since Farah is holding the private key, only she can decrypt the message. Public keys will prevent Max from finding out what messages John is sending to Farah, but it does nothing to stop Max

from pretending to be John and sending Farah a misleading message. With public key encryption, there is no true secure means by which to help Farah ensure that John, and only John, can encrypt and send her information.

Let us take another pertinent example, the Internet or Things (IoT) technologies, such as drones, garage door openers or automobiles. Each of these devices sends and receives data through easily intercepted radio transmitting technology. A drone has been programmed to decrypt four commands, “Up”, “Down”, “Left” and “Right”. The drone would be programmed with more complex command codes but let us say the programmers assumed the encryption would protect them. The drone receives a request from the drone pilot, named Alice, to send over an asymmetric key upon start-up and transmits a post quantum level public key. Any person, say Malory, within transmitting range can intercept the public key. Malory will not be able to decrypt the command codes Alice is transmitting to the drone. However, because Malory has intercepted the public key, and since anyone can encrypt data using that public key, she can easily encrypt and send her own commands to the drone and cause the drone to, for example, crash into a nearby hospital.

Another example applies to garage doors. If Erik intercepts a garage door public key, for a large underground parking lot, he can sneak in behind Sarah’s car and Sarah will have no idea the public key was used by Erik to stalk her via unapproved access. This is the same in the case of cars. If Alice connects her smart phone to the car and Malory intercepts the public key, Malory could take over unwanted functions of the car.

There is a real-world vulnerability, which currently exists and results in extremely regular data breaches caused by the repeated use of simple and easy to remember usernames and passwords. If corporation “A” is hacked and all the unencrypted usernames and passwords are stolen, there is nothing to stop hackers from reusing the stolen usernames and passwords and logging into other large corporate online accounts. This is how the Disney Plus service was hacked during their initial start-up.

In the example of unmanned drones, determining the identity of the message/command sender is paramount. Dr. Coupal described in his paper how the Bi-Symmetric Encryption works:

> *“Bi-Symmetric Encryption uses a unique and novel handshake incorporating encrypted session key combinations, allowing user’s login credentials, biometric data, credit card data, or command/activation codes to be quickly and correctly processed, without directly transmitting this confidential data[1]. The plug-and-play, hybridized encryption system employs concepts like asymmetric encryption meshed with more secure symmetric encryption. A significant difference from commonly employed asymmetric encryption is that during the initial handshake to set up communication, no vulnerable data is exchanged. Should the sender key communication be intercepted by a hacker, they still cannot pretend to be the originator of the communication to the receiver.”*

You cannot decrypt, what you cannot intercept

The Bi-Symmetric handshake provides a new and novel encryption feature, not found in any other encryption system. The handshake was setup specifically to exchange encrypted, randomly generated data instead of login credentials such as passwords and command codes, while still achieving the ability to ascertain the authentication of both parties. If the login data, command codes or credit card data are not transmitted, how can it be intercepted and decrypted?

“During the initial handshake, private keys are generated from or found in the form of login credentials, credit card information, biometric data, or other personal credential information or pre-shared private keys, which are then used to start the handshake and are never actually transmitted”.
~ Dr. Cyril M. Coupal

[1] Please visit http://saskpolytech.ca/about/applied-research-and-innovation/DIReG.aspx

Third Party Academic Review

At Terranova TCU Communications we understand the claims we are making about our encryption API software sound extremely ambitious. Our software was developed over several years starting in 2017 when we watched a news documentary on how easy it is to break into key fob enabled vehicles. A thief could simply walk up with a tablet and portable transmitter, execute a brute force attack and be in the car in less than 30 seconds. The Bi-Symmetric handshake was specifically designed for encryption of open-air radio communications where command codes are easily intercepted and recorded. The Bi-Symmetric handshake was born out of this realization in which a unique and novel type of handshake can provide an excellent solution, one which is also happens to be quantum resilient.

To authenticate the claims on our encryption software, we engaged the services of the Saskatchewan Polytechnic Digital Integration Centre of Excellence (DICE) group to perform a short NRC-funded analysis on our Bi-Symmetric Hybrid Encryption API System.

Dr. Cyril M. Coupal PhD, ISP, ITCP, Senior Research Associate from the DICE group was kind enough to perform the evaluation. Dr. Coupal's paper is written from the point of view of e-commerce with several mentions of Bluetooth, automotive key fobs, and related radio transmitting technologies, this of course extends to unmanned vehicles. Within this paper we directly quote from Dr. Coupal's third-party academic peer review of our quantum resilient software.

Third Party Academic Review

Ransomware has become a flourishing, global, criminal industry. In just a few years the scale and severity of attacks have grown at an alarming pace as cyber criminals look to exploit cybersecurity vulnerabilities to maximize profit worldwide. It is a crime without frontiers as a single attack can rapidly spread across borders, with devastating effects, an example in point is the 2017 WannaCry ransomware attack that affected 150 countries.

Ransomware is a form of cybercrime, a highly sophisticated, highly lucrative, and evolving white-collar crime that not only risks the personal and financial security of individuals, but also threatens national security and human life. Businesses, schools, governments, hospitals, critical infrastructure and entire cities are now regularly targeted, their networks disrupted, and held hostage.

It is a type of malware – software designed to cause harm to a computer or a computer network for financial profit. The malware is designed to encrypt files on a device, rendering them unusable. Malicious actors then demand ransom in exchange for decryption.

Generally, an attack has two main goals: the primary goal is financial profit, the demand of the ransom payment in cryptocurrency, (usually in BTC) to decrypt the victim's files, and, secondary and subsidiary goal is the theft/ex-filtration of data and the threat of exposing the victim's data on the Internet, including copyright protected trade and industry secrets, highly sensitive personal and non-personal data if additional ransom is not paid. This is called 'double extortion'. Attackers use a victim's data as a bargaining chip, a further vehicle of extortion on the victim for the speedy payment of the ransom, or as an asset to hold on to for later sale, selectively, to other criminal groups, or for later deployment in pursuance of further crime. Because the victim is dealing with criminal gangs, there are no guarantees that, even after having paid the ransom, the data will be safely returned.

By the end of 2019, such was the level and sophistication of Ransomware, that cyber security analysts began referring to it with terms normally used for legitimate business models; a 'service market', a big business market, a 'big game hunting' market for criminal groups run as professional organizations.

The "Ransomware as a service" (RaaS) model in particular allows criminals without technical sophistication to conduct Ransomware attacks anywhere in the world. And, at the same time, technically knowledgeable criminals are conducting increasingly sophisticated attacks fueled by the ransom payments.

- **Current Challenges**
- **Ransom Payments**
- **Lack of legal clarity and certainty/ Sanctions Compliance**

For anyone in the private or public sector who has been the victim of a ransomware attack, the question of whether to pay or not to pay the ransom becomes an existential one. Faced with such a predicament, it is important that a clear and internationally recognized legal framework is put in place that will create legal certainty on such a pressing issue. Presently there is no such legal framework in place. No international or indeed national law enforcement agencies have reached a consensus on whether such a payment should be made illegal, a decision which will undoubtedly involve difficult policy considerations.

Presently, victims agonizing about whether they should proceed to engage with the attackers, do so in a legal vacuum and may expose themselves to unwanted liability if they have not sanctioned to be compliant.

Making a ransom payment per se is not unlawful. However, the current legal position is far from clear, or reliably consistent, due to varying global laws.

The International Sanctions Regime

In the United States, facilitating ransomware payments on behalf of a victim may violate the US Treasury Department's Office of Foreign Assets Control ('OFAC'), issued October 2020. This guidance is particularly relevant to those companies who provide services to ransomware victims, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments, including cryptocurrency exchanges, and money services businesses. It may also trigger legal obligations under the Financial Crimes Enforcement Network (FinCEN) regulations: "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," October 1, 2020.

According to their guidance, OFAC will consider ransomware payments as a sanctions violation if the recipient is on the Specially Designated Nationals and Blocked Persons List ('SDN' List), another blocked person, or covered by comprehensive country or region embargoes.

The broad jurisdictional scope of this guidance is noteworthy: it states that violations by a non-U.S. person that cause a U.S. person to violate any sanctions, or U.S. persons facilitating actions of non-U.S. persons in an effort to avoid U.S. sanctions regulations, are also prohibited. While this guidance may seem straightforward, it raises serious legal issues which have remained unresolved; principally, there is no legal test as to what constitutes 'due diligence' on the part of the victim in determining the identity of the recipient/attacker, and the liability OFAC would assign to each stakeholder.

Furthermore, there is the broad and rather vague scope of civil liability, as OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if he/she did not know or have reason to know he/she was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC. It seems the mere payment of the ransom to a designated person with a sanction nexus may be sufficient to trigger a violation and civil penalty.

The United Kingdom and The European Union

There is a cyber sanctions framework in place in the EU and the UK. On 17 May 2019, the Council adopted Council Regulation (EU) 2019/796, (the "Regulation"), which establishes a framework for the EU to impose sanctions in relation to cyber-attacks that constitute an external threat to the EU or its Member States. The Regulation is broad in scope and is not specific to any particular country, but is intended to catch all external cyber threats. It is of note that the Regulation catches within its scope threats to the information systems relating to the "governance and the functioning of institutions, including for public elections or the voting process". Cyber-attacks against third states or international organizations also fall within the ambit of the framework where necessary to achieve the objectives of the EU's Common Foreign and Security Policy.

The UK played a key part in pushing through the cyber sanction's framework, and it has implemented and transposed the Regulation into domestic legislation, with The Cyber Attacks (Asset Freezing) Regulations 2019, which came into force on 11 June 2019. With the UK's exit from the EU, The Cyber (Sanctions) (EU Exit) Regulations 2020 have been implemented which replace and replicate the 2019 Regulations.

A "designated person" means a person, entity, or body listed in Annex I to the Council Regulation. As of November 2020, a list has been published containing only the names of 8 individuals, and 4 companies.

The UK Regulations adopt the EU restrictive measures to deter and respond to cyber-attacks. These include the freezing of funds and economic resources of persons responsible for, or otherwise providing financial, technical or material support to cyber-attacks or attempted cyber-attacks.

Unlike the American sanctions, the UK sanctions legal framework creates criminal offences for acts done in contravention to the prohibitions. It also creates criminal offences for failure to comply with a request for information and compliance with reporting obligations.

Following the flow of cryptocurrency is a very complex and costly process

Arguably, it is extremely onerous for a victim to identify the payment recipients under the short timelines of a ransomware attack, bearing in mind the decentralized nature of the attack and of the method of payment in cryptocurrency. The demand for the ransom payment in cryptocurrencies adds another layer of difficulty for a victim to be able to trace and identify the recipient and thus be sanctions compliant.

Attackers have become well versed in the use of blockchain with its transparent ledger of transactions by law enforcement and digital forensic agencies in tracing the payments. In order to obfuscate law enforcement and the forensic tracing process, cyber criminals are now using decentralized exchanges (DEX), which by their very nature, do not have a middleman /intermediary, and are extremely difficult to regulate, as opposed to centralized exchanges (CEX), financial entities subject to anti-money-laundering and 'KYC' regulations.

Attackers demand the payments to be made to un-hosted/self -hosted wallets, (wallets that are not hosted with an exchange). An un-hosted wallet is effectively software installed on a computer/ device. The funds are controlled by the individual without the need for an intermediary. Users of un-hosted wallets interact directly with a digital currency system without the involvement of a financial institution, service provider or another intermediary, such as a centralized exchange. Importantly, users of un-hosted wallets can receive, send, and exchange their crypto assets with other un-hosted wallets without revealing their identity. This makes it almost impossible for law enforcement, let alone a victim of an attack to trace the identity of the ransom recipient.

Ransom payments fuel further attacks and are directly responsible for the boom in the ransomware criminal industry

According to the Chain Analysis 2021 Crypto Crime Report, the total amount paid by ransomware victims increased by 311% in 2020, reaching nearly $350 million worth of cryptocurrency. [https://blog.chainalysis.com/reports/ransomware-ecosystem- crypto-crime-2021]

Although there is a strong presumption against making the ransom payment built into both the OFAC guidance and the UK/EU Regulations, there is no legal clarity as to the status of making a payment to an organized cyber-criminal group.
The concept itself profoundly offends the old common law principle of aiding and abetting/assisting in the commission of crime, which in itself is an offence.

There are serious policy considerations to be made here. Despite the fact that no country, including the UK has come forward to criminalize such conduct, the existing money-laundering UK law, namely the Proceeds of Crime Act 2002, ('POCA') does recognize this conduct as unlawful.

There is a strong argument that a person who pays the ransom *"enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person",* cf. section 328 of the Proceeds of Crime Act 2002, ('POCA').

Section 340 of POCA entitled ***'Interpretation'*** provides helpful definitions.
'*Criminal property'* is defined under section 340(3):
" (3) Property is criminal property if-

(a) it constitutes a person's benefit from criminal conduct, or it represents such a benefit (in whole or part and whether directly or indirectly), and
(b) of the alleged offender knows or suspects that it constitutes or represents such a benefit."

'Criminal conduct' is defined in section 340(2) as conduct, which either constitutes an offence in any part of the UK, or would constitute an offence in any part of the UK of it occurred there.

In accordance with section 340(4), it is immaterial who carried out the conduct, or who benefited from it. Section 340(11) defines the offence of money laundering:

"Money laundering is an act which:
(a)constitutes an offence under section 327, 328 or 329,
(b)constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph (a),
(c)constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph (a), or
(d)would constitute an offence specified in paragraph (a), (b) or (c) if done in the United Kingdom"

The prosecution must prove that the accused person knew or suspected that the property is criminal property, (i.e. the proceeds of crime). The threshold for proving suspicion is low: *'suspicion'* was defined by the Court of Appeal in R-v-Da Silva (2006) EWCA Crim 1654 that a person *"must think there is a possibility, which is more than fanciful, that the relevant facts exist."*

There cannot be any doubt that the ransom payment constitutes criminal property, (most jurisdictions now recognize that cryptocurrency is 'property' in law), representing the hackers' benefit from criminal conduct, namely from extortion/blackmail and the Ransomware attack, both criminal offences in most advanced jurisdictions.

Further legal considerations may also come into play; firms that pay ransoms (and their facilitators) should also consider whether they have regulatory anti-money laundering reporting obligations under Part 7 of POCA 2002 and the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 to submit a Suspicious Activity Report ('SAR') to the National Crime Agency in respect of information that comes to them in the course of their business if they know, or suspect or have reasonable grounds for knowing or suspecting, that a person is engaged in, or attempting, a money laundering or terrorist financing offence.

They may commit an offence if they have 'knowledge' or 'suspicion' of money laundering activity or criminal property, do something to assist another in dealing with it, and fail to make a SAR. Submitting a SAR protects an individual and an organisation by providing a potential defence against money laundering financing offences, (known as consent, appropriate consent / prior consent defences).

Conclusion

Navigating the complex and unclear international sanctions regimes when dealing with a ransomware attack and the demand for payment is a fraught process, which leaves victims of attacks vulnerable.

The technical solution presented in this paper, the Bi-Symmetric handshake, provides a new and novel quantum resilient encryption feature, which may just offer the much-needed harbour of safety against the onslaught of ransomware attacks.

Global Foundation for Cyber Studies and Research (GFCYBER) is an independent, nonprofit and non-partisan think tank, which conducts studies and research and provides consultation on cyberspace challenges and issues from the intersecting dimensions of policy and technology for the betterment of a globally-connected world. The foundation works on the philosophy that together we can secure the cyberspace!

Contact Us:

5614 Connecticut Avenue, N.W., No. 209,
Washington, D.C. 20015, USA.

www.gfcyber.org
info@gfcyber.org
@gfcyber