Black Hats, White Hats, and Hard Hats

Making Encryption socially responsible

This paper addresses the commercial risk of data breach, and introduces the Light Blue model for socially responsible encryption.

The Cost of Cyber-Crime

Between 2016 and 2017, in a series of five leaks, a hacker group called the Shadow Brokers dumped dozens of National Security Agency software exploits on the web, free to criminals and security analysts alike. Having gained notoriety, the Shadow Brokers then tried auctioning exploits, using a monthly subscription model, then catalogue sales[1].

What use are these exploits? In the case of the WannaCry ransomware attack[2], data on randomly infected end-user computers was encrypted, and a Bitcoin ransom was demanded to decrypt it. Some victims complied. Others simply wrote off their infected machines.

It is impossible to know how many secret attacks may have occurred, using this technology, or similar technology from other sources.

IBM in its 2017 Cost of Data Breach Study[3] found that the average cost of a data breach is $3.62 million[4], with an average probability of 27.7 percent that organizations in the study will have a material data breach in the next 24 months.

Those are detected incidents. Sarbjit Nahal, managing director and head of thematic investing at Bank of America Merrill Lynch, says that as many as 70% of attacks may go undetected.[5]

[1] Burgess, M. 2017, 'Hacking the hackers: everything you need to know about Shadow Brokers' attack on the NSA', Wired, accessed 15 August 2017, <http://www.wired.co.uk/article/nsa-hacking-tools-stolen-hackers>.

[2] Based on the EternalBlue exploit, leaked by the Shadow Brokers hacker group on April 14, 2017.

[3] IBM Ponemon Institute, 2017 Cost of Data Breach Study: Global Overview, e-book, accessed 16 August 2017, <https://www.ibm.com/security/data-breach>.

[4] Amounts in this document are all in USD.

[5] Turner, G. 2015. 'Cybersecurity Index Beats S&P 500 by 120%. Here's Why, in Charts', The Wall Street Journal, accessed 17 August 2017, <https://blogs.wsj.com/moneybeat/2015/09/09/cybersecurity-index-beats-sp-500-by-120-heres-why-in-charts/>.

In 2015, Lloyd’s of London estimated that cyber-attacks cost businesses as much as $400 billion a year globally.[6] Juniper research recently predicted that the rapid digitization of consumers’ lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019.[7]

In my experience, as a systems analyst working in financial services in the oil & gas industry, the largest potential loss is from insider trading, using stolen information, where millions of dollars can be made per transaction, by criminals trading on non-organised OTC markets[8]. We simply can't know the cost of this. The victims are long-term investors such as pension funds and insurance companies.

Ginni Rometty, Chairman, President and CEO of IBM Corp., recently said that “Cyber-crime is the greatest threat to every company in the world”.

The Problem With Networks

Every business is a consumer of modern cryptography services. When you access a secure website, using the HTTPS protocol, all communications between your browser and the website are encrypted. Virtually every financial transaction that occurs globally is encrypted. When you speak using Skype, every message is encrypted. These events happen without the need for you to do anything special: cryptography is woven into the fabric of the way we communicate in the modern world.

Nonetheless, it remains possible to communicate electronically without encryption.

[6] IBM, 2017, 'IBM’s CEO on hackers: “Cyber-crime is the greatest threat to every company in the world”', accessed 18 August 2017, <https://www.ibm.com/blogs/nordic-msp/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/>

[7] Juniper Research. 'Cybercrime Will Cost Businesses Over $2 Trillion By 2019', accessed 19 August 2017, <https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion>

[8] Over-the-counter (OTC) derivatives are contracts that are traded directly between two parties, without going through an exchange or other intermediary.

Most forms of email aren’t encrypted by default. Many kinds of network traffic aren’t encrypted. Data moving along unencrypted channels is vulnerable to interception, by moderately skilled individuals, using freely available tools. For experienced criminals, using sophisticated malware such as those released in the Shadow Brokers downloads, these channels are completely open, and the incentive exists to exploit them. Why hold up a bank with high risk when a network engineer in a van outside a business can generate similar income? For any business that moves unencrypted information across networks, the risk of data theft is real.

This dynamic is of crucial importance to mining and resources companies, where valuable commercial information is frequently sent over unsecure public networks, to and from unsecure locations. Formal mechanisms for encryption on remote projects are often completely absent. This may be despite a head office culture of data security. Why is this so? The reasons include:

- The difficulty of securing remote networks.
- The need to sometimes use arbitrary connections such as satellite phones.
- A lack of understanding or standards for encryption in organisations.
- The inconvenience of encrypting and decrypting documents.
- A lack of understanding of the risk of data theft.
- Simple carelessness.

From the point of view of precautionary security, public networks should always be assumed to be unsafe. It simply isn’t possible to know in all cases when information might pass along an unsecured wire. Therefore, valuable commercial information should always be encrypted.

Does Encryption Work?

In a word, yes. Even the simplest obfuscation reduces the risk of interception and cyber-crime.

Properly executed end-to-end encryption can be considered to be secure. Only the people communicating can read the encrypted data. No eavesdropper can access the cryptographic keys needed to decrypt the conversation - not even the company that provides the messaging service.

Genuine end-to-end encryption can be hard to achieve. One question is: who holds the keys? In some cases, vendors providing encryption services hold keys themselves, in a form they can use to decrypt messages when required to by law enforcement.

Furthermore, all forms of encryption are potentially vulnerable to social engineering attacks, where users are tricked into providing credentials, and man-in-the-middle attacks, in which an intruder impersonates both parties in a transaction.

Another question is whether the code is correct: do vendor programs really do what they claim to do?

There are also rumours, although so far without much evidence, that the NSA has already broken some of the global standard encryption systems, such as the AES[9] standard, widely used by industry and banks.[10]

Nonetheless, strong encryption is the best tool we have for thwarting cyber-criminals. DigiCert estimates that with standard desktop computing power it would take

[9] The Advanced Encryption Standard is a symmetric encryption algorithm developed by Joan Daemen and Vincent Rijmen.

[10] There's a stronger argument that the NSA [and potentially other customers of advanced cryptology] have made inroads into the implementation of algorithms, rather than the algorithms themselves. See for example Bruce Schneier, 'Can the NSA Break AES?', Schneier on Security, accessed 10 August 2017, <https://www.schneier.com/blog/archives/2012/03/can_the_nsa_bre.html>

4,294,967,296 x 1.5 million years to break a 2048-bit SSL certificate. Or, in other words, a little over 6.4 quadrillion years.[11]

The Social Problem of Encryption

The social problem of encryption is that the same mathematics that makes privacy possible means that criminals can operate in secret. This is particularly problematic in light of modern terrorism, which uses sophisticated communications tools for logistics and planning.

To overcome this, governments routinely ask cryptography service providers to include backdoors that enable them to decrypt ciphertext. This puts vendors in a difficult position. Backdoors may create weaknesses that can be exploited by a different set of criminals. This may already be happening, without your knowledge.

Introducing Light Blue

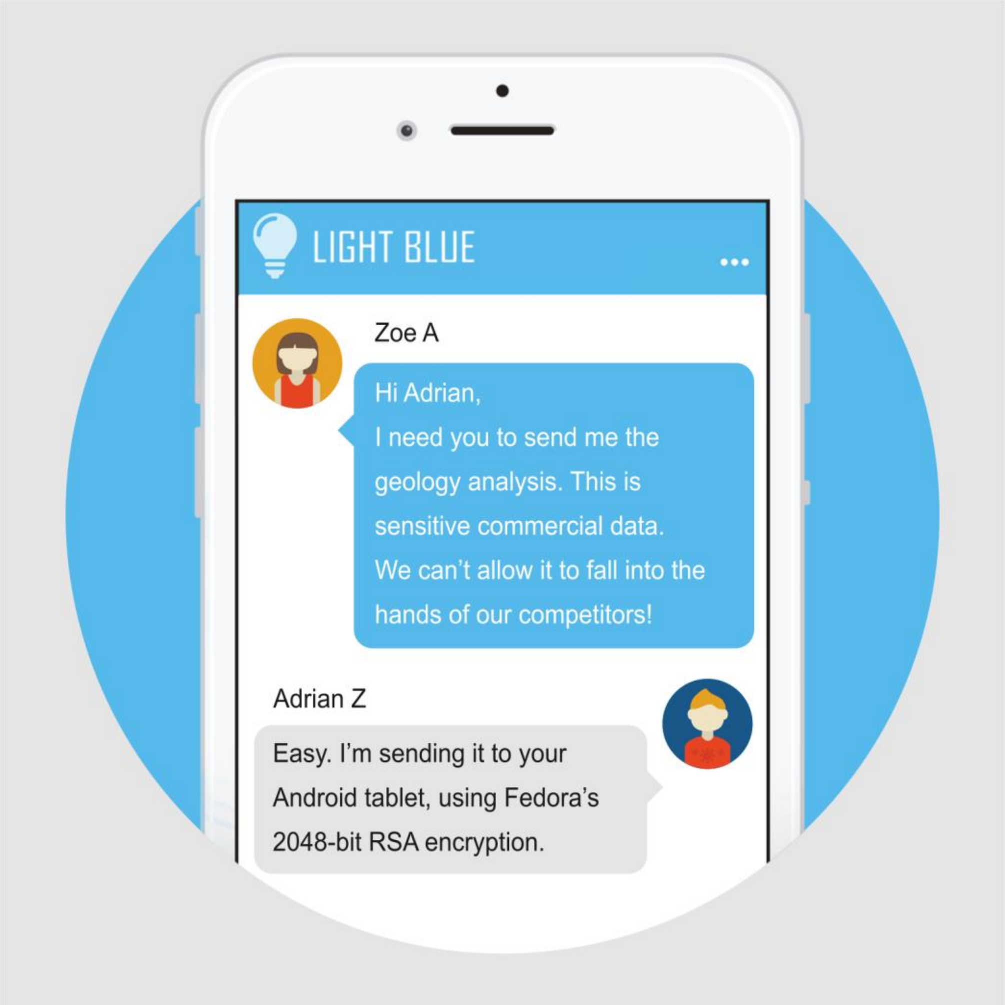
We wish to propose a model for socially responsible encryption, called **Light Blue**.

In the Light Blue model, a vendor provides rule-based private key access to the government of the customer’s choice from the outset. This is done openly, with the customer’s consent, using the government’s freely available public key. The Light Blue design includes methods and tools for achieving this.

As well as being a **model**, which can be used by anyone, Light Blue is also a **system**, which we're in the process of developing, initially for Android devices. The Light Blue

[11] DigiCert, 'The Math Behind Estimations to Break a 2048-bit Certificate', accessed 20 August 2017, <https://www.digicert.com/TimeTravel/math.htm>

app will go live for beta users in the Google Play store on 1/1/2018.

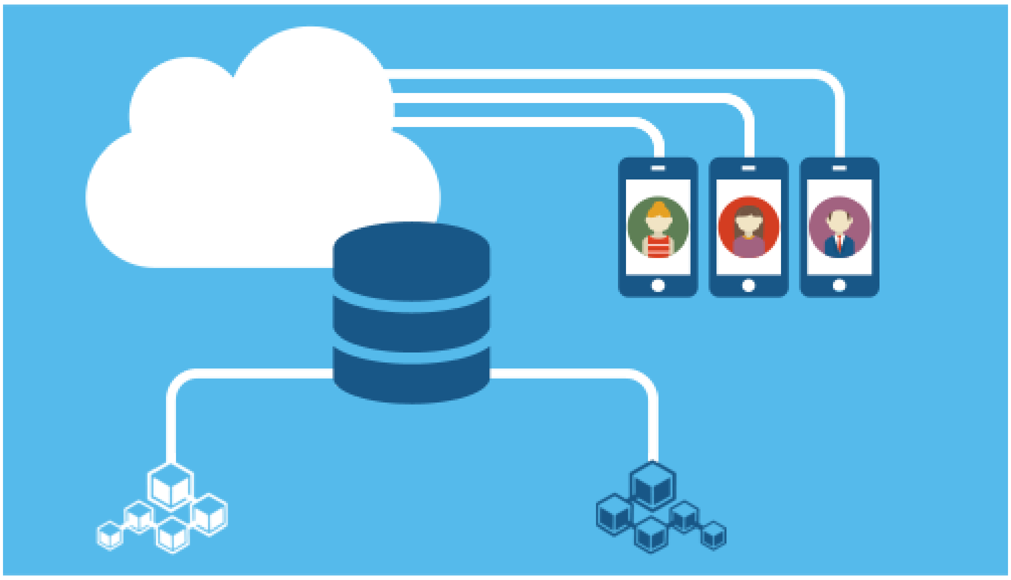


Zoe A

Hi Adrian,
I need you to send me the geology analysis. This is sensitive commercial data. We can't allow it to fall into the hands of our competitors!

Adrian Z

Easy. I'm sending it to your Android tablet, using Fedora's 2048-bit RSA encryption.



Light Blue will be open source, and free. The code will be published on GitHub when ready. We invite developers to build their own Light Blue clients.

How Light Blue Works

Light Blue is a true end-to-end encryption system, but one in which there are **two recipients** for each message: the primary recipient, who receives the message immediately, and the government of the sender's choice, who must wait. Messages encrypted for governments are only released to them under controlled circumstances, such as by the production of a warrant.

Light Blue is based on message duplication, over-encryption and blockchains:

By **message duplication**, we mean that a copy of each new message is encrypted for the authorities at the same time it is sent to its intended recipient. Instead of Light Blue providing backdoors, or holding private keys in a usable form, each user's messages are stored in a personal blockchain [called a preservation blockchain].

By **over-encryption**, we mean that preservation blockchain messages are encrypted in a series of wrappers, first using the user's private key, then the authorities' public key, then the Light Blue public key.[12] The user's X.509 certificate is also encrypted and stored in the same way. When the authorities satisfy the rules for receiving a preservation blockchain, we first remove our encryption layer then store the still-encrypted certificate and messages in a new blockchain [called a delivery blockchain], which we provide to the authorities.

A **blockchain** is a data structure where data can be stored semi-publicly in a linear

[12] Not all of the message is over-encrypted. The payload is encrypted using a symmetric key. The symmetric key is then over-encrypted using RSA encryption. This is necessary because the size of data that can be efficiently encrypted using RSA is limited. With the commonly used v1.5 padding and a 2048-bit key, the maximum size of data which can be encrypted with RSA is 245 bytes.

container space, called a block. Anyone can verify who stored that information because the container is digitally signed. In the case of Light Blue, that means signed with the owner's private key. Only the owner can unlock what’s inside a container because only they hold that key. Because each block is a cryptographic function of the preceding block, blockchains can’t be altered, only added to.

Blockchains rose to prominence as the underlying technology of the Bitcoin cryptocurrency. The importance of blockchains for Light Blue is that they provide an immutable record of transactions.

The **Light Blue implementation workflow** is as follows:

When a new Light Blue user subscribes using the app:

1. The device creates a public-private keypair in an X.509 digital certificate.
2. A password-protected copy of the certificate is stored in secure storage on the device.[13]
3. The user's public key is encrypted using the Light Blue public key and is sent to the Light Blue webservice, along with the user's other public information, where it is stored in a relay database, which is used to help mediate access between users.
4. An unprotected copy of the certificate is encrypted using the user's private key, then the authorities' public key, then the Light Blue public key, and sent to the Light Blue webservice, where it is becomes the first record in the user's preservation blockchain.

When a user sends a message:

[13] Android uses dm-crypt, which is the standard disk encryption system in the Linux kernel.

1. The message is encrypted using the recipient's public key and is sent to the Light Blue webservice, where it is stored in the relay database.

2. A second copy of the message is encrypted using the sender's private key, then the authorities' public key, then the Light Blue public key, and is sent to the Light Blue webservice, where it stored in the sender's preservation blockchain.

3. The device then uses Firebase Cloud Messaging [FCM] to ping the recipient that a message was sent. If the combined payload is < 4k, then the message itself is included in the ping.

When a user receives a message:

1. If the ping contains the message, then the recipient's device decrypts the message and notifies the user in a toast.

2. If the ping doesn't contain the message, the recipient's device calls the Light Blue webservice, which returns any waiting messages. The recipient's device decrypts those messages and notifies the user in a toast.

3. A copy of each incoming message is encrypted using the recipient's private key, then the authorities' public key, then the Light Blue public key, and is sent to the Light Blue webservice, where it stored in the recipient's preservation blockchain.

When the authorities request a user's messages:

1. We run a server program that removes the Light Blue encryption from each record in the requested user's preservation blockchain. This is done by decrypting the record using our private key, and storing the result in a new blockchain, called the delivery blockchain. The outermost layer of encryption of each record in the delivery blockchain is the authorities' encryption. Only the authorities can decrypt this information.

2. We then provide the delivery blockchain to the authorities by courier.
3. The authorities use their private key to remove their layer of encryption, exposing the user's unprotected X.509 certificate, which can be used to decrypt the user's messages.

Features of this model:

- All traffic is encrypted.
- There are no backdoors to weaken encryption.[14]
- Vendors and developers can't decrypt users' keys or messages.
- The authorities can't decrypt anything without vendor [or community] co-operation.
- Light Blue users are less likely to be investigated by governments, because the systems is less likely to be used by those wishing to transmit harmful or inappropriate data.

Does Light Blue solve the social problem of encryption? No. Criminals can simply use other systems. But Light Blue reduces the size of the space in which criminals can operate. As more people use systems like Light Blue, clandestine communications will become progressively easier to identify, by virtue of being a larger subset of a smaller set of transactions. If systems like Light Blue become widely accepted, then all vendors will become less inclined to provide systems that criminals can use. Eventually, irresponsible encryption may become so socially unacceptable that no vendors will sell such systems.

[14] Apart from the cryptographic problem of the same information being encrypted twice using different keys. We intend to quantify this mathematically.

Who Decides?

One problem with encryption services is that in most cases, users have to trust vendors to be honest about their methods and code. We hope to implement a structure where no one has to trust our business, only the system itself.

One piece of the puzzle is the protocol for the handover of requested blockchains to authorities, and the management of the process. Ideally, this shouldn't be done by us or any future Light Blue developer, but by some form of trusted third party. Once the app is complete, we'll start a consultative process to put that in place.

The second piece of the puzzle is to make the Light Blue source code open source. This provides many advantages:

- The cryptographic community can audit the code for correctness.
- Being an open source vendor increases trust.
- Other developers can find new uses for the model and code.
- Users can see that the code does what it says it does.

By placing both the code and the blockchain handover process in the public domain, there's no requirement for users to trust our business or its employees for the correctness of the system. Instead, they trust the community.

We welcome comments, and criticisms of these points, from the community.

Appendix – Interactions With Governments

We hope to form relationships with individual governments, in which each government provides us with the public key from a public-private cryptographic keypair.

This should be a **published** public key, so that any user can look in the open source code to prove that the key being used is correct, and corresponds to the government requested by the user.

For example, if Jane Doe is an Australian citizen, and specifies the Australian government as her handover recipient, then the system would use the Australian government's pubic key to encrypt messages in her handover blockchain. Thus, only the Australian government can decrypt her X.509 certificate, and thus gain access to her messages.

We expect that all governments have published public keys, that enable citizens to send them encrypted messages.

Our task is to approach those governments, and collect those keys.

Author:

Steve Asher is the CTO of Mineral Blue, and the technical director of QEM

steve.asher@mineralblue.com.au

QEM Solutions:

Mineral Blue is supplied by QEM Solutions, 1 Telford Mews, Beattock, Moffat, Scotland, DG10 9SG

www.qemsolutions.com

www.mineral.blue

Meet Mineral Blue

Mineral Blue is an advanced, cloud-based Safe Work system for the mining and resources industries.

Are you drowning in a sea of paper?

Our brief, when developing Mineral Blue, was to streamline safety processes using the Internet and mobile devices. By reducing administration time, we empower managers to provide a safer workplace

Learn More

Email our sales team:

ask@mineral.blue

Mineral Blue is provided by **QEM Solutions**. QEM provides consultancy, management and design services for construction and engineering.

www.qemsolutions.com

The Bottom Line

Mineral Blue isn't about the Internet. It's not about permits, or risk assessments. Mineral Blue is about time, and money. Time saved in major industrial processes like shutdowns means more time spent producing end products like gas and iron ore. Cost savings from increased efficiencies at the point of production are amplified throughout the business cycle.

These are major business benefits, achieved by the smart use of technology.

Mineral Blue **will** save you money. It will also **make** you money.

www.mineral.blue