A SECURE DIGITAL SOCIETY WITHOUT STRONG ENCRYPTION **IS UNTHINKABLE**

BY BART PRENEEL

COSIC, KU Leuven, Belgium.

EMERGING POLICY QUESTIONS FOR QUANTUM ENCRYPTION
By David W. Opderbeck

WHO CONTROLS YOUR PHONE: CLIENT-SIDE SCANNING AND THE FUTURE OF OWNERSHIP
By John Bergmayer

THE ENCRYPTION DILEMMA: ATTEMPTING TO RESOLVE THE UNRESOLVABLE
By Keith Martin

A SECURE DIGITAL SOCIETY WITHOUT STRONG ENCRYPTION IS UNTHINKABLE
By Bart Preneel

Visit www.competitionpolicyinternational.com for access to these articles and more!

A SECURE DIGITAL SOCIETY WITHOUT STRONG ENCRYPTION IS UNTHINKABLE

By Bart Preneel

This concise article delves into the pervasive deployment of encryption across billions of devices, safeguarding our data both during communication over networks and storage within our devices. Next it discusses the strengths and weaknesses of encryption. The discussion encompasses distinctions between link encryption and end-to-end encryption, highlighting the intricacies of securely managing encryption keys. Additionally, the looming challenge posed by the advent of large-scale quantum computing threatens our encryption systems. On a positive note, advancements in encryption techniques are facilitating expanded protection, encompassing the safeguarding of data during processing. The article concludes by outlining the ongoing debate surrounding encryption, particularly focusing on government access to citizens' data.

01
INTRODUCTION

Keeping secrets is essential to the human condition, and for this reason, encryption is said to be as old as writing itself. Until the beginning of the 20th century, encryption was only available to kings, generals and diplomats. In the 1920s, the emergence of wireless communications resulted in a small-scale commercial deployment of encryption devices for critical business communications. In the 1970s the automation of financial services led to increased usage of encryption implemented in expensive hardware devices.
The encryption explosion in the 1990s was driven by two main developments: the arrival of the world wide web that brought the internet to the average citizen and the deployment of mobile communications. The need for encryption was obvious through the risk of sending credit card numbers and the interception of mobile phone calls of celebrities. Fortunately, chip cards presented an inexpensive way to store keys and perform cryptographic computations, while at the same time computers became much faster which allowed to replace expensive hardware by low-cost encryption in software. In addition to encryption for hiding data, other cryptographic building blocks were developed to authenticate devices and to provide secure boot and update. In the last decade cryptography has played a growing role in the financial sector as illustrated by the emergence of cryptocurrencies.

The digitization of society is reaching an inflection point. At this moment, there are more than ten billion "personal computers" including PCs, laptops, game consoles, tablets, smart phones and smart watches. The average user carries several dedicated devices varying from car keys, bank cards, access cards, eID cards or e-passports; it is expected that these 20+ billion devices will disappear as they will be integrated into smart phones or watches. In 2024 the Internet of Things ("IoT") will grow to twenty billion things: it becomes increasingly more difficult to buy a household appliance or a car that is not connected to the internet; cars have become computer networks on wheels that communicate with the environment over several channels. Finally, all these devices are being connected to "the cloud," which can either be a public cloud or a private cloud for a specific application.

The picture that emerges is that a large part of daily life, including personal and commercial interactions is being mediated by electronic devices. In order to keep these devices and their interactions secure, encryption is essential. More specifically, cryptography is needed to boot devices securely, to authenticate to other devices and to protect both stored data and communications. Without encryption, it would not be possible to buy things online, share information on social media, manage our finances, consult our medical reports or work remotely. As the IoT develops, this also applies to managing our houses, our cars, and our cities. In summary, one can estimate that the number of cryptographic applications has grown in four decades from a few million to over fifty billion and will exceed 100 billion by 2030.

02
COMMUNICATIONS AND STORAGE

Historically encryption has been used to allow secure *communications* in the presence of adversaries. Today we understand that it is quite easy to intercept wireless communications: with a suitable antenna, Bluetooth, Wi-Fi or 2G/3G/4G/5G signals can be intercepted well beyond their intended range. Governments have always had the ability to intercept plain old telephone phone calls. The Snowden documents have shown that this capacity has been extended to the internet: governments scoop up connections at tens of Gigabits of information per second; after filtering out the cat videos, 10-20 percent is retained for further analysis.

Encryption can help here: wireless technologies such as Bluetooth, Wi-Fi, Lora and 2G through 5G provide by default encryption between the device and the access point or base station controller. Typically, the first generations of these standards are weak, but over the years the protection became more robust. While this offers protection against a curious neighbour or the other customers in the coffee shop, the information is decrypted at the access point or base station controller; the mobile operator or the owner of the coffee shop have access to all the data. This kind of protection is called "link encryption," as it only protects one communication link. Connections between a user and a website are built of multiple links; even if encryption is used, every intermediate node can see the unprotected information.

For strong protection, one would like to have "end-to-end encryption": this means that the encryption runs between the user device and the application server or between two user devices. Examples of the first case are the SSL/TLS protocol to protect web traffic, while messaging protocols (such as Signal, WhatsApp, iMessage and recently also Messenger) and email encryption (OpenPGP, S/MIME) belong to the second category. This is clearly preferable, as this creates a fully private conversation without access for an intermediary.

Next to increased communications, we have seen an exponential growth of *storage*: large quantities of data are stored on user devices such as hard disks, USB drives, and smart phones. Very often this data is sensitive: it may contain personal pictures, and financial or medical data. In order to protect against loss of theft of the device, most of these devices today offer encryption. Even larger quantities of data are today stored in the cloud. This results in convenient access to our media and data from any device. In this case encryption is also essential to protect data against cloud providers or hackers.
Encryption uses clever mathematics to protect large quantities of data. It does not create this protection "out of the blue": encryption shifts the protection of data to the protection of keys. How keys are established and managed is essential for the security.

In some applications this secret key is physically delivered by the service provider to the user in a smart card: a bank card in the financial sector and a SIM card for mobile communications. There is a trend towards mobile banking without cards and eSIMs replacing SIMs: this means that a different method will be needed to establish a secret key.

Many applications use an ingenious method to agree on a secret key. With a mathematical trick, an Internet server can generate a key for encryption (that can be made public), while the key for decryption (called the private key) is kept secret. This is known as public-key cryptography.[2] Now the Internet server can widely distribute its public key and users can encrypt information under this public key; this information can only be read by the Internet server.[3] A similar technique allows two WhatsApp users to agree on a secret key to protect their messages. Public-key cryptography is used to protect the web traffic (the SSL/TLS protocol), Virtual Private Networks ("VPNs"), messaging protocols and email.

"In some applications this secret key is physically delivered by the service provider to the user in a smart card: a bank card in the financial sector and a SIM card for mobile communications

If a state-of-the-art encryption algorithm is deployed with a strong key management and a secure implementation, even powerful governments cannot read the communication. There are still legacy applications using weak encryption algorithms that are vulnerable (such as the GSM encryption and the WEP protocol for Wi-Fi). The Achilles heel of encryption is the key establishment. First, methods to generate the key can have technical flaws, or there can be technical flaws in the methods to communicate the key to the other party (in an extreme case one network operator used the same key for every user). Second, governments can use legal means to request access to secret or private keys (cf. infra). Alternatively, one can undermine the distribution mechanism of the public key: on the web public keys are distributed by a trusted third party, the Certification Authority ("CA"). If a CA misbehaves and provides users with an incorrect public key, breaking the encryption becomes easy for the attacker.

Similar key management issues can occur for stored data: most consumer-market laptops have hard disk encryption enabled. But if the hard disk is stolen and plugged into another laptop, it will simply decrypt all the data. For business laptops, a key management mechanism is provided that requires a password or key before decryption. But for consumer laptops this is too complex and the hard disk will decrypt by default, resulting in encryption without security.

Even if there is a secure key establishment process, encryption can become insecure due to implementation weaknesses: one has to make sure that the secret key cannot be extracted from the implementation. A first problem is to prevent attackers from reading the key from memory; protecting software implementations against this attack is particularly difficult. Research[4] has shown that the time to perform a cryptographic computation can leak information on the key. For some devices, power measurements[5] or electromagnetic radiations can be problematic. The problem becomes even harder if an opponent can influence the computation by injecting faults with a laser or an electromagnetic pulse (so-called fault attacks). Protecting cryptographic implementations against these attacks is challenging, in particular for low-end applications such as IoT devices.

Despite these difficulties, the increasing use of encryption is a success story: more than 80% of web traffic is encrypted today: this means that billions of browsers inter-

2 Whitfield Diffie & Martin E. Hellman, *New directions in cryptography*. IEEE TRANS. INF. THEORY 22(6): 644-654 (1976).

3 In practice public-key encryption is too slow: client devices will send a secret key and subsequent communications will be protected with this key.

4 Paul C. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*, in CRYPTO 1996, 104-113 (Neal Koblitz, ed., 1996).

5 Paul C. Kocher, Joshua Jaffe & Benjamin Jun, *Differential Power Analysis*, in CRYPTO 1999, 388-397 (Michael J. Wiener ed., 1999).

act with close to 400 million secure servers.[6] Most mobile phones have strong hard disk encryption and billions of users communicate with end-to-end encrypted messaging. Yet there are still many problems: there are threats of state actors on the web ecosystem that distribute incorrect public keys; companies deploy similar techniques in commercial products to issue (inside the company) incorrect public keys to snoop on web traffic of employees. None of the regular phone calls on the fixed network or on 2G/3G/4G/5G are end-to-end encrypted which means they are easy to intercept by network-level hackers and by governments. The same weaknesses apply to messaging via SMS. Snapchat provides end-to-end encryption for snaps (photos and videos) but not for chats and messages. Many cloud services and advertising services massively collect sensitive user data; in the best case, they use an encrypted connection to send the data to the cloud, but sometimes this data is sent unencrypted over insecure networks. The weakest point remains the endpoints: spyware tools such as Pegasus[7] compromise the user device and give an attacker full access to all the data: encryption cannot protect against this threat as the data needs to be accessible to the user.

03

FACING THE QUANTUM THREAT: POST-QUANTUM CRYPTOGRAPHY

In the 1980s Richard Feynman & Yuri Manin invented a quantum computer, a computer working with qubits. Unlike a bit in a digital computer that is 0 or 1, a qubit can be 0 and 1 at the same time, which is called superposition. Such computers would be extremely useful to simulate complex processes studied in physics and chemistry. In 1994, Peter Shor invented a quantum algorithm to factor large integers and to compute discrete logarithms. Unfortunately, all widely deployed public-key encryption methods rely on the difficulty of these mathematical problems. In other words, if a large quantum computer with a few thousand qubits can be built, all public-key encryption methods in use today can be broken.

In the 1990s a race started to build a large quantum computer. Thirty years later, billions of dollars have been spent and several approaches have made some progress: quantum computers with 50 to a few hundred noisy qubits have been built – it is believed that if these noisy computers can be scaled up to 10-20 million qubits, they would be powerful enough to break public-key encryption.

Experts are divided on the question how long this scale-up will take: optimists believe that 5-10 years are enough, while some others believe that 15-20 years are needed. Some other experts are of the opinion that it may take many decades or that it will never happen. Unfortunately, we cannot afford a wait and see approach. Today, nation state adversaries are scooping up all encrypted communications and store them, in the hope that they can decrypt in 2035, 2040 or 2050. Some information does not need long-term protection, but nation-state secrets and medical data can be sensitive for 50 years and more. This quantum threat has motivated the cryptographic community to develop new public-key algorithms that can resist attacks on large quantum computers, called post-quantum cryptography or quantum-safe cryptography. This has been a lengthy process, culminating in a high-profile open competition organized by NIST (National Institute for Standards and Technology, U.S.). The first standards are expected for 2024, and additional standards will become available in the next years. This is only the first step: companies need to integrate these standards in their products, have their products certified and integrate them into solutions. Most encryption deployments have limited algorithm agility, which means that this migration process will be long and costly. A full migration towards post-quantum cryptography is expected to take 7 to15 years from now, depending on the application. Most organizations (except for the NSA) plan to keep using both current algorithms and new algorithms at the same time; this hedges against the risk that an unexpected flaw would be identified in one of the newer post-quantum algorithms.

04

COMPUTING ON ENCRYPTED DATA

The Big Data and AI trend consists in collecting massive quantities of data in the hope to extract value out of it. Consider for example the advertising ecosystem, where sophisticated algorithms are deployed to profile users and show

6 https://letsencrypt.org/stats/#percent-pageloads.

7 https://en.wikipedia.org/wiki/Pegasus_(spyware).

them the most suitable ads. This profiling is problematic as it can contain sensitive data on health or sexual orientation. Encryption can protect data sent to the cloud and stored in the cloud, but current methods to not allow to extract value from encrypted data.

New encryption techniques have been developed to solve this problem: the data can remain protected yet it becomes possible to compute on it. A first technique is Fully Homomorphic Encryption (FHE), that allows a cloud provider to compute on encrypted data and subsequently send the result in encrypted form to a third party for decryption. The cloud provider never sees the data. A second technique is secure Multi-Party Computation ("MPC"): here data is divided into pieces, where each piece is sent to a different party using secret sharing: a piece by itself is fully random (that is, it conveys no information), but the combination of all the pieces reveals the data. The parties can now jointly perform computation on their pieces: a complex function of the data can be computed without any party ever seeing the data. These approaches were proposed more than 40 years ago and have been steadily improved since; only in the last few years have these techniques become efficient enough to deal with large-scale problems. One can also prove that the computation has been performed correctly. For FHE, the computational overhead was initially huge, but orders of magnitude of improvement have been gained; with dedicated hardware the last step can be made towards practical efficiency. For MPC, the bottleneck lies in the communication overhead. As an example, both FHE and MPC can be used for machine learning on encrypted data: both training a neural network and inference. Similar to public-key encryption, one can expect that these techniques that were once seen as esoteric will be integrated in widely deployed solutions to protect our data.

05
GOVERNMENT ACCESS: THE CRYPTO WARS

Even if governments fully understood the importance of protecting communications, they initially tried to *control* cryptography: their view was that governments require strong cryptography, but citizens should only have access to weak cryptography: that means, cryptography that offers some protection but that can easily be broken by governments. How did they achieve this? A first approach was to restrict academic research on cryptography. This had limited impact, but as an example, the EU-funded project RIPE was told it could study cryptographic mechanisms for authentication but not for encryption. Between 1993 and 1999 no encryption research was funded by the EU. Second, governments developed encryption standards that use short keys, or weak encryption algorithms, or the combination of both. This approach was applied successfully to the DES standard, developed for the U.S. Government in 1977: while the algorithm itself is well designed, its key was limited to 56 bits. A key of this size was in the 1970s sufficient against an average attacker, but it could be recovered by a powerful government. The problem with this approach is that because of Moore's "law," computers get two times faster every 18 months: consequently, breaking DES in the 1990s became feasible for attackers with limited budgets. Unfortunately, DES was kept in use until the early 2000s, much longer than it should have been. The GSM (2G) ciphers designed in the late 1980s are another example: the A5/1 algorithm is not very strong and has a 64-bit key (that was reduced in practice to 54-bit keys); the A5/2 algorithm is much weak than its 64-bit key would suggest. Again, these algorithms remained in use for more than 30 years, much longer than originally intended.

A third approach to restricting access to strong encryption consists of controlling import, usage or export. While the first two becoming less important, there are today still tight controls[8] on the export of some encryption and cryptanalytic devices.

As encryption moved from a hardware to a software technology, controlling cryptography became much harder: one can print the code in a book (e.g. the code of the PGP email encryption program[9]) and rely on "freedom of speech" legislation to freely distribute the book. Currently the EU and U.S. do allow export of strong encryption for mass market software such as operating systems and browsers, but dedicated solutions and cryptographic hardware are still tightly controlled.

As it became too hard for governments to control encryption devices, they shifted gears and required key escrow: products can encrypt data, but a copy of the decryption key needs to be provided to law enforcement. An example of such as solution was the Clipper chip, proposed in 1993 by the U.S. government as an alternative to a phone encryption device developed by AT&T using strong

8 E.g. EU dual use export controls, https://eur-lex.europa.eu/EN/legal-content/summary/dual-use-export-controls.html

9 PHILIP ZIMMERMAN, PGP SOURCE CODE AND INTERNALS, MIT PRESS, ISBN 0-262-24039-4 (1995).

encryption. Civil society, industry and academia pointed out the weaknesses[10] of this approach and the Clipper chip was abandoned. The main argument against backdoor access is that it creates an additional weakness in the system that is likely to be exploited by bad actors. A non-technical argument is that it seems extremely difficult to manage access for law enforcement and intelligence services from multiple nations for data present in multiple jurisdictions.

It turned out that defeating the Clipper chip was a Pyrrhic victory in the crypto war: from the Snowden documents it became clear that intelligence services were very effective in getting access to encrypted data through a broad range of tools including manipulation of standardization processes, backdooring cryptographic standards (e.g. DUAL_EC_DRBG[11]), backdooring hardware encryption devices from commercial players (e.g. CRYPTO AG), exploitation of implementation weaknesses, using security letters to request private decryption keys, exploiting backward compatibility with weak versions present for export control, etc. Interestingly, the attack on a backdoor in a Juniper router[12] by an unknown threat actor provided a strong indication that backdoors are indeed abused by other parties as predicted earlier by the experts.

Despite the success of intelligence agencies in breaking encryption, law enforcement agencies started to complain in 2014 that they are "going dark." More recently, an EU-level closed working group has been created that attempts to address the same problem. While law enforcement may have fewer tools available than intelligence agencies, they are known to have deployed powerful spyware tools that provide full access to smart phones of suspects – such access provides a wealth of information on multiple targets that was never available before (including all contacts, locations, interactions, messages, audio, video). Moreover, large scale collection of metadata and widespread deployment of cameras provide a huge data trove; in combination with AI techniques, law enforcement has powers which they never had in history. In spite of this, the war against encryption is continued with increased efforts.

In 2016 the next battle in the Crypto war was fought: the high-profile case of Apple versus the FBI dealt with access to a confiscated iPhone of a terrorist, the San Bernardino shooter. The FBI tried to force Apple to provide access; Apple refused, pointing out the risk of a large number of requests of law enforcement agencies from all over the world and the risk to undermine the security of all iPhone users. The FBI dropped the case and paid a company for a tool to get access with a hardware hack; it turned out that the iPhone did not contain any valuable information (which could be expected as the suspect had destroyed all his other devices before the shooting). This story prompted experts to update their report on the risks of backdoor access to encryption.[13]

"Despite the success of intelligence agencies in breaking encryption, law enforcement agencies started to complain in 2014 that they are "going dark."

For the next crypto war, the battlefield is changing again. Law enforcement has shifted the focus of the public debate on encryption from terrorism and serious crime towards detection of Child Sexual Abuse Material ("CSAM"), as illustrated by the EU draft CSAM regulation - also known as #chatcontrol. Their argument is that the growing use of end-to-end encryption of messages precludes scanning for CSAM content at the service providers: the CSAM proposal intends to introduce universal client-side scanning of all devices for known and even new content (the latter using AI). Experts have pointed out that such an approach violates human rights and is wide open to abuse: this functionality is likely to be abused in several countries to automatically and at scale detect citizens possessing content critical of the regime. A second battle ground at EU level is the eIDAS 2.0 regulation: depending on the details of the implementation, browsers could be restricted in implementing existing or new protection methods to detect and block bogus certificates. Some of these suspicious

10 Hal Abelson, Ross J. Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller & Bruce Schneier, *The risks of key recovery, key escrow, and trusted third-party encryption*, WORLD WIDE WEB J. 2: 241-257 (1997).

11 https://en.wikipedia.org/wiki/Dual_EC_DRBG.

12 Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla & Hovav Shacham, *Where did I leave my keys?: lessons from the Juniper Dual EC incident*, COMMUN ACM 61(11): 148-155 (2018).

13 Harold Abelson, Ross J. Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter & Daniel J. Weitzner, *Keys under doormats*, COMMUN. ACM 58(10): 24-26 (2015).

clauses were introduced in last minute changes without full transparency on their intention. In other jurisdictions, legislation has been approved or is being considered that gives governments the power to force service providers to insert backdoors.

All the past crypto wars have one element in common: the absence of an open and fact-based debate on the impact of the digitization of society on law enforcement. All experts (including ex-directors of the NSA) agree that strong encryption is essential to protect our economy and our society. Weakening encryption will lead to a less secure society. Law enforcement should develop effective ways to combat crime, while avoiding mass surveillance and respecting human rights. It should focus on making the best possible use of the massive quantities of data and metadata available. The current developments involve increasingly sophisticated tools such as AI and spyware, which substantially increases the risk for abuse. In order to balance this development, the independent supervision of law enforcement agencies should be strengthened substantially ■

All the past crypto wars have one element in common: the absence of an open and fact-based debate on the impact of the digitization of society on law enforcement

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL