HIGH-ASSURANCE ENCRYPTION

IF IT'S NOT BROKEN DON'T FIX IT!

WHITEPAPER

SENETAS

Security without compromise

The continuing calls by law enforcement agencies in the US, UK and Europe for legislation to mandate the inclusion of "backdoors" in the world's most secure and effective data encryption devices must be defeated - for the protection of all citizens.

Although the mandate requests that this weakness be designed-in exclusively, for the use of law enforcement, these backdoors will destroy the overall integrity of the world's best encryptors overnight!

Governments, law enforcement, defence forces and enterprises have benefited from the most secure, dedicated encryption products for more than 20 years.

All beneficiaries of the best encryption technology have one thing in common: a requirement for high-assurance encryption - encryptors that are secure, certified and adopt the best encryption key management available. Beneficiaries demanded 100% trust in these products.

Therefore, any built-in or designed-in weakness for law enforcements access will destroy that trust and once this has happened there will be no going back.

In light of this, propositions that require vendors to deliberately weaken robust encryption by providing 'backdoors' for law enforcement agencies are both counter-productive and potentially dangerous.

This paper was requested by the Austrailian Strategic Policy Institute (ASPI) as a contribution towards the 'encryption backdoors' debate. ASPI is an independent think tank and advises strategy and defence leaders.

There may be no more important data security topic today than law enforcement's persistent calls to weaken 'unbreakable' encryption (the FBI's term for high-assurance encryption) by forcing vendors to add backdoors to their secure products.

Across the US, UK and Europe, law enforcement agencies are dedicating time and resources to pursuing this counter-intuitive and potentially dangerous proposition; all in the name of counter terrorism.

It's a truism to say that new technologies are just as available to good guys as they are to bad guys. Whatever the new technologies, the only difference lays in their use – the good guys use them for better purposes than the bad guys.

Why is robust encryption 'unbreakable'? In short specific law enforcement agencies are referring to 'high-assurance' encryption products that have a number of security attributes. The most significant attribute is the use of state-of-the-art client side encryption key management.

Although the current debate is one around weakening robust encryption, discussions started with calls to ban it completely. In March 2015, the Guardian reported the FBI's and Europol's calls for a ban on 'unbreakable" encryption.

In November 2015, the Daily Telegraph profiled the UK's new Investigatory Powers Bill, which requires service providers to hand over decrypted customer data when a warrant is issued; thus killing providers' (such as Apple and Facebook) ability to offer customers genuinely robust encryption security. This latter situation of 'investigative powers' has been put to the test in the US – the FBI versus Apple. The FBI, on the face of it, reasonably argues that Apple should do everything to assist it to 'break' the security features of its iPhone product in one specific case of a known terrorist, who caused enormous harm. This individual's iPhone is expected to contain a great deal of valuable information that is not only robustly encrypted, but protected by a '10 failed attempts destroys the data' feature.

Apple argues that it would be in breach of customers' 'trust' if it were to 'break' even this criminal's iPhone security. CEO, Tim Cook publicly argues that such action would compromise its technology that benefits the majority of law-abiding citizens.

His point is two-fold – the FBI has 100% access to the metadata and that data would likely meet the FBI's investigative needs. He also argues the line that 'for the greater good' the FBI should not be empowered to undo a security feature commonly used by all Apple customers.

It seems clear that Tim Cook's underlying concern includes the lack of certainty when it comes to law enforcement's ability to self-regulate.

The principles of the FBI versus Apple case are obviously closely linked to calls for encryption 'backdoors' to deliberately weaken robust encryption technology. In the former case, law enforcement is asking a vendor for the 'door keys'. Whereas in the latter case, law enforcement is demanding all vendors 'leave the keys under the mat'!

Encryption technology has protected data networks and sensitive data in transit for the general public, governments and commercial organisations for decades.

As the threat of cyber-criminals and terrorist activities have accelerated, robust encryption products have been protecting us all.

Technology has no morals. It is equally available to both the good guys and the bad guys. With the best will in the world, if you develop backdoors for law enforcement, law breakers will have access to them too.

There is simply no such thing as a robust security solution with a backdoor. Encryption security is either robust - providing end-to-end encryption without any weak-points – or it is not.

The idea of weakening robust encryption solutions seems to ignore the intrinsic role encryption security plays in the modern world.

Encryption is used to secure everything from banking and online purchasing to security exchanges, critical infrastructure, CCTV networks, cloud services and telecommunications.

The weakening of encryption threatens to undermine the entire digital economy.

As the US intelligence community announced it would continue to pursue legislation against "unbreakable encryption", former FBI Director James Comey urged vendors to "voluntarily stop offering end-to-end encryption".

The trouble is, the moment any vendor capitulates and weakens their encryption, they will have breached the trust of every current and potential customer – including governments and global corporations.

Backdoors, if they exist, will be available to be exploited by increasingly capable cyber-criminals, terrorists and rogue states. No organisation or individual will be able to trust that their data and privacy are truly secure.

As Apple CEO, Tim Cook said: "…you can't put the genie back in the bottle…"

WHO WATCHES THE WATCHMEN?

Like all security, information security is about trust and integrity. Nothing must ever be allowed to interfere with the integrity of cyber-security solutions. If backdoors are put in place, we are faced with the complex issue of oversight. Who is responsible for administering law enforcement's access to, and use of, the backdoor?

Managing the governance required to maintain checks and balances, and prevent agencies from over-reaching their powers, would be both expensive and contentious.

Here are five crucial issues that highlight the dangers and naiveté of the proposition to weaken robust encryption:

1. DON'T LEAVE THE KEYS UNDER THE MAT

Realistically, by imposing encryption backdoors, commercial organisations and individuals will be exposed to weaker encryption that may be exploited by cyber-criminals and terrorists alike.

2. TRAPS FOR THE TRUSTING

Blind faith in the system is a high risk strategy. By implementing encryption backdoors, the ultimate losers will be the organisations and individuals the encryption was intended to protect.

3. ADMINISTRATION AND GOVERNANCE

If encryption backdoors are mandated, systems administration will be flooded with issues, resulting from a loss of integrity of encryption solutions. Not to mention the knock-on effect on the digital economy.

4. TRUSTWORTHY DATA SECURITY

The very existence of an encryption backdoor increases systems vulnerability and will adversely affect encryption vendors' reputations. Trust in the performance of a product is a core component of a robust data security strategy.

5. A TECHNICAL PERSPECTIVE

Mandating encryption backdoors for major vendors does not address the issue of terrorists' encrypted communications as they can simply move jurisdictions or use their own bespoke encryption algorithms. Furthermore, encryption experts fail to see how anyone may selectively allow law enforcement access and exclude terrorists.

DON'T LEAVE THE KEYS UNDER THE MAT

Calls to weaken robust encryption in order to aid law enforcement in their surveillance of potential terrorists raises a number of issues. They reflect conflicting views of what an effective national data security strategy looks like and impact on basic principles, such as security, trust and civil liberty.

Any inclusion of back-doors, no matter how noble the purpose, is the equivalent of "leaving the keys under the mat".

The Netherlands government was among the first EU countries to reject the proposition raised by Europol because it "…remains committed to the wider benefits of strong encryption".

The idea of adding encryption backdoors and/or software that enables law enforcement's surveillance of decrypted data is illogical, simplistic and one-sided.

Agencies that are calling for the implementation of backdoors are reacting to the developing terrorist threat, but without considering the bigger picture – specifically, effective national data security and a trusted digital economy.

The reality is that many terrorist and criminal organisations are technologically advanced and in a position to exploit any security weaknesses. The call for backdoor access by law enforcement is the digital equivalent of leaving the keys under the mat.

The French Ministry for Digital Affairs also announced its opposition to backdoors, stating "it would be both counter-productive and leave sensitive citizen personal data unprotected"

Governments must resist the short-sighted and simplistic appeals by law enforcement agencies, look beneath the surface and consider the logical dangers and damage of weakening the wider digital economy's robust encryption security.

TRAPS FOR THE TRUSTING

If history has taught us anything, it is that Governments are rarely trusted to effectively manage the governance and oversight of enacting law enforcement powers.

Faith in the system is both naive and risky. The arguments in favour of weakening robust encryption do not address a number of key considerations for law enforcement.

> *"The encryption problem for law enforcement is a need for it to think laterally and work collaboratively to develop an approach that is cooperative, scrutinised and includes vendors and policy makers."*
>
> **Anthony Bergin (ASPI)**

> *"Law enforcement's proposition reflects its over reliance on single-source intelligence, an increasing neglect of human intelligence assets and a failure to think laterally - making them resort to a 'big hit approach."*
>
> **John Coyne (ASPI)**

The fundamental flaws in law enforcement's 'big hit' approach are the assumptions they make about terrorist behaviour. Namely, that back doors will not cause terrorists to:

> Cease to communicate

> Move into different jurisdictions

> Use their own bespoke encryption

> Exploit other aspects of communications technologies to overcome backdoors

The short-sighted call for introducing backdoors also ignores the fact that terrorists will be in a position to exploit the new vulnerabilities to their benefit.

Technology is unable to differentiate between the good guys and the bad guys. If the good guys have to play by the rules and the bad guys don't, there will only be one winner in the end.

SENETAS
Security without compromise

ADMINISTRATION AND GOVERNANCE

The practicalities of the call to weaken robust encryption are where legislators only need to look to see how such a 'big hit' approach would also be of little law enforcement benefit.

Data security and digital economies depend upon trust, data integrity and privacy. These cannot be assured when law enforcement has mandated backdoor access.

Society in general is wary of law enforcement's attempts to increase their reach and powers; even with complete transparency and oversight. Any surveillance initiative on the scale recommended requires judiciary scrutiny as a part of a truly democratic process.

Guardian journalist James Ball highlights the administrative impracticalities of enabling law enforcement's access to backdoors. Including:

> The depth of encryption security technologies used in so many aspects of modern life – from online shopping to internet banking and social media

> Encryption is an important protector of much of what we do and think; it has implications for freedom of speech and human rights

> Under a backdoor encryption policy, or even a robust encryption ban, everyone who encrypts sensitive data is disadvantaged

Ball concludes that there is no such thing as selective encryption: "It is impractical to selectively identify, capture and analyse terrorist data".

Then there is the issue of cross-international borders – jurisdiction. How does one country implement an encryption backdoor policy when its neighbours do not?

> No one government may enforce such a policy upon another

> Control, process and security may be impossible to manage

> In an environment of mandated encryption backdoors there are other obvious issues:

> Trusting the competency of the agencies and their staff

> Identifying rogue law enforcement staff

> Preventing systems breaches that may compromise security and data integrity

"Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently political tool… the Snowden revelations motivate a reassessment of the political and moral positioning of cryptography. They lead one to ask if our inability to effectively address mass surveillance constitutes a failure."

Philip Rogaway,
University of California

SENETAS
Security without compromise

TRUSTWORTHY DATA SECURITY

Law enforcement agencies appear to have overlooked that data encryption solutions are the intellectual property (IP) of the vendors that developed them – the integrity of which is crucial. By mandating vendors to provide law enforcement agencies with backdoors, they also undermine the vendors' IP.

Any attempt to interfere with vendors' robust encryption products by implementing backdoors will destroy those products' integrity and trust.

Effective data security policy planning begins with the mandated protection of data security technologies and their protection from all threats to their integrity.

Only then will legitimate citizens and commercial and government organisations trust they are operating in a safe digital economy.

Revered security expert Bruce Schneier agrees with France and Netherlands governments, but puts is more simply: "it is not just counter-productive, but stupid to nobble robust encryption."

A TECHNICAL PERSPECTIVE

A serious concern, expressed by security commentators, is that encryption backdoors are the first step on the road to the overall weakening of the security infrastructure.

Law enforcement's proposition is based on the presumption that mass data surveillance is effective. Others argue that it is not, and never has been; quoting distrust and prohibitive costs.

The proposition by law enforcement reads like an overreaction to how their use of technology has fallen behind the times and failed to keep up with the 'enemy' when it comes to communications surveillance.

Cryptocat's on-line encrypted chat service and Chatsecure's encrypted messaging service have outpaced available intercept technologies; so calls to weaken encryption have a sense of closing the stable door after the horse has bolted.

What law enforcement agencies seem to be overlooking is that encryption security has served nations and economies very well for many years – enabling secure global banking transactions, safe national infrastructure and protecting government secrets and commercial intellectual property.

"A backdoor for law enforcement is a backdoor for everyone. You cannot design a system that would selectively admit the good guys and exclude the bad guys."

WHERE TO NOW?

Right now, policy makers and governments need to spend more time with security and encryption experts before rushing into 'big hit' plans that would ultimately be self-defeating.

The contradictory comments by former UK Prime Minister David Cameron and former US President Barack Obama in 2015 highlight the risks of technically uninformed opinions and strategies.

Whatever the approach, it is essential to be mindful of the extent to which encryption is at the heart of most economic activities and has become deeply engrained in our digital economy.

For policy makers to suggest that we undo all of that, when it has only just become mature, suggests a dangerously high-risk approach.

From a macro-economic perspective, countries that opt to weaken encryption as proposed will likely find it difficult to export goods or services that fail the "trust test".

Major exporters may be forced to relocate to countries that enforce robust encryption if they are to maintain trust.

The implications of encryption backdoors and any other plans to mandate the weakening of robust encryption (such as shared encryption keys) threaten what we now take for granted – secure banking transactions, personal data, national infrastructure and intellectual property.

Apple CEO Tim Cook summed up the issue when he referred to encryption backdoors as a 'sledge hammer' and that data security is about trust.

In his view, weakening security that protects the majority to keep an eye on a very small minority, makes no sense.

Apple adopts end-to-end, robust encryption to meet customers' need for trust. Similarly, 'high-assurance' robust encryption security vendors invest heavily to ensure that trust.

"To kill that trust with an ill-informed and self-serving 'sledge hammer' solution to terrorist communications will have a permanent, damaging effect on the security of the vast majority."

GLOBAL SUPPORT AND DISTRIBUTION

Senetas high-assurance encryptors are supported and distributed globally (excl. AUS & NZ) by Gemalto – the world's largest data security company - under its SafeNet Identity and Data Protection Solutions brand.

Gemalto also provides pre-sales technical support to hundreds of accredited partners around the world; including systems integrators, data network providers, cloud and data centre service providers, telecommunications companies and network security specialists.

TALK TO SENETAS OR OUR PARTNERS

Senetas and Gemalto also work with customers' own data network service providers, systems integrators and information security specialists to specify the optimal high-assurance encryption solution for their needs.

Wherever you are, simply contact Senetas or Gemalto to discuss your needs. Or, if you prefer, your service provider may contact Senetas or Gemalto on your behalf.

CERTIFIED HIGH-ASSURANCE NETWORK DATA ENCRYPTION

Whatever your Layer 2 Ethernet network security needs, Senetas has a high-assurance solution to suit. They support data network links from modest 10Mbps and 100Mbps to high speed 1Gbps and 10Gbps as well as 10 x 10Gbps and ultra-fast 100Gbps bandwidth.

Certified, scalable, agile and easy to use; Senetas high-assurance encryptors provide maximum data security without compromising network performance.

SENETAS CORPORATION LIMITED

E info@senetas.com
www.senetas.com

Senetas manufactures high-assurance Layer 2 Metro Area and Carrier Ethernet network encryptors. They support all Layer 2 protocols and topologies.

Our multi-certified encryptors are used by some of the world's most secure organisations; including governments and defence forces, commercial and industrial enterprises, Cloud, data centre and telecommunications service providers in more than 40 countries.

SafeNet

SafeNet CN Series Ethernet encryptors

www.gemalto.com

GEMALTO DISTRIBUTION & SUPPORT

Senetas CN Series certified high-assurance network encryptors are distributed and supported internationally by Gemalto (North America, Europe, Asia, Middle East and Africa) as SafeNet CN Ethernet Encryptors.

BROKEN-WP0617