**IT for CEOs & CFOs** is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

# IT Security

## Self-encryption Deception: A High-level View

Bernard Parsons

**Bernard Parsons**
CEO and Co-Founder
Becrypt

***Biography***

*Bernard Parsons is the CEO and Co-Founder of Becrypt (www.becrypt.com).*

*Establishing Becrypt in 2001 with the aim of addressing the growing security requirements of endpoint technology, Bernard has built the company into a leading supplier of end-user device security products and services, with a focus on product assurance, multiple platform support and flexible delivery: from being embedded within the platform, to hosted within the Cloud.*

*Furthermore, Bernard has ensured Becrypt helps the most security-conscious organisations to be positioned as leaders in enabling value from the use of secure technology.*

*For his dedication to digital technology, Bernard was bestowed with an MBE in the 2018 New Year's Honours List.*

**Keywords** Hardware, Software, SSD, Encryption, NCSC, Cybersecurity, Data
**Paper type** Research

### Abstract

*In recent years, protection of sensitive data has received increased attention, particularly in the light of new European data protection regulations. As the frequency of data breaches and attacks continues to rise, security researchers have discovered multiple critical vulnerabilities in some of the popular self-encrypting solid-state drives (SSD) that could allow an attacker to decrypt disk encryption and recover protected data without knowing the password for the disk. In this article, the author gives his view on the latest research.*

### Introduction

The security and vulnerability of hardware-based disk encryption of solid-state drives (SSDs) has been increasingly probed recently, as the frequency of data breaches and attacks continues to rise. One school of thought asserts that theoretically this form of encryption is similar to, or superior than, software-based encryption implementations.

Directly challenging this view, recent research[1] carried out at Radboud University in the Netherlands by Carlo Meijer and Bernard van Gastel, has revealed a more worrying reality. Both highlight what they claim to be structural as opposed to incidental issues with a range of disk encryption products, referencing problems with the market in general, as opposed to specific vendors.

After analysing a significant number of hardware models, through the reverse engineering of firmware, it appears that a selection of hardware-based encryption products are flawed, uncovering a pattern of critical issues, including complete encryption bypass and access to user data without knowledge of passwords or keys. To make matters worse, full-disk encryption software built into popular operating systems will rely on hardware-based encryption if the SSD supports it.

Full-disk encryption is typically the solution of choice for data at rest protection, compared to file and folder-based solutions, as the approach addresses concerns such as sensitive data leakage through unencrypted temporary files and page files. Hardware-based encryption has developed in part as it offers the advantage of not holding the encryption key in computer memory, which can render devices susceptible to attacks whilst powered on. Historically hardware-based solutions had offered potential performance advantages, however today this has been made less relevant, as hardware extensions such as AES-NI are becoming increasingly prevalent on modern laptops, allowing hardware-based acceleration of encryption operations through software-based products.

## Implementing good security

Hardware encryption often typically relies on proprietary crypto schemes that are both hard to audit and implement, with the consequences of making mistakes that completely undermine security. Furthermore, the complexity of relevant standards by the Trusted Computing Group (TCG Opal) can contribute to the difficulty of implementing cryptographic schemes correctly.

Whilst Meijer and Gastel highlight that implementing good security can be difficult, it is typically not beyond the abilities of vendors, as demonstrated when publicised issues are promptly fixed. The issue is perhaps more about incentives favouring the easy route; it's much easier to implement credential management if you accept a few trade-offs in cryptographic design.

Of course, weak implementation is by no means a challenge that is particular to encryption products. Through recent work with a UK government department, Becrypt experienced their rejection of a management tool, which is advertised as a security tool, on the basis of the vulnerabilities it introduced as opposed to its security functionality. The thorough technical analysis undertaken by the government department concerned was beyond the capability of many potential customers of such products, demonstrating that although implementing security well can be difficult for vendors, knowing whether security has been implemented well can be even more difficult for buyers.

Arguably, incentives within the cyber security industry are currently somewhat skewed. It is far easier and more profitable for a vendor to demonstrate return on marketing investment, than justifying the cost of an independent assessment of a product's security architecture and implementation against meaningful security claims. The marketing budgets of leading vendors can not only significantly outstrip R&D spend, but are high by tech industry standards in general. As pointed out by Peter Cohen[2] in 2017 the world's largest security vendors had sales and marketing budgets that averaged 41% of their total revenue, with some as high as 60%. By definition this drives buyer norms, which in turn drives vendor investment.

**IT for CEOs & CFOs** is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

## Independent verification of software and hardware-based encryption

There will be a need for variants of both hardware and software-based encryption within the market for some time to come, driven by diverse requirements such as device form-factors and organisational threat models. However, ensuring that both software and hardware-based encryption products can continue to provide an acceptable level of assurance will depend on appropriate scrutiny of the architecture, crypto scheme, and implementation details, allowing for security claims to be independently verified.

Meijer and Gastel advocate that implementations are audited and subject to as much scrutiny as possible, suggesting vendors should aim to achieve greater levels of transparency in publishing their crypto schemes, architecture, and corresponding code to encourage independent review.

Product certification schemes, such as the UK National Cyber Security Centre's (NCSC) Commercial Product Assurance (CPA) approach, applicable to both software and hardware-based encryption, provide a mechanism to achieve independent and expert validation of product implementation. CPA goes beyond the remit of the FIPS 140-2 standards, which check the correctness of cryptographic algorithm implementation, to ensure that security claims are comprehensive and relevant and that all cryptographic schemes are correctly designed to meet stated objectives. CPA extends to implementation concerns, including coding standards, build standards, and through-life management, providing an arguably superior form of audit.

If organisations looking to implement encryption ensure products have been assured by such schemes during the procurement process, they should feel greater confidence that the necessary steps have been taken to appropriately protect their organisation's data. Those caught out by current vulnerabilities in hardware-based products should, at the very least, look to tighten data security by disabling SSD-based encryption, and look towards a software-based alternative. This will assure users that the recently discovered vulnerabilities, allowing one to circumnavigate passwords to decrypt sensitive data, are addressed.

Becrypt fully supports the argument for independent scrutiny of product implementation for security products, using appropriately thorough product assurance schemes. Ideally these schemes will evolve to keep pace with both technology and increasingly sophisticated attacks. Perhaps in an increasingly regulated market, where liabilities will increase across the board, the popularity and investment rationale for product assurance and other methods of independent test and validation, whilst not in themselves perfect, will be one of the mechanisms that rebalances market dynamics.

**Reference**

[1] https://www.ru.nl/publish/pages/909282/draft-paper.pdf
[2] https://petercohen.me/cyber-security-industry-addicted-marketing/