

The New Encryption Generation: Closing the Gap

It's not the disk, it's the data. Today's organizations require an intelligent, multilayered approach to encryption that automatically safeguards data without complicating essential IT and user operations. By Pete Bartolik

Contents

- 1 Executive Summary
- 2 Introduction
- 2 Data in the Line of Fire
- 4 Changing Needs for Security Management
- 5 Data on the Move
- 6 Endpoint Data Protection
- 8 Conclusion

Brought to you compliments of



Executive Summary

Concerned about the damage and liabilities of lost and stolen data, enterprises are turning to encryption as a backstop to prevent corporate and customer information from ending up in the wrong hands. Outdated, first-generation encryption technologies, however, often deliver less than promised—either leaving critical gaps in security, preventing the legitimate recovery of data or, even worse, encouraging operational compromises that can be exploited. Organizations today need a more intelligent, multilayered approach to encryption that automatically safeguards data without complicating essential IT and user operations. This white paper examines the limitations of first-generation encryption processes that often deliver less-than-promised performance, spur user resistance, conflict with operational infrastructure and process requirements, and can even leave data stored in unencrypted locations where it is easily visible to unauthorized users

>> For more information on data encryption, visit www.credant.com.

>> **Full disk encryption poorly aligns with the operational realities of today's enterprise: the need to lower IT overhead, protect against insider threats, ensure worker productivity, and centrally manage and enforce security.**

Introduction

There's nothing worse than not being able to protect your stored data. That's why most organizations today are investing in encryption, at least for critical areas of their operations. But some of those enterprises may in fact be relying on products and processes that create a false sense of security and may actually foster nonsecure practices.

The use of devices to conceal information is said to date back to the Spartans, who used a device called a skytale (or scytale) to obscure recognition of written communications. The marriage of ciphers and electromechanical encryption devices prior to World War II created an explosion in the science of cryptography. But German military reliance on their Enigma encryption device was compromised by British military intelligence.

In today's world, computers have increased the strength of encryption technologies while also providing the raw horsepower to quickly employ multiple forms of decryption techniques. To ensure that a recipient of encrypted information would be able to decrypt it, cryptographers in the United States (and earlier in a secret United Kingdom project) developed the concept of public key encryption, which enables encryption by a shared "public key" to be decrypted by a nonshared "private key."

In the early 1970s, the National Institute of Standards and Technology (NIST) in the United States solicited development of what ultimately became the Data Encryption Standard, or DES, for encryption of nonclassified U.S. government data. A stronger technique, Triple DES, resists "brute force" attacks by encrypting each message block three times, effectively creating a 168-bit key.

Triple DES, or 3DES, is widely used today but is rapidly giving way to the Advanced Encryption Standard, or AES, which was adopted as the U.S. standard in 2002 following a five-year development and evaluation process by NIST. AES provides for encryption key sizes of 128, 192 and 256 bits.

Data in the Line of Fire

Today, encryption is used not only to transmit information, but also to store information so that it cannot be compromised inadvertently or maliciously. But as enterprises have become more attuned to the need to shield information to comply with a host of regulations and laws covering financial information, privacy and so forth, they have recognized that it is practically impossible to build an impenetrable fortress around their data.

Encryption is becoming increasingly required on individual user devices for employees and contractors, due to the risk of network intrusion and potential compromise

outside the organization's network protection. Many organizations have become cognizant of the risk of unencrypted data on laptop computers that can be misplaced or stolen and network-attached devices that can be accessed externally or exposed to internal threats.

Organizations also need to be able to shield information on shared devices, to ensure that each user has access only to the information that is appropriate to his or her task. For example, an IT worker or contractor performing maintenance on the CEO's laptop should not be able to read confidential documents.

Historically, organizations have relied on two encryption techniques:

- **File/folder encryption**, which encrypts just the files and folders that are specified
- **Full disk encryption**, which encrypts every bit on the hard drive, including the operating system

Both of these techniques have some inherent strengths, but are also fraught with problems for the modern enterprise. Worse, their usage may create a false sense of security and cause users and IT organizations alike to engage in risky behavior and processes.

File/folder encryption is without a doubt the simplest way to encrypt information, and it places little if any burden on performance because it does not encrypt the operating system. This technique encrypts only the specific files and folders as designated by the user or administrator. The downside is that users can easily store data in the clear in unencrypted folders, placing too much control in the hands of the user and negating the value of the protection.

The advantage of full disk encryption is that every bit of data on the disk is encrypted regardless of where the data resides, including the operating system. Unfortunately, full disk encryption poorly aligns with the operational realities of today's enterprise: the need to lower IT overhead, protect against insider threats, ensure worker productivity, and centrally manage and enforce security.

At a minimum, full disk encryption creates training issues with end users who must learn how to walk through a "preboot authorization" process to "unlock" access to the drive on their system. According to a leading industry analyst, PCs using this type of encryption are at a high "brick rate"—meaning the system is now about as useful as a brick—because bit errors resulting from failed disk clusters and sectors can result in the inability to recover data.

The recovery process for a full disk encryption system, even when successful, can effectively compromise organizational security. That's because to recover a system, an IT staffer, contractor or service bureau will have to decrypt the entire volume and

>> **“Protecting endpoint data requires more than just simply encrypting all bits on disk. You also need to make sure you are protecting existing operational processes and ensuring user transparency.”**

Chris Burchett

Chief Technology Officer
CREDANT Technologies, Inc.

stream that data off to another drive. “That’s a rather serious issue,” says Chris Burchett, chief technology officer at CREDANT Technologies, Inc. “Now you’ve got the extra copy of decrypted data lying around and the IT person has access to all the information that was on that system. How do you make sure that extra copy is deleted or destroyed before somebody else can access it? Do you have a control process over that? In terms of operational security that’s a really big, glaring hole.”

Full disk encryption also places a significant burden on IT organizations when it comes to managing the encryption key that secures the drive and all the data on it. Many systems using such a device-centric technique require the end user or admin to copy an encryption key manually to a USB drive or a shared network store. “There’s a huge operations gap if there are shares that are open and somebody can get access to all of your keys,” says Burchett. If IT does not have control over the keys, and there’s no automatic key escrow in place, the organization runs the risk that the key can’t be accessed, which could result in the inability to recover the information locked on that device.

Full disk encryption technology also fails to protect data from illicit administrative access, or insider threats. Because it supports only a single key for the drive, all users have the same data access privileges, regardless of their role in the organization. The IT administrator mentioned earlier, for example, could not be prevented from accessing the CEO’s sensitive data while repairing, patching or updating it. Nor could a contractor with temporary access be restricted only to the files and data necessary for the task at hand. To protect against insider threats and other compromises, organizations need tighter security with more flexibility—a data-centric, not device-centric, solution.

A flexible approach with assured security meets the needs of today’s organizations, where data is constantly on the move and outside of the firewall. IT needs to assure both users and auditors that it can provide secure access to mobile and remote users.

Changing Needs for Security Management

Recovery and key management issues aside, full disk encryption makes it difficult to manage security and support devices from a single, centralized platform. As with patch management, this outdated technology can actually promulgate risky procedures during the preboot authorization process.

Security experts agree that one of the most crucial elements of security management today is the ability to implement operating system and application patches as quickly as possible to eliminate any discovered vulnerabilities before they can be exploited.

The preboot authentication of full disk encryption systems can prevent patch management systems from operating in the way they were intended to. That’s because

>> **“Our goal was to crack a laptop that was lost or stolen. We came up with attacks to beat the network to death, but when it came to a stolen laptop penetration, Credant was unbeatable in this game.”**

Randall K. Nichols

Chairman

INFOSEC Technologies

patches typically require reboots, sometimes several, and can't be completed unless there is a user present to enter the preboot password.

Some encryption vendors will provide a work-around to the patch management issue by allowing IT to configure a system to reboot a designated number of times without requiring preboot authentication. “Now that means the key is open automatically, and clearly that's not a state of encryption,” Burchett says. “Now you're in the realm of obfuscation. They're trying to conceal your data, but it's not encrypted because the key is stored there or the credential to open the key is stored there.” For some companies, Burchett adds, that may actually create periods when the organization is not in compliance with particular regulations or laws and may trigger a requirement to notify regulatory authorities if devices are lost while keys are open.

“Protecting endpoint data requires more than just simply encrypting all bits on disk,” Burchett says. “You also need to make sure you are protecting existing operational processes and ensuring user transparency. To be compliant with some regulations, an organization also needs integrated auditing and reporting capabilities so that in the event a device is actually lost or stolen they are able to report that the device was in fact encrypted, that the data is protected, and there's no subsequent risk involved. In some instances, IT needs the ability to remotely 'kill' the device. Either way, a single platform of device detection, policy enforcement for multiple types of users, and audit and reporting capabilities is most effective.”

Data on the Move

For most organizations today, the mobile workforce has exacerbated security concerns. Many are only just coming to grips with laptop security. But there is just as great a risk with other intelligent devices, such as smartphones, and easy-to-conceal peripheral devices such as USB memory sticks and flash memory cards.

At a major Midwestern bank, the IT team recognized in 2004 that it needed a more effective means to deal with the issues of mobile security. “Like most companies our size, and especially being spread across several states, we had laptops that just would walk every year—stolen or lost, four or five laptops every year,” according to the IT manager, who asked not to be named. “We just saw that we really could have a situation where we lose some sensitive data, and we wanted to be way out in front of that.”

The bank selected CREDANT Mobile Guardian (CMG) software for endpoint data protection. During the product evaluation process, IT initially focused on full disk encryption vendors. “Unfortunately, with a lot of those solutions, they did not have the ability to secure multiple different platforms in a single console, and one of the requirements I had early on was a single console,” says the manager. “I wanted to be

able to secure my laptops, secure my desktops, secure USB drives; I wanted to have a central console and I can look at everything.”

The organization also wanted to avoid preboot authentication. “That is a massive change to the end user that we didn’t like; we wanted to minimize the impact to the end user,” he says.

Endpoint Data Protection

Data security has evolved beyond simply securing “bits on disks.” To ensure data protection in today’s dynamic IT environment, leading analysts recommend that security protects what matters most: the data. This requires a solution with a single, integrated security architecture and a data-centric, policy-based encryption approach that can be consistently enforced wherever the data resides—across heterogeneous endpoint device types, operating system platforms and end users.

With its history in securing endpoint devices, CREDANT concluded that the paradigm must shift from full *disk* encryption to full *data* encryption. While full disk encryption technology may, on the surface, seem like the easiest and most comprehensive approach to data security, it is not the best methodology in the long run due to lack of protection against the insider threat, as well as significant manageability, recovery and usability issues.

Enterprises today need a full data encryption solution that simultaneously meets their security, IT operations and compliance needs. CREDANT responded by developing CREDANT Mobile Guardian (CMG).

INFOSEC Technologies, a counterterrorism/counterespionage firm specializing in sensitive investigations and computer security countermeasures, performed a penetration test and security review of CREDANT Mobile Guardian with full data encryption as it was under development, according to INFOSEC Chairman Randall K. Nichols, who is also chair and director of CyberSecurity, Computer Forensics and Information Assurance, at Utica College in New York. Nichols says that over a

Encryption Feature Comparison

	Support unattended (WoL) patch management processes	Support existing data recovery, IT and help desk processes	Encrypt all sensitive data, known or unknown	Protect privacy of individual users’ data on a multiuser device	Protect data on noncorporate devices (affiliates, personal)	Ensure that solution is transparent to end users	Easily managed within a DLP/policy-based environment
CREDANT Mobile Guardian	✓	✓	✓	✓	✓	✓	✓
Full Disk Encryption	✗	✗	✓	—	—	✗	✗
Full File Encryption	✓	✓	✗	✓	—	✓	—

>> **Enterprises today need a full data encryption solution that simultaneously meets their security, IT operations and compliance needs.**

four-month period, a three-person team attempted to crack the system with the most sophisticated tools available. "Our goal was to crack a laptop that was lost or stolen," Nichols says. "We came up with attacks to beat the network to death, but when it came to a stolen laptop penetration, Credant was unbeatable in this game."

The new CMG offers the single-system security architecture, single management console and transparent end-user interface to operate a scalable yet easily deployed and managed security solution. Driven by CREDANT's policy-based Intelligent Encryption technology, CMG is the only technology that provides multiple layers of security to meet the needs of data and device protection balanced with an organization's operational processes and end-user needs for transparency and ease of use. CMG employs five layers of Intelligent Encryption to tighten security, simplify management, and ensure greater end-user acceptance:

- **User data encryption** protects each user's data from being accessed by any other, even if they are sharing a PC.
- **Application data encryption** protects all data written by specified applications, irrespective of where and how the data is written.
- **External media encryption** protects data written to external media, including USB memory sticks, iPods, CDs and DVDs, and so forth, to reduce data leakage threats.
- **Common data encryption** protects data from being access by an unauthorized user.
- **System data encryption** protects system and program files on a hard disk that is not protected by other encryption layers.

Because CMG does not encrypt the operating system, it doesn't create a drag on system resources. Plus, it can perform an initial encryption of a loaded disk drive in a fraction of the time that full disk encryption requires.

Unlike file/folder encryption, CMG technology is foolproof when it comes to end-user compliance. "Unlike file/folder technologies, CMG is a file system filter driver that catches all reads and writes to the file system, not just the 'magic folder' you set up to be encrypted," says Burchett. CMG requires no replacement or alteration of the master boot record, therefore avoiding interoperability issues with existing applications.

CMG ensures that IT personnel, whether in-house or outsourced, can access a PC for routine maintenance and recovery processes without being exposed to sensitive data, thereby protecting the organization from insider malicious activity. CMG supports multiple keys for data privacy, protecting a user's folder from access by other users sharing devices. It also features automated encryption key escrow that guarantees data recoverability from the moment encryption begins.

Ensuring protection for all sensitive data, CMG also protects local and domain credentials, as well as paging files and temporary files and folders. In addition, the system collects administrative proof that data is encrypted and in compliance.

Conclusion

CREDANT's integrated policy-based platform provides comprehensive controls to ensure data is always secure across a broad range of devices—without compromising IT operational processes or security. CMG comprises security policies that enforce any or all of the five levels of Intelligent Encryption and that allow all sensitive data to be encrypted automatically, wherever that data resides. CREDANT security provides the encryption simplicity associated with full disk encryption technologies, but without the associated headaches, and with the assurance that endpoint devices and media adhere to enterprise security policies.

Pete Bartolik is a Hopkinton, Mass.-based freelance writer.