The most secure EFSS solution, period.

CYPHRE'S BLACKTIE™ SECURITY:

HARDWARE GENERATED ENCRYPTION/PROTECTING SESSION SECRETS

WHITEPAPER

Author
Jack Smith

§ ABSTRACT

Cyphre's BlackTIE™ security protects enterprise data and adds strong cryptographic barriers around each piece of data to prevent a security breach. This paper discusses attacks targeting encryption keys and validates Cyphre's BlackTIE™ protection against those attacks.

§ INTRODUCTION

Enterprise data must be protected by a robust computer security and data protection solution. Continuous and rapid advances in computer security are necessary to keep up with the velocity and volume of malicious attacks. New data security breaches regularly make national headlines. Quantifying the problem illustrates the enormity of the problem as hundreds of millions of confidential enterprise records are exposed by each security breach.

This study discusses and verifies Cyphre's BlackTIE™ protection of encryption keys and cryptographic secrets.

This real-world test was performed on production COTS infrastructure using reproducible internal and external attack vectors. Without Cyphre's BlackTIE™ security, it was confirmed that:

1. Internal attacks by malicious software render encryption worthless.
2. External attacks targeting memory buffers were able to expose encrypted session keys.

With Cyphre's BlackTIE™ security, both the internal and external attacks against encryption secrets were 100% prevented, resulting in no exposure of encryption keys.

§ PROTECTION

The rapid pace of innovation and development in cloud applications, server virtualization and mobile devices creates new vulnerabilities every day. The unfortunate truth is that even when all of the best security practices are in place and followed, enterprises are at risk of security breaches caused by previously unknown, Zero-Day vulnerabilities.

Furthermore, a single breach of security typically allows the malicious perpetrator to access huge volumes of sensitive data. The impact of each security breach is enormous and increasing, causing significant financial, compliance and public relations damage to enterprises.

To combat and address these risks, Cyphre's BlackTIE™ security features have been specifically designed to protect data from exposure and dramatically minimize the data leakage if such an event did occur.

§ ENCRYPTION

Encryption of data is one of the most effective techniques used by data security experts to protect enterprise information. The mathematical locks used by encryption are amazingly strong, and while it is easy to unlock the data using the key, it is nearly impossible to decrypt the data without it. Once data is encrypted, use of the data is authorized and managed by controlling access to the encryption key.

The industry has proven that this approach is powerful and effective, but does have an inherent weakness. Simply put: the key must exist, it must be stored somewhere, and it needs to be accessible when locking or unlocking the data. Malicious attackers are intelligent and clever; they know they need to steal the encryption keys, and have devised many attacks specifically targeted at key theft.

§ SOFTWARE BASED ENCRYPTION

The overwhelming majority of systems use software-based encryption techniques. These systems are effective, but because the encryption software executes from memory and stores all of its data in memory, exposure of that memory to a malicious attacker completely defeats the protection. Numerous published attacks are focused on stealing secrets and encryption keys from memory, and these attacks have shown to be very effective.

§ HARDWARE BASED ENCRYPTION

Cyphre's BlackTIE™ security protects the encryption keys in main memory by using protected hardware-generated and protected keys, as well as hardware-based encryption. If an attacker is able to access the server's main memory, a Cyphre BlackTIE™ Key is still protected and is unusable by an attacker.

§ SUMMARY

At this point, the landscape of existing encryption-based protection has been laid. It is clear that encryption techniques have incredible value, and strength, but the current status quo needs to be improved. The encryption itself is very strong, but the numerous attacks against server memory are compromising software based techniques.

In addition to its many other benefits, Cyphre's BlackTIE™ security resolves these deficiencies by processing the keys and encryption in a hardware layer that is not exposed to main memory or vulnerable to memory attacks.

§ VALIDATING THE PROTECTION

In order to demonstrate the value and effectiveness of Cyphre's BlackTIE™ security, we performed real-world testing on production COTS infrastructure of systems vulnerable to the Heartbleed Bug. Our tests specifically looked for exposure of encryption keys and cryptographic secrets, with and without the benefits of BlackTIE™ security.

Heartbleed is a well-known OpenSSL vulnerability that enables malicious code to view security related memory buffers. The OpenSSL bug existed for a long time, and the level of expertise required to exploit the vulnerability was very low. The Cyphre infrastructure and hardware-based encryption are designed to prevent attacks, like Heartbleed, which leak secrets or expose memory to attackers.

Simply put, Heartbleed allows attackers to steal your keys. With those keys, they can unlock your data.

§ TEST METHODOLOGY

Three production COTS servers were configured, all vulnerable to Heartbleed (CVE-2014-0160), but with all other security patches in place. One server was configured to use Cyphre's BlackTIE™ security, and the others were used as an experimental control.

Each system was subjected to a variety of internal and external attackers exploiting the OpenSSL vulnerability, and attempting to view memory. Internal attackers include any malicious agent running on the local infrastructure, and external attackers are attempting to penetrate the security from outside the local network.

The data returned from each attack was stored and later scanned for encryption keys. The scan specifically looked for TLS encryption keys, including the TLS master secret. These protect the privacy of the encrypted communication tunnel between the client and server.

§ TARGET SYSTEM

The test systems were freshly installed systems with all known patches. We used readily-available tools and techniques to perform these attacks.

Setup:	Three (3) platforms were configured Each platform was configured as both a web server and as a web client All software was fully patched and all software was properly configured
OS:	Ubuntu 14.04.2 LTS
Web Server:	Apache/2.4.7
TEST	
Internal:	Malware scanned server memory before, during, and after client connections
External:	Malware used Heartbleed to expose OpenSSL memory buffers
Post-Process:	Scan captured data for TLS Session Keys and TLS Master Secrets

§ INTERNAL ATTACK METHODS - GENERAL INFORMATION

Internal attacks come from any malicious agent with access to run directly on the same infrastructure. Many of these breaches start as minor intrusions that are then escalated by the malware to achieve full-privileged access running directly in the operating system.

One of the often touted benefits of virtualization is complete isolation of the guest operating systems from each other. Unfortunately, this isolation is not nearly as complete as the industry wants it to be, and several effective attacks have been published and demonstrated that breach the guest isolation.

With the continuous expansion of cloud services and virtualization, the challenge of securing critical virtual infrastructure is increasing in complexity and cost. Vulnerabilities have come to light that enable attacks from infrastructure and virtual machines entirely outside of the enterprise control that can breach security and access protected data.

§ INTERNAL ATTACK - WITHOUT CYPHRE'S BLACKTIE™ SECURITY

For our internal attack testing, we monitored the OpenSSL process and scanned the process memory for usable cryptographic secrets.

Results:	100% exposed 158,064 tests were attempted 158,064 of tests succeeded at extracting the cryptographic secrets

Every test was successful at revealing encryption keys. While this sounds dramatic, it is not surprising, and may be considered obvious to a security researcher. This test highlights that exposure from internal attacks is extreme. An attacker or malicious insider that can run directly on a machine can see every piece of data in main memory.

§ INTERNAL ATTACK - WITH CYPHRE'S BLACKTIE™ SECURITY

The Internal attack test was repeated with Cyphre's BlackTIE™ security enabled. One of the important features enabled is the use of BlackTIE™ Keys for TLS sessions, which enables the security engine to protect cryptographic secrets from main memory attackers, regardless of their privilege level.

Results:	0% exposed 224,064 tests were attempted Zero (0) of tests succeeded at extracting the cryptographic secrets

This test is a perfect example of the benefit of Cyphre's BlackTIE™ keys. The Heartbleed vulnerability was still present in this system, but the memory buffers exposed simply did not contain the TLS master secret. With Cyphre's BlackTIE™, these encryption keys are protected.

§ EXTERNAL ATTACK METHODS - GENERAL INFORMATION

External attacks come through the internet connection and attempt to penetrate the server from the network. Attacks of this sort occur constantly from all over the world.

Every cloud service is exposed to attack, simply by virtue of being available on the internet.

§ EXTERNAL ATTACK METHODS - WITHOUT CYPHRE'S BLACKTIE™ SECURITY

For our external attack testing, we repeatedly used the Heartbleed vulnerability and captured the data returned from the target systems. This attack was concurrent with valid traffic and client connections.

Results:	1.11% exposed 158,064 tests were attempted 1,748 of tests succeeded at extracting the cryptographic secrets

Although 1% may initially sound low, this is a surprisingly high result. Servers are attacked hundreds of thousands of times per day. If even 1% of those succeed, the server security will be breached quickly.

§ EXTERNAL ATTACK METHODS - WITH CYPHRE'S BLACKTIE™ SECURITY

The external attack test was repeated with Cyphre's BlackTIE™ security enabled. One of the important features enabled is the use of BlackTIE™ Keys for TLS sessions, which enables the security engine to protect cryptographic secrets from memory buffer attacks and leaks like Heartbleed.

Results:	0% exposed 158,064 tests were attempted Zero (0) tests succeeded at extracting the cryptographic secrets

This demonstrates the effectiveness of Cyphre's BlackTIE™ security. By protecting encryption keys, Cyphre prevents attackers from eavesdropping on the client-server communication.

§ TEST CONCLUSIONS

Without protecting memory, an internal attacker is able to steal all the secrets, and an external attacker is able to steal secrets in slightly more than 1% of attacks. These examples are simply two of many possible threats that create risk to enterprise data. New attacks will continue to be discovered, published and exploited.

Overall, these tests show how absolutely critical it is for enterprises to protect servers from malicious attackers. Cyphre's BlackTIE™ security adds this layer of protection, providing deeper and stronger levels of data security than conventional methods.

For enterprises needing to address current and forthcoming regulatory and compliance requirements, Cyphre's BlackTIE™ encryption technology ensures an unprecedented level of security and protection.

§ BIBLIOGRAPHY

http://www.coloradosupport.com/how-easily-can-hackers-steal-information-by-exploiting-heartbleed-security-watch-tests-the-vulnerability-to-find-out/

https://blog.cloudflare.com/the-results-of-the-cloudflare-challenge/

https://blog.cloudflare.com/answering-the-critical-question-can-you-get-private-ssl-keys-using-heartbleed/

http://securitywatch.pcmag.com/security/322691-heartbleed-is-scarily-easy-to-exploit
https://twitter.com/1njected/status/453797877672706048

rowhammer

http://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html
http://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf

CVW-2012-0056

http://blog.zx2c4.com/749

Cache attack to recover Encryption Keys

http://www.daemonology.net/papers/htt.pdf

Heartbleed CVE-2014-0160