DISPERSED DATA ENCRYPTION:

THE KEY TO BETTER INFORMATION SECURITY

WHOOSH®

PROTECTING AND POWERING YOUR DATA®

White Paper | March 2016

EXECUTIVE SUMMARY 3
ABOUT THE AUTHOR 3
DEFENSE IN DEPTH 5
GENUINE DEFENSE IN DEPTH 6
JUST ENCRYPT EVERYTHING! 7
DEVELOPING BETTER ENCRYPTION 8
TACKLING COMPROMISED CREDENTIALS 11
CONCLUSION 12
ABOUT FHOOSH 13

EXECUTIVE SUMMARY

Many enterprises are beginning to operate on the assumption that their network has already been compromised and are adjusting their security strategies accordingly. Most certainly need to upgrade their detection and containment capabilities but security teams also need new technologies to be able to implement basic security, such as data encryption, far more rigorously. This white paper looks at the problems of current information security strategies and why encryption and other technologies have failed to protect enterprise data.

It then explores a more robust approach to encryption, developed by San Diego-based cybersecurity firm FHOOSH, that breaks data apart and separately encrypts it before storing it in dispersed locations, leaving it completely worthless to hackers. FHOOSH technology means protecting data can actually be easier, faster and more efficient than leaving it in plaintext, and with inherent detection and multilayered authentication, it delivers encryption that is robust at all levels.

ABOUT THE AUTHOR

Michael Cobb, CISSP-ISSAP, is a 20-year veteran of IT security with a passion for making industry best practices easier to understand and implement. As an advisor on security controls and information-handling practices to companies and government agencies large and small, Cobb has helped numerous organizations achieve ISO 27001 certification and successfully migrate data and services to the cloud. Cobb has also worked with CESG, the information security arm of the United Kingdom's GCHQ (Government Communications Headquarters), to promote security best practices in government. A renowned author and presenter, Cobb has written numerous technical articles and webcasts for leading IT publications, as well as a book on IIS security. He also has been a Microsoft Certified Database Manager and a registered consultant with the CESG Listed Advisor Scheme (CLAS).

Current information security strategies are clearly failing to protect enterprise data. A wide range of cybercriminals continue to compromise enterprise networks and steal terabytes of data from organizations in every sector of the economy on a regular basis, despite layers of defensive technologies. Further stacking the odds in favor of the cybercriminal and against security teams, is the expansion of the attack surface that must be defended due to trends in technology such as open network architectures, BYOD (Bring Your Own Device), IoT (the Internet of Things), cloud computing and big data. New approaches and technologies are needed to secure today's more exposed and accessible data. Many enterprises are beginning to operate on the assumption that their network has already been compromised and are adjusting their security strategies accordingly. This has led many to increase their monitoring and threat detection capabilities, but the cybercriminals still remain ahead of the game. Most enterprises certainly need to upgrade their detection and containment capabilities but they also need to implement basic security, such as data encryption, far more rigorously.

Encryption should be the ultimate safeguard to protect stolen data, which is why it's mandated in so many compliance and regulatory standards to ensure data confidentiality. HIPAA and California Senate Bill SB 1386 are explicit in noting that notification of a data breach is not required if the information is encrypted. However, performance, integration, analytics and reporting concerns have deterred many from implementing encryption as a standard practice. When data has been encrypted, poorly configured deployments, lax key management, or compromised credentials have enabled attackers to routinely defeat this layer of defense.

Sensitive and valuable information needs better protection from compromised and misused credentials if encryption is going to fulfill its role of ensuring confidentiality.

But encryption executed correctly can be the answer to protecting data when a system is compromised. This white paper looks at the problems of current information security strategies and why encryption and other technologies have failed to protect enterprise data. It then explores a more robust approach to encryption that breaks data apart and separately encrypts it before storing it in dispersed locations, leaving it completely worthless to hackers. Developed by San Diego-based cybersecurity firm FHOOSH, the design of the encryption process also creates an innate capability to detect unauthorized access and is faster than storing data unencrypted. Promising easy integration with all types of data stores, could it be that FHOOSH encryption finally delivers data security that enterprises so badly need?

DEFENSE IN DEPTH – WHY ISN'T IT WORKING?

The information assurance concept of Defense in Depth is generally accepted as a comprehensive and best practice approach for protecting IT systems and the data they process and store. Deploying multiple and varied security controls throughout the network prevents direct attacks against critical systems, and provides redundancy should one control fail or a vulnerability be exploited. In theory it should make an IT system resilient to attack, but hackers continue to steal supposedly well-protected data from the world's biggest organizations. And the situation is getting worse. According to the Privacy Rights Clearinghouse, 53 million data records of U.S. residents were exposed due to security breaches in 2005. The number of breached records for 2015 is already over 153 million. According to the 2009 Verizon Data Breach Investigations Report, 285 million records were compromised in 2008. The 2015 report puts the figure for 2014 at over 700 million records, and 2015 looks to be just as bad following major breaches at Anthem, Ashley Madison, Office of Personnel Management, Premera and VTech.

Security teams have to defend all possible entry points and attack vectors, while the attacker has to find and exploit just one vulnerability.

The main reason for the continued success of cybercrime is that security teams have to defend all possible entry points and attack vectors while the attacker has to exploit just one vulnerability. This asymmetry highly favors the attacker, particularly as the number of network entry points continues to expand due to the adoption of BYOD, cloud computing and generally more open and collaborative networks. There will always be someone, in-house or a third-party supplier, who can be lured into visiting a booby-trapped website, tricked into opening a malicious Word document or simply revealing their network credentials.

Vulnerabilities, design flaws and configuration errors in the underlying systems and applications can all be exploited to circumvent perimeter controls. For example, Bitdefender suffered a data breach because a server was operating with an outdated software package that contained known flaws – this was blamed on human error – while a recent targeted attack run by the APT28 hacking crew exploited two zero-day flaws to compromise an "international government entity."

Many IT systems over rely on or overestimate the level of protection access control lists (ACLs) or rules-based access control technologies can provide. The management and administration required to keep ACLs current is daunting enough but cloud computing, new data types, and increased third-party access are making it a herculean task leading to inevitable errors and oversights. According to research by Intermedia and Osterman Research, 89 percent of employees leave their jobs still with a valid login and password to at least one business application belonging to their former employers. A key failing of many preventative controls is that malicious users can easily bypass them if they have or can obtain the credentials of a system administrator or valid user. In the Target data breach a phishing attack compromised the login credentials of a heating and cooling contractor servicing Target stores. This allowed the hackers to access Target's network and upload their malware to cash registers within Target stores, eventually stealing millions of credit card numbers.

There is also the problem of insider misuse which preventative defenses can do little to stop. According to Verizon's 2015 Data Breach Investigations Report 55 percent of insider misuse incidents involved abuse of the access individuals have been entrusted with and occur in virtually every industry; and for the first time regular end users are at the top of the list of offenders. Some of the largest data breaches yet seen have been carried out by insiders. For example, the data stolen in 2014 by an insider at the South Korean Credit Bureau eventually compromised the identities of over 40 percent of all South Koreans. And of course there's Edward Snowden, the NSA contractor behind one of the largest leaks of classified information in U.S. history.

GENUINE DEFENSE IN DEPTH

Defense in depth was originally a military strategy aimed at delaying, rather than preventing, the advance of an attacker. Given the failure of perimeter- and protection-centric security models, many security experts are now advising enterprises to develop security strategies based on the assumption that hackers will attack and break into their networks, and shift focus towards a detection and containment model. Prevention technologies such as firewalls, intrusion detection systems and antimalware solutions will always be the frontline protecting a network's resources, but enterprises need to revisit the layers of their defenses that buy an organization time to detect, contain and respond to an attack, thereby reducing and mitigating the consequences of a breach.

One big advantage of this approach is that it puts the attacker at a disadvantage. It is now the security team who only has to find one clue that will reveal their presence while the attacker has to evade detection the entire time. New technologies are emerging that claim to be better at detecting malicious activity within a network but it's still a game of cat and mouse and one which the hackers continue to excel at. This is why encryption is so important because even if an attacker manages to access and steal encrypted information it is just worthless garbage. The network may have been compromised, the attacker may be well hidden, but nothing of value can be stolen.

JUST ENCRYPT EVERYTHING!

Encrypted data is intrinsically protected as it is unreadable. This is why encryption is the cornerstone of the Payment Card Industry Data Security Standard, which requires customer data to be encrypted while it is both stored and in transit. Many businesses are now including clauses in contracts with their partners requiring that sensitive data, especially that which contains personal information about their customers or employees, must be encrypted. So why don't we just encrypt everything and forget about other safeguards like monitoring and detection? Well, encryption has also been failing as a security control, and for a variety of reasons.

Do security teams need new technologies, new strategies or just to be able to do the basics better?

One reason encryption hasn't protected stolen data is because it was never encrypted in the first place! This can be attributed to poor practice or poorly configured encryption schemes. In the Bitdefender breach, encryption wasn't used to protect its customers' most sensitive data such as usernames and passwords allowing the hacker to use the stolen credentials in attacks against some of Bitdefender's clients. Incorporating encryption and hashing techniques can be complicated and tedious so application developers often don't bother or only use it for the most sensitive of data, leaving information that is still of value to an attacker unencrypted. A recent survey by UBM Tech found that 66 percent of respondents did use data encryption but its use on internal networks was patchy at best. A quarter of those respondents who didn't encrypt their internal traffic said that performance degradation was their biggest concern, with infrastructure shortcomings, costs and key management other common reasons given.

A crucial facet of protecting data with encryption is key management. In a survey by Venafi, more than half of the companies in the report did not know how many keys and certificates they had, or where they were stored. Equally alarming was that most security professionals didn't know how to respond if encryption keys were compromised during a breach and only eight percent said that they would replace potentially compromised keys and certificates.

Encryption can be a drag on performance and there can be surprising differences in the performance of encryption libraries even when performing the same type of encryption. In one test the difference between two 256-bit AES encryption libraries was 100 fold – that equates to 10 hours of batch processing versus 5 minutes. Also the number of columns in a table which are encrypted will affect performance as each read of a row in the table will result in separate decryption calls. The interface to the key management server represents another potential drag on performance – keys should never be stored on the same server as the encrypted data. While a single key retrieval from a key server may take just a few milliseconds, the performance impact can be dramatic when thousands of key retrievals are needed from a key server. To reduce key retrieval times many systems cache encryption keys but if this isn't done securely they can be exposed to an attacker.

DEVELOPING BETTER ENCRYPTION

The growing need for effective encryption solutions that are not only robust but easy to implement and manage has seen various new or improved technologies emerge. To try and reduce the likelihood of another Heartbleed or POODLE scenario the IETF's Using TLS in Applications working group is providing common guidelines and best-practices for using TLS in applications. The infamous Heartbleed bug was a result of a surprisingly small bug in OpenSSL's implementation of the TLS heartbeat mechanism, and a variant of the POODLE attack exploits certain implementations of the TLS protocol which don't correctly validate encryption padding. By specifying a set of best practices the IETF hopes to make it easier for developers to use TLS without the risk of leaving encrypted network traffic open to attack.

Microsoft is also hoping its SQL Server 2016 Always Encrypted feature will make it easier for developers to keep sensitive data encrypted. The process of encrypting and decrypting data is handled at the database driver level so the database never sees unencrypted values of sensitive columns, though to maintain reasonable performance, non-sensitive columns such as primary keys have to be left unencrypted.

The Trusted Platform Module (TPM), an international standard for a secure cryptoprocessor, has been around for a while and is now appearing on millions of devices from computers to mobile phones and even automotive systems. These secure integrated circuits provide hardware-based cryptographic and security-related functions such as system integrity checks, disk encryption, and key management, delivering improved protection for any processes that need encryption services without inconveniencing the user.

FHOOSH high performance technology breaks apart, disassociates, separately encrypts and disperses data with the added benefit of innate threat detection.

As ease of use and speed are key requirements for encryption to be more widely adopted, FHOOSH has designed its patent-pending bankLevel+™ cybersecurity from the ground up to deliver high-speed encryption as part of a comprehensive system. FHOOSH secureObjects™ is the first product to incorporate bankLevel+ technology in a single deployable package. Built around standard interfaces including the Amazon S3 API, support for Python and low-level shell scripting, FHOOSH secureObjects aims to solve the issues which have left many enterprise encryption projects floundering.

The open architecture format provides a number of implementation options from desktop applications to enterprise processing engines. For example, FHOOSH secureObjects may be directly embedded in a standalone application providing an application developer with immediate out-of-box API functionality for persistent encrypted object storage in the cloud or locally, and in either a relational or non-relational database. Developers need not worry about spinning up their own database layer and adding encryption functionality from scratch.

For Web application development, FHOOSH secureObjects runs as any other server-based library would. The secureObjects API exposes a wide variety of API calls (including various PUT, GET and DELETE calls) to a data store, thereby providing the Web application an entire suite of functionality related to secure data access. Finally, support for Python and front-end scriptability means that FHOOSH secureObjects could be installed as a REST-based service or embedded in-line within an existing infrastructure data pipeline.

What makes FHOOSH encryption technology truly different though is that it encapsulates decomposition and dispersal while actually reducing data storage and retrieval times. Independent performance tests conducted by managed security services provider LP3-SecurIT showed FHOOSH secureObjects able to encrypt and store objects, sized 1GB and larger, 10 to 15 times faster than when using standard encryption. It also consistently achieved PUT speeds more than six to eight times faster than when storing data without encryption. Such impressive speeds not only improve the user experience but lower the total cost of ownership, and enable better returns on existing infrastructure investments. (Test report results can be downloaded here.)

Furthermore, because the encrypted data is dispersed and stored in a unique manner FHOOSH has been able to build detection algorithms into the architecture to quickly and easily recognize abnormal access behavior such as incorrect compound key combinations. This triggers an automatic rotation of encryption keys and alerts to admin staff, dramatically reducing the ability and time of hackers to access FHOOSH-protected data.

FHOOSH ENCRYPTION IS FAST, VERY FAST

Independent performance tests confirm that FHOOSH secureObjects consistently achieves PUT speeds more than 6–8x faster than storing data without encryption, and 10–15x faster than storing data using standard encryption for objects sized 1GB and larger.

The point at which data is decrypted for authorized use is dependent on infrastructure demarcation points and use-cases: Web page form fields on a user's validated browser session, for example. Another scenario would be decrypted data directly ingested through a data pipe behind a firewall within a customer's infrastructure. To enable complex data analytics and reporting on encrypted information, a proprietary FHOOSH security algorithm tags analytics and reporting fields for fast access while maintaining data security and integrity.

TACKLING COMPROMISED CREDENTIALS

It's easy to fall into the trap of assuming data is safe just because it's encrypted, but compromised credentials can expose encrypted data. In the Anthem breach for example, a lot of newspaper headlines criticized the fact that the data was stored unencrypted. However, encryption alone wouldn't have prevented the attack from being successful, as it was carried out with stolen database administrator credentials, which typically include the ability to decrypt data. This and other large-scale breaches at Ashley Madison, the Office of Personnel Management and Experian show that sensitive and valuable information needs better protection from compromised or misused credentials if encryption is going to fulfill its role of ensuring data confidentiality.

FHOOSH implements several best practices to counter the threat of credential misuse and abuse including compound key access to gain entry.

FHOOSH implements several best practices to counter the threat of credential misuse and abuse. At a minimum it requires two Administrative logins (a superior and a subordinate), each contributing a portion of the required access key to gain entry. This concept is called "compound key" access and forces multiple independent logins to provide correct credentials. If an attacker manages to compromise one set of credentials, access to FHOOSH-protected data still won't be granted.

Encryption keys both for user data and for data-store credentials are stored in a separately protected secureObjects instance. Called secureKeys™, it is designed specifically for integrated user account and key management. One of its unique features is the use of key rotation algorithms to change keys periodically, or quickly rekey credentials of administrators when a threat is detected. Keys are stored using the same FHOOSH methods that are used for storing data, that is, keys are disassociated from the underlying data, decomposed, separately encrypted and dispersed. Additionally, FHOOSH incorporates is own Multi-Factor Authentication (FMFA™) system that integrates with secureKeys to provide another level of required security protocols in the authentication and authorization process.

To ensure this new approach to safeguarding data is sound, FHOOSH has had it monitored and verified by leading security organizations.

Exclusive control of your encryption keys means you control who can see your data, no matter what happens to the data itself. It also means government and law enforcement agencies have to come to you with a request for the keys and not some cloud service provider. Although services like Google Cloud Storage, SkyDrive, Dropbox and Windows Azure have introduced or plan to introduce automatic encryption for all data at rest or in transit they still hold the encryption keys, so it's still possible that they can access data or provide the keys to government agencies who request them.

The FHOOSH user "passphrase" is not stored but must be supplied at time of access. The passphrase is one element of a set of required ingredients used to build the decryption keys. FHOOSH has proven the efficacy of using passphrases in this way when leading third-party security firms were unable to decrypt FHOOSH-stored data despite being given all data and source code, plus full administrative access.

CONCLUSION

Security teams need new technologies, new strategies and the ability to do the basics better if they're to avoid being at the center of the next data breach hitting the headlines. The importance of the protection that strong encryption provides has in recent years been overlooked in favor of attack prevention tools. While encryption alone doesn't make a system secure, it can keep information secure and should be an integral part of any data security plan. It can't prevent a Web application falling victim to a SQL injection attack or a database administrator being tricked by a phishing email, but it can significantly reduce the impact of the ensuing attack. Cybercriminals may be able to bypass or evade other security technologies, but properly encrypted data is resilient to all forms of attack.

Regulatory requirements, customer and partner demands all point to the need for an encryption platform that can handle a wide range of data types, applications and user populations. FHOOSH technology means protecting data can actually be easier, faster and more efficient than leaving it in plaintext and with inherent detection and multilayered authentication it delivers encryption that is robust at all levels. The fact that FHOOSH's encapsulation and data dispersion capabilities operate separately from the underlying encryption algorithms means they can be used with standard- and compliance-mandated algorithms, both now and in the future. With security built in from architecture to implementation, the FHOOSH platform can integrate with existing databases, object stores, file systems and unstructured data to safeguard assets without displacing existing infrastructure investments.

ABOUT FHOOSH

FHOOSH cybersecurity safeguards organizations' critical business and customer data from cyberthreats by storing it in a state that is worthless to hackers. Patent-pending FHOOSH technology breaks apart, disassociates, separately encrypts then disperses data, and it does so more than 6–8 times faster than storing data unencrypted. The system also immediately recognizes and reports intrusion attempts on FHOOSH-protected databases, object stores and file systems. Validated by leading cybersecurity firms, FHOOSH bankLevel+ security integrates with existing infrastructure. With security built in from architecture to implementation, FHOOSH protects and powers valuable information for corporations, institutions and government.

For more information,
contact:

FHOOSH, Inc.
7660 Fay Avenue, Suite H136
La Jolla, CA 92037

(888) 4 - FHOOSH
info@fhoosh.com
fhoosh.com