White Paper

Weaknesses of the Cryptographic Unit Service Provider (CUSP) Mode of Encryption

Why businesses should avoid using the CUSP mode on the IBM i and IBM z Platforms

THIS WHITE PAPER discusses several potential problems related to the use of the CUSP mode of encryption by business users. CUSP mode encryption is only implemented on IBM i and IBM z platforms, is not interoperable with other AES encryption modes. The CUSP mode of encryption has not been proposed or adopted as a NIST standard, and has not been generally reviewed or accepted by the professional security community.

Townsend SECURITY

www.townsendsecurity.com

724 Columbia Street NW, Suite 400 • Olympia, WA 98501 • 360.359.4400 • 800.357.1019 • fax 360.357.9047 • www.townsendsecurity.com

Abstract

When encrypting data, the most widely accepted cryptographic standard is the Advanced Encryption Standard (AES).

AES is defined by the National Institute of Standards and Technology (NIST) in the FIPS-197 standards document. AES supports eight modes of encryption, each of them having been extensively tested and vetted for security, recovery, and durability. When compliance regulations make reference to "industry standard encryption", they are referring to the encryption modes identified in the NIST documents on AES.
Other modes used in AES are not NIST certified and are not even certifiable. Some products offer only the CUSP mode of encryption, which is not NIST certified and not certifiable. CUSP mode encryption is only implemented on IBM i and IBM z platforms, is not interoperable with other encryption modes. The CUSP mode of encryption has not been proposed or adopted as a NIST standard, and has not been generally reviewed or accepted by the professional security community.

This paper discusses several potential problems related to the use of the CUSP mode of encryption.

Regulatory Standards & Compliance

There are many regulations that govern the protection of sensitive data, PCI DSS, PA DSS, HIPAA and HITECH, as well as a variety of state privacy regulations (45 states). All of these regulations recommend or require the use of encryption based on industry standards.

The industry standards most frequently referenced by these regulations are those published by NIST. For encryption, the Advanced Encryption Standard (AES) is most commonly referenced, and this standard is defined by NIST in its publication FIPS-197.

In addition to the AES encryption standard, NIST publishes nine recommended modes of encryption for use with AES. At the time this paper was written, these included:

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Counter (CTR)
- Output Feed Back (OFB)
- Cipher Feed Back (CFB)
- Cipher-based Message Authentication Mode (CMAC)
- Counter with Cipher Block Chaining-Message Authentication Code (CCM)
- Galois Counter Mode (GCM)
- XEX Tweakable Block Cipher with Ciphertext Stealing (XTS-AES)

Modes of encryption are recommended by NIST after they have been extensively reviewed by the professional cryptographic community. This is an international group of cryptographers whose long experience and analytic work are important to the vetting of proposed modes of encryption. In some cases it takes years of work before a mode is approved by NIST; many mode submissions are never approved for use.

IMPORTANT: The CUSP mode of encryption is not included in the NIST list of recommended modes, and has not been submitted to NIST for consideration. It is therefore not a part of the NIST standards, or of any other generally accepted body of standards, and has not been formally reviewed by the cryptographic community. Therefore, the use of CUSP mode would be outside the scope of most data security regulations.

Encryption Certification

In an effort to help organizations get encryption right the first time, the NIST provides a testing and certification protocol for all of the recommended modes of encryption. The tests are administered by NIST-chartered testing laboratories through the National Voluntary Accredited Laboratories Program (NVLAP). These laboratories are empowered to do preliminary testing of encryption solutions, with final approval reserved for the NIST itself.

Any provider of encryption technologies may submit their work for certification to the NIST standards. Purchasers of encryption software can be assured that any solution certified by NIST has been independently reviewed, and has passed stringent tests on its conformance to the standard. Upon completion of these tests, the solution is awarded a certificate of validation. Only those solutions that meet published NIST standards can be certified. Certificates are publicly available on the NIST web site.

IMPORTANT: There is no NIST certification protocol for the CUSP mode of encryption. It is not possible to claim that an encryption product using CUSP has been certified by NIST, or that it is in anyway compliant with the NIST standard.

Implications for Compliance

Because the CUSP mode of encryption is not defined by any standards body, it is impossible to tell if it even could

meet the minimum requirements of any data protection regulation. This is most clear in the HIPAA and HITECH guidance which indicate that only encryption methods approved by NIST provide a "safe harbor" from breach notification requirements. CUSP mode may also run afoul of the requirements of PCI DSS, GLBA, and many state privacy notification laws which make reference to NIST standards.

IMPORTANT: Customers contemplating the CUSP mode of encryption should be aware that their data protection mechanism could fail to provide "safe harbor" from breach notification requirements, and may not limit their legal liability in the event of a data loss.

Intellectual Property Implications

One advantage of using NIST certified encryption methods is that they are free of patent and other intellectual property rights claims. By definition, no method or mode of encryption adopted by NIST can be encumbered by intellectual property claims. The CUSP mode of encryption was developed by IBM and has not been approved by NIST or even proposed for review. Standards bodies will not adopt patented, copyrighted, or proprietary protocols as standards because the intellectual property issues impede the testing process. The cryptographic community learned painful lessons from the 1980's and 1990's when one company held patents on certain encryption methods.

IMPORTANT: It is doubtful that encryption providers that service platforms other than IBM i and z would ever implement or support the CUSP mode of encryption due to it's proprietary nature.

Security Implications

Internationally security standards bodies are careful to properly vet any proposed standard before it is formally adopted. This is especially true of NIST. Any new technology undergoes an extensive period of review by professional cryptographers. Many promising standards are proposed, yet never adopted by NIST. This may be because of security concerns, or due to other factors such as performance or suitability for a specific purpose. In any case, a cryptographic standard that has been adopted by NIST has undergone an exhaustive security review. This rigorous process leads to better standards, better solutions based on these standards, and more secure data.

And when you consider the number of encryption solutions that attempt to meet the NIST standards, it is interesting to note the high rate of failure in the NIST certification candidates. In one study by NIST, the failure rate of vendor solutions was more than one third (37 percent)! This underscores the fact that encryption is difficult to achieve, and many who try just can't achieve.

IMPORTANT: The failure rate of non-standard encryption methods is probably much higher, because many do not even pass the independent laboratory tests that are run prior to the NIST testing. Because non-standard modes of encryption are so rarely used, their creators are less likely to know if there is a problem that has caused a data loss or breach. The CUSP mode of encryption fits this pattern to a 'T'. Its overall security is unknown and untested, and if it has been compromised, there is no standards body to report the vulnerability to.

Compatibility Implications

Software vendors generally adhere to the published standards for encryption. If an encryption solution has been implemented correctly, it will inter-operate with any other solution that has implemented to the standard. (Of course, the way to know if a solution has been implemented correctly is through the NIST certification process). When you encrypt data with a standard method, you or your business partners should be able to decrypt that data using any other software that has implemented the same method. This capability is important to your overall security practice because you do not want to have to decrypt data in order to transfer it to an outside entity, or to another application within your own company. NIST standard encryption solutions will, by definition, inter-operate with other certified applications regardless of the vendor.

IMPORTANT: The CUSP mode of encryption is not a standard, and has rarely been implemented in any operating system, computer language, or hardware module. This mode of encryption is guaranteed to be incompatible with the vast majority of software solutions and OS vendors. As data protection regulations continue their evolution towards "end-to-end encryption" requirements, the non-standard CUSP mode of encryption will not be compliant.

Recommendations

The following common sense recommendations can help you avoid the problems of being isolated with a proprietary and/or non-standard encryption method:

- Don't implement any encryption or encryption key management solution that is not based on standards

such as those published by the well recognized international standards bodies such as NIST, ANSI, X9, or ISO.
- Insist on NIST certification for any solution that you deploy. This will go a long way to insuring that you are using appropriate encryption techniques, that you are in alignment (and will stay in alignment) with compliance regulations, and that you are using a well-implemented technology.
- Require that your software vendor disclose any potential license, patent, or intellectual property claims that may exist for their encryption solution. Know who wrote your encryption solution and who ported it to your platform. Learn the pedigree of that solution in order to avoid becoming entangled in intellectual property lawsuits.
- Review any existing implementation you may have created that uses non-standard methods such as the CUSP mode of encryption. Inquire into the methods for standardizing and certifying the solution that you are evaluating to ensure it will not leave you on a technological island.
- Verify any claim or NIST certification here and here.

Townsend Security

Despite an orgnization's best efforts, their data will get out. That's reality. The best way to secure critical information is with strong encryption and key management.

Townsend Security provides NIST-certified encryption and logging solutions for the Enterprise. Our encryption, key management, tokenization, and logging solutions protect sensitive data from loss, theft and abuse whether it rests within, or is transmitted outside, of your organization.

Our certified database encryption and key management solutions are guaranteed to meet the encryption and key management meet or exceeds the standards in PCI, HIPAA, HITECH and more. Organizations worldwide rely on PTSS for their data privacy needs.

Web: www.townsendsecurity.com
Phone: (800) 357-1019 or (360) 359-4400
International: +1 360 359 4400
Email: Info@townsendsecurity.com

References

IBM, "z/OS Cryptographic Services, Integrated Cryptographic Service Facility, Application Programmers Guide", 1997, 2008.

IBM, "IBM System i Security: Protecting i5/OS Data with Encryption", B. Hagemeister, et al, July 2008.

National Institute of Standards and Technology, Department of Commerce "Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation", Morris Dworkin, 2001.

National Institute of Standards and Technology, Department of Commerce "Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", Morris Dworkin, May 2005.

National Institute of Standards and Technology, Department of Commerce "Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", Morris Dworkin, May 2004.

National Institute of Standards and Technology, Department of Commerce "Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: The Galois/Counter Mode (GCM) and GMAC", Morris Dworkin, November 2007.

National Institute of Standards and Technology, Department of Commerce "Special Publication 800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices", Morris Dworkin, January 2010.

Appendix

Data Security Standard (PCI DSS)

PCI Payment Application Data Security Standard (PA DSS)

HIPAA and the HITECH Act of 2009 and subsequent Department of Health and Human Services guidance (45 CFR 170, NPRM, IFR, and related)

State privacy regulations (45 states), and proposed federal legislation (see US House Bill 2221 "Data Accountability and Trust Act", and US Senate Bills 1490 and 139).

Notes

Note 1: Nothing in this paper should be construed as legal advice and you should not interpret it in that way. Consult with a qualified attorney if you have legal questions about intellectual property constraints. Consult with a qualified QSA auditor if you have questions about PCI DSS compliance.

technical, compliance, and end-user staff working together.