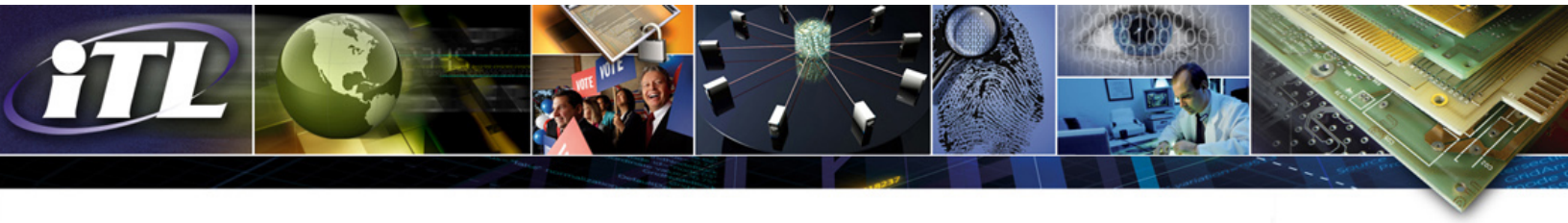


ITL BULLETIN FOR AUGUST 2015

RECOMMENDATION FOR RANDOM NUMBER GENERATION USING DETERMINISTIC RANDOM BIT GENERATORS

Elaine Barker, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

Cryptography and security applications make extensive use of random numbers and random bits. NIST has been making recommendations for random number generation for many years. However, in response to public concerns about the security of one of the generators specified in an earlier recommendation, NIST has formally revised its recommended methods for generating random numbers, releasing Special Publication 800-90A Revision 1, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*.

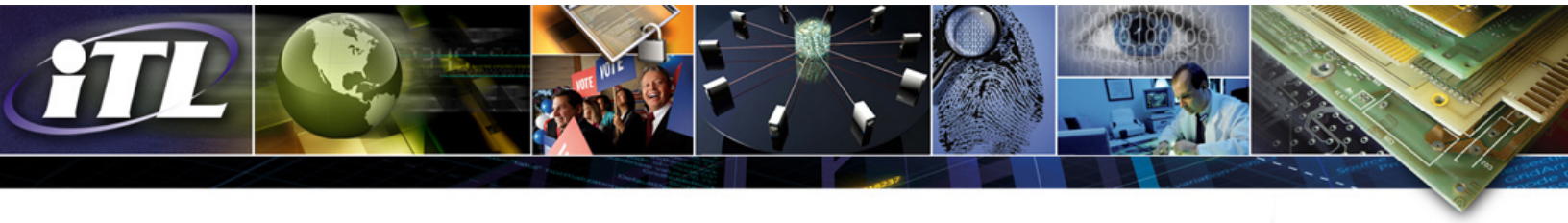
One of the most significant changes to previous recommendations is the removal of the Dual_EC_DRBG algorithm, often referred to conversationally as the "Dual Elliptic Curve random number generator." This algorithm has spawned controversy because of concerns that it might contain a weakness that attackers could exploit to predict the outcome of random number generation.

SP 800-90A Rev. 1 continues to include three other algorithms based on hash functions and block ciphers that were present in the previous versions of the document and are still considered to be secure.

The revised version also contains several other notable changes. One concerns the CTR_DRBG—one of the three remaining random number algorithms—and allows additional options for its use. Another change recommends reintroducing randomness into deterministic algorithms as often as it is practical, because refreshing them provides additional protection against attack. The document also includes a link to examples that can help developers to implement the SP 800-90A random number generators correctly.

Background

Federal Information Processing Standard (FIPS) 186-2, *Digital Signature Standard* (2000), specified the first NIST-approved methods for random number generation. However, with the advent of stronger computers and more reliance on cryptography, newer techniques are needed for the generation of random bits. NIST responded to this need with the development of NIST SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, which was first published



in 2006, and later revised as SP 800-90A in 2012. This publication described algorithms that could be used to reliably generate random numbers, a crucial step in using cryptography.

As specified in SP 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, random number generator mechanisms from FIPS 186-2 will no longer be approved after December 31, 2015, and only those from SP 800-90A can be used for U.S. government purposes after that date.

Recommended Techniques

SP 800-90A specifies techniques for the generation of random bits that may then be used directly or converted to random numbers when random values are required by applications using cryptography.

SP 800-90A describes random bit generation that is based on a deterministic strategy. According to this strategy for generating random bits, it is necessary to compute bits deterministically using an algorithm; this class of random bit generators (RBGs) is known as Deterministic Random Bit Generators (DRBGs). A DRBG is based on a DRBG mechanism as specified in SP 800-90A and includes a source of randomness. A DRBG mechanism uses an algorithm (i.e., a DRBG algorithm) that produces a sequence of bits from an initial value that is determined by a seed obtained from the output of a randomness source. Once the seed is provided, and the initial value is determined, the DRBG is said to be instantiated and may be used to produce output. Because of the deterministic nature of the process, a DRBG is said to produce pseudorandom bits, rather than random bits. The seed used to instantiate the DRBG must contain sufficient entropy to provide an assurance of randomness and support a desired security strength. If the seed is kept secret, and the algorithm is well designed, the bits output by the DRBG will be unpredictable, up to the instantiated security strength of the DRBG.

DRBG Specifications

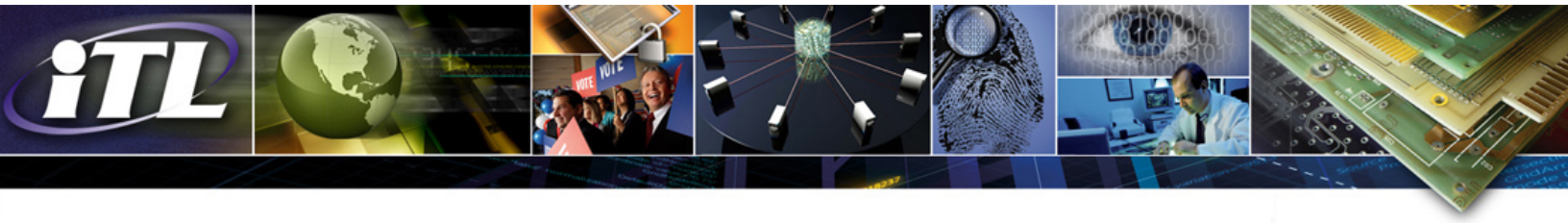
SP 800-90A specifies several DRBG mechanisms. The selection of a DRBG mechanism depends on several factors, including the security strength to be supported and what cryptographic primitives are available (e.g., a cryptographic hash function or the Advanced Encryption Standard, AES). An analysis of the consuming application's requirements for random numbers should be conducted in order to select an appropriate DRBG mechanism.

In addition to specifying the DRBG mechanisms, this Recommendation provides:

- Assurance and conformance-testing requirements (see below);
- Pseudocode examples for each DRBG mechanism; and
- A detailed discussion on DRBG mechanism selection.

Assurance

A user of a DRBG employed for cryptographic purposes requires assurance that the generator actually produces (pseudo) random and unpredictable bits. The user needs assurance that the design of the



generator, its implementation and its use to support cryptographic services are adequate to protect the user's information. In addition, the user requires assurance that the generator continues to operate correctly.

The design of each DRBG mechanism in SP 800-90A has received an evaluation of its security properties prior to its selection for inclusion in this Recommendation.

Conformance Testing

Conformance testing for implementations of SP 800-90A Rev. 1 will be conducted within the framework of the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP). The requirements of this Recommendation are indicated by the word “shall.” Some of these requirements may be out-of-scope for CMVP or CAVP validation testing, and thus are the responsibility of entities using, implementing, installing, or configuring applications that incorporate this Recommendation.

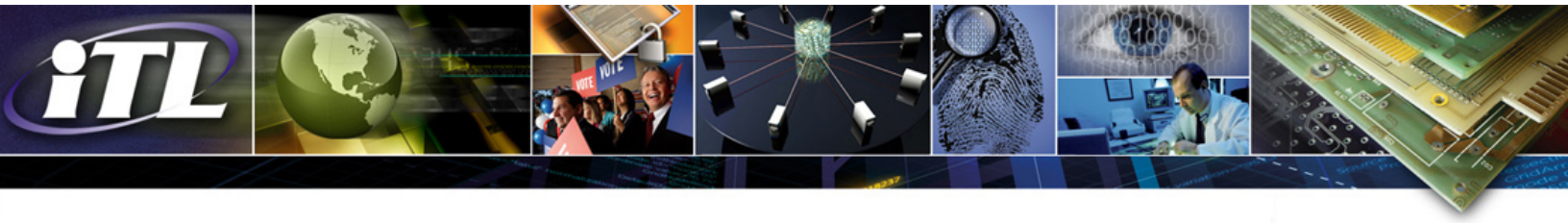
SP 800-90A Rev. 1 clearly differentiates testable requirements from policy recommendations that cannot be verified during laboratory testing. In addition, the optional security requirements for DRBG implementations are identified. Changes from the previous version of SP 800-90A do not affect the work of the CAVP, since this program stopped testing Dual_EC_DRBG implementations in 2014. However, the latest improvements of this publication affect how the CMVP works with it. Some of the new mandatory security requirements related to the known-answer-tests for the DRBG primitives cannot be tested by the CAVP. The CMVP sent specific guidance to all accredited Cryptographic and Security Testing (CST) laboratories about how to conduct and report the testing of the new mandatory security requirements in SP 800-90A Rev. 1.

Conclusion

NIST Special Publication 800-90A Rev. 1 helps product developers and vendors to select appropriate techniques for the security they want to achieve. NIST makes recommendations, and it is up to the implementer to select what is appropriate.

This Recommendation specifies several DRBG mechanisms, all of which provided acceptable security when the Recommendation was published. However, in the event that new attacks are found on a particular class of DRBG mechanisms, a diversity of approved mechanisms will allow a timely transition to a different class of DRBG mechanism.

This Recommendation comes at a good time for the CMVP in view of the upcoming RBG transition at the end of 2015. Old random number generators (RNGs) from FIPS 186-2 will no longer be approved after December 31, 2015, and only the DRBGs from SP 800-90A Rev. 1 can be used to generate cryptographic keys and nonces for U.S. government use. The additional programmatic enhancements to the CMVP to support this new version of SP 800-90A allow NIST to continue to provide valuable service to improve



the security and technical quality of cryptographic modules employed by federal agencies in the United States and Canada.

Related Work

SP 800-90A is the first of a series of publications on random bit generation. SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation*, will discuss the development and validation of the entropy sources that are ultimately required for random bit generation. SP 800-90C, *Recommendation for Random Bit Generator (RBG) Constructions*, will provide approved constructions for random bit generators using the DRBG mechanisms in SP 800-90A and the entropy sources in SP 800-90B. Drafts SP 800-90B and SP 800-90C are currently available at this website. Updated drafts of these documents are expected to be available for public comment in late 2015.

Additional Resources

NIST SP 800-90A Rev. 1, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, June 2015

NIST SP 800-90B (Draft), *Recommendation for the Entropy Sources Used for Random Bit Generation*, September 2013

NIST SP 800-90C (Draft), *Recommendation for Random Bit Generator (RBG) Constructions*, September 2013

NIST SP 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov