

Heartland E3 System & Identity-Based Encryption

October 8, 2009

Evaluation Summary and Report

Independent Security Evaluators
www.securityevaluators.com

End-to-End Encryption and Identity-Based Encryption

The E3 System is intended to cryptographically protect payment card information at all points in a payment network, from the initial card swipe to long-term storage. To accomplish this goal, the E3 System incorporates a tamper-resistant encryption module into each E3 point-of-sale (POS) terminal. Payment card information data is encrypted at the initial swipe, and remains protected at all times in transit and storage. In fully implemented systems, cleartext card data is never exposed, except within a small number of dedicated Hardware Security Modules (HSMs) in the terminal and network.

Key distribution is one of the greatest challenges in deploying secure payment networks. In an end-to-end system, cryptographic protection is "carried with" the data. Therefore transaction information can be rearranged or moved between databases without risk of breach.

A side effect of this approach is the ability to encrypt data with many distinct keys; this reduces the possibility that a single-point compromise will lead to a system-wide breach. In the E3 System each transaction batch is encrypted with a distinct key, which can be updated every day. Key management on this scale is made possible using Identity-Based Encryption (IBE), an advanced form of public key encryption.

Key Distribution, Management and Revocation

The E3 System does not expect E3 POS terminals to store sensitive long-term secret keys. IBE permits the terminal to encrypt data using a set of non-secret "public" parameters. Critically, this encryption is one-way: knowledge of these parameters does not permit an attacker to decrypt ciphertexts.

Unlike traditional public-key encryption schemes, however, IBE allows for simplified key updates and distribution of decryption effort. In an IBE system, encryptors use identities in place of public keys. An identity is an arbitrary string, e.g., the name of a recipient or destination system. The corresponding decryption keys can be derived by a central party known as a Private Key Generator (PKG).

The Boneh-Boyen IBE System

The E3 System uses an IBE scheme developed by Dan Boneh and Xavier Boyen [2]. The Boneh-Boyen scheme is in the elliptic curve setting, and uses subgroups with an efficiently computable bilinear map. The technique and the underlying mathematics have been well studied in the cryptographic literature [2, 5]. More important, the Boneh-Boyen scheme is provably secure under a mathematical assumption known as the Decisional Bilinear Diffie-Hellman assumption [7].¹

Key management on this scale is made possible using Identity-Based Encryption (IBE), an advanced form of public key encryption.

Full details of the Boneh-Boyen implementation (BB1) can be found in RFC 5091 [3], authored by Voltage Security, Inc. The implementation achieves full collusion resistance via the technique described in [2, §7] (Theorem 7.2). Additionally, it employs techniques of Fujisaki and Okamoto to achieve full security against chosen-ciphertext attack (CCA2) [4, 14].

All elliptic curve operations are implemented in a 512-bit supersingular curve with a 160-bit prime, which is distributed as part of the master parameters for the IBE system. Using the techniques of [9] we can estimate the security of the BB1 system deployed within this curve as roughly equivalent to that of RSA encryption at a 1,024-bit key size.²

¹Although a full proof is not specified by Voltage, Inc., the specific implementation used by the E3 System employs the useful when enciphering long, high-entropy plaintexts such as the full Track 1/Track 2 datablock.

Fujisaki-Okamoto transform in the Random Oracle Model to reduce the strength of this assumption to a computational problem, the Bilinear Diffie-Hellman Problem. This assumption is strictly weaker than its decisional variant.

²This comparison is based on the running time of the best known attacks in the EC setting (EC-DLP/MOV) and RSA (factoring), see [9].

To learn more about E3 technology, visit
E3secure.com.

Bibliography

- [2] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In Christian Cachin and Jan Camenisch, editors, EUROCRYPT '04, volume 3027 of LNCS, pages 382–400. Springer, 2004.
- [3] X. Boyen and L. Martin. Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems.
- [4] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Advances in Cryptology -CRYPTO '99, volume 1666 of Lecture Notes in Computer Science, pages 537–554, 1999.
- [5] Steven D. Galbraith, Kenneth G. Paterson, and Nigel P. Smart. Pairings for cryptographers, 2006. Cryptology ePrint Archive: Report 2006/165.
- [7] Antoine Joux. A one round protocol for tripartite diffie-hellman. In ANTS-IV: Proceedings of the 4th International Symposium on Algorithmic Number Theory, pages 385–394, London, UK, 2000. Springer-Verlag.
- [9] Dan Page, Nigel Smart, and Fre Vercauteren. A comparison of MNT curves and supersingular curves. *Applicable Algebra in Eng, Com and Comp*, 17(5):379–392, 2006.
- [14] Peng Yang, Takashi Kitagawa, Goichiro Hanaoka, Rui Zhang, Kanta Matsuura, and Hideki Imai. Applying Fujisaki-Okamoto to Identity-Based Encryption. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, 16th International Symposium, pages 183–192, 2006.