



Impact Report

Voltage rolls with format-preserving encryption, expands IBE Business

Analyst: [Nick Selby](#)

Sector: [Enterprise Software](#) »»

Date: 12 May 2008

At this year's **RSA** convention, the most commonly heard gripe from the security boffins in attendance was that there was nothing new going on. We beg to differ – we saw a couple of very cool incremental improvements to extant products. One was **Voltage Security's** Format-Preserving Encryption, or FPE. Crypto experts were saying that this was no big deal – and we certainly don't claim the crypto chops to debate that. Even Voltage says that its FPE is based on several previous works dating back to the 1980s (see 'Technology' below).

But management of a system that enables a very large organization to convert, for example, credit card numbers to a 16-digit numeric ciphertext that is as hard to reverse as a 128-digit string encrypted by AES-128? That ain't nothing. In fact, that's really, really cool.

The 451 Take

The need for such a system is obvious: with the Payment Card Industry Data Security Standards (PCI-DSS) mandating that credit card numbers held by merchants be encrypted using specific encryption strength, those with extremely large systems of legacy kit-like mainframes are in a bind. Either they upgrade their ancient mainframes (which can't cope with anything bigger than a 16-digit string or nonnumeric characters in a credit card field) at an astronomical cost in dollars, time and training, or find a – yes – new approach. Voltage FPE, according to the rep of a very large organization we spoke with, works like a charm. We're convinced it's on to something bigger, possibly, than the identity-based encryption that's gotten it this far. That the crypto itself is not totally new is beside the point. Innovative incremental enhancement of an existing technology is innovation, and managing gazillions of keys so legacy systems think they're still dealing with credit card numbers when in fact they're dealing with garbage is not just new, it's extremely cool.

Context

Voltage claims 475 customers in a range of verticals. Publicly mentionable customers include **XL Capital**, **US Airways**, **Eastman Kodak** and **ING** (though none of those are the large customer we spoke with about the FPE deployment). Sales are 70% direct, and it claims an average deal size of \$150,000. Deals range from \$60,000 to \$5m. Voltage says it's cash-flow positive from operations, but not US GAAP profitable.

Headcount is at 75, with about 40% of those in development, and the company says it is hiring in both engineering and sales. Investors include **Trident Capital**, **JAFCO Ventures**, **Hummer Winblad Venture Partners**, **Morgenthaler Ventures**, **Menlo Ventures** and **Cipio Partners**. Investment to date totals \$42.6m. Voltage last raised funding in November 2007, and says it is not currently seeking another round.

Products

Voltage's identity-based encryption products use a recipient's email address as a key, and work in a fairly straightforward manner: upon sending an encrypted message to an unregistered recipient, Voltage sends the recipient an email with a link to follow to an SSL-encrypted registration page, where the user chooses a password. A second email from Voltage to the user confirms and contains another link to the Voltage site, where the user logs in and is shown the message. Once logged in, the user may reply to the encrypted email, forward it to other users, etc. It's been licensed by a number of customers like **Microsoft, Code Green Networks, Sendmail, Proofpoint, Secure Computing** and others, including some very large organizations.

Voltage SecureData, the newest product incorporating FPE, has at least one very large deployment. It is outside North America, and we have twice spoken at some length with two architects at the customer, which is a 'large, mid-six-figure deal' at a government-owned national retail concern.

Technology

While we maintain that management of this system is no small feat, Voltage and cryptography boffins clearly state this is nothing 'new.' Voltage itself says: 'The algorithms proposed ... have security proofs in the cryptographic literature ... based on constructions that go back at least to 1986.' Voltage cites a paper by M. Luby and C Rackoff, 'How to Construct Pseudorandom Permutations and Pseudorandom Functions,' as a key starting point.

In 1997, Harry Smith and Michael Brightwell posited in their paper ('Using Datatype-Preserving Encryption to Enhance Data Warehouse Security,' presented at the 20th National Information Systems Security Conference in Baltimore, Maryland) not just that database fields built to hold an eleven-digit (including hyphens) Social Security number (SSN) could not even hold a DES-encrypted version of the SSN – but also that programs would be incapable of processing the encrypted version as a SSN because the DES-encrypted version of a SSN probably won't even contain a single digit. The paper is a fun read.

In 2000, researchers John Black of the University of Nevada, Reno, and Phillip Rogaway of the University of California at Davis, California, wrote a paper called 'Ciphers with Arbitrary Finite Domains' that set forth methods for strong encryption of finite-length strings, based on Rogaway's earlier work.

Voltage itself publishes a white paper on the subject that shows how it produces the encryption specifically to deal with personally identifiable information such as SSNs and credit card numbers. For SSNs, one problem encountered was that often a call-center agent or other untrusted person would need to ask a caller for the last four digits of their SSN as part of a verification process. According to Voltage, a prefix cipher scrambles five-digit decimal values using a key (K) and what Voltage calls its arbitrary tweak value (T). A Feistel-style cipher encrypts the nine-digit decimal value using K; H(P) is a hash function converting four-digit decimal values to an arbitrary bit string. Then two keys are created, the first scrambling the first five digits of the SSN, the second (K2) scrambling the last four digits. In this way, the call center agent can be given just K2, which will reveal the last four digits for confirmation purposes, while systems with access to K1 and K2 can get the whole number. The credit card method is similar, with more moving parts.

Competition

Column-level database encryption comes from vendors like **Vormetric, Protegrity** and **Ingrian Networks**. The database vendors themselves – **Oracle, MySQL AB**, Microsoft, et al. – offer fairly broad encryption. But really, for this kind of thing, many organizations are looking to point products to encrypt on the devices that store the data – no matter for how long or short a time – from the likes of **BitArmor Systems, Check Point Software Technologies (Pointsec), Credant Technologies, GuardianEdge Technologies, McAfee (SafeBoot), PGP Corp, Utimaco Safeware, WinMagic** and others. Or they're looking to firms that provide storage media encryption, along the lines of **EMC/RSA, IBM, Hewlett-Packard, NetApp** and

others. HP, **Thales e-Security**, **SafeNet**, **nCipher**, **CipherOptics** and others do point-to-point encryption or hardware security modules of the kind used to protect ATM networks. Others must be looking at FPE, but we're not seeing them.

Voltage has been seeing good traction with its email encryption, especially with its OEM business. **Trend Micro** picked up **Identum** – the other player that used the recipient's email address as a public key for email encryption. Other email competition comes from **Tumbleweed Communications**, **Cisco Systems/IronPort Systems (PostX)**, **Zix Corp**, PGP and **Entrust**. Voltage is quick to note that these vendors sell PKI-based systems, while it sells its proprietary identity-based encryption.

Voltage's partnerships in anti-data-leakage (ADL) – Code Green and EMC/RSA (**Tablus**) – raise indirect competition from the dozens of vendors in that space. Also, how Voltage will be affected by IBM's announcement of a deal that includes ADL vendors **Fidelis Security Systems** and **Verdasys** along with PGP remains to be seen. Other PKI vendors include RSA, **VeriSign** and **Certicom**. Competition from point-to-point encryption vendors comes from **BeCrypt**, **AppGate Network Security** and **KoolSpan**, as well as from SSL VPN vendors.

SWOT analysis

| Strengths | Weaknesses |
|---|---|
| Voltage has good name recognition, serious people and some powerful partners. It also is using an innovative twist to repurpose some established technology to address a very common issue – compliance with PCI-DSS. | Even if commercial competition is light now, cultural competition – that is, winning over multiple departments in organizations large enough to have such old and heterogeneous architectures – sounds like a long and complex sales cycle. |
| Opportunities | Threats |
| The largest of firms share the problem of huge legacy systems that can't suck and blow anything except exactly what they expect: 9-, 11- or 16-character strings. PCI-DSS offers opportunities galore. | If the encryption part really is no big deal, then others with good encryption and key management chops – nCipher, SafeNet, HP, IBM – might find this a lucrative path. |

Related analysis

451 Market Insight Service

[Claiming positive cash flow and customer growth, Voltage tacks on \\$12m in funding](#)

With new funding, the identity-based encryption vendor says it's hit two consecutive quarters of cash-flow-positive operations. We expect more growth and new products in the coming months. (6 Nov 2007)

[Voltage announces SecureMail V3, adds anti-phishing and central management](#)

MIS Analyst Note, 02/05/07

[Voltage Security takes its identity-based encryption to the PKI mainstream](#)

MIS Impact Report, 04/20/06

The company claims it has an asymmetric encryption algorithm with a management system, which it says will give public key infrastructure a run for its money and greatly simplify key management and disaster recovery.