



Image: Kamalova

heightened security

By Peter Haapaniemi

A few years ago, two men, whose sons played youth hockey together in Troy, MI, struck up a friendship during games and practices. In time, their conversations ranged far beyond goals, penalties and ice time and ended up on the somewhat esoteric topic of data encryption.

Their conversations eventually led to the founding in May 2006 of Pure Entropy Technologies, a Troy-based startup that is working to take the practice of data encryption to new levels. Pure Entropy focuses on a fundamental component of the security landscape — information. In the fight against terrorism, information is power — and officials have a vital interest in keeping data and communications safe. And it's not just a government challenge. Businesses often find criminals working to steal customer information that can be used in identity theft and other forms of fraud.

Introducing JUMBLE™ technology

In the fight against terrorism, information is power.

Pure Entropy's business is built around a proprietary encryption technology called JUMBLE, which provides extremely high levels of security. Where a typical security method for business might use an "encryption key" with a length of 128 bits, JUMBLE uses a 2,048-bit key. "We think it's able to satisfy the most extreme security needs," says Tom DeAgostino, Pure Entropy co-founder and general counsel.

The JUMBLE technology stands out for more than tight security. It operates differently than traditional encryption technologies, which results in a very low demand on computing power and network bandwidth. In other words, it can be used on virtually any electronic device with almost no effect on speed, performance or bandwidth and a very light load on battery power.

"It is also 'data agnostic,' meaning it can encrypt any form of digital data, including text, audio and real-time streaming video," says DeAgostino. As a result, the technology can be used anywhere in an IT infrastructure and in a variety of devices, including laptop computers, PDAs and cell and satellite phones. That's key for military communications, where the security of messages can mean the difference between success and failure — and life and death.

The JUMBLE technology's unique traits make it especially interesting for use in the growing range of video applications found in military and security operations. Today, officials have equipped everything from fighter jets to unmanned observation aircraft and bomb-defusing robots with video cameras. These devices feed signals back from dangerous areas to decision makers who are out of harm's way. Naturally, the ability to secure these transmissions without impairing the performance of the device or the network will be increasingly important.

"You can have a soldier in the field sending real-time streaming video back to central command, fully encrypted. They can capture the battle and other information for strategic and tactical purposes," says DeAgostino. Overall, he adds, "We see a huge market in video streaming and our JUMBLE technology is a singularly unique security solution. Pure Entropy is the only known company that can provide streaming high-definition, real-time video encryption without any significant impact on bandwidth."

A two-pronged approach

After launching Pure Entropy, DeAgostino and his team spent time lining up funding, and the company marked the successful completion of its first round of financing in August 2007. But the Pure Entropy team was also out educating the marketplace, talking to various government officials. The JUMBLE technology passed a number of government security tests, but the company found that government decision-making and procurement cycles moved fairly slowly.

"Initially, we started at the top, meeting with high-ranking officials at the Pentagon, figuring we could push this down," says DeAgostino. "But we came to the conclusion that that's not the way to work."

As a result, Pure Entropy adjusted its strategy in two ways. First, to make headway in the government and defense business, the company decided to work through partnerships and collaborate with other companies that already had relationships with public-sector agencies. DeAgostino prefers not to mention the partners by name, due to the intense security concerns in the industry. But, he says, "We are developing strategic alliances to integrate our product into other companies' existing product lines." That approach allows Pure Entropy to leverage its partners' existing government business, and also opens the door to creating an ecosystem of partners who can adapt the JUMBLE technology to a variety of new uses.

The second leg of the strategy has been the launch of a sister company — called Encryption Security Solutions — that focuses on bringing the JUMBLE technology to commercial markets. The need, certainly, is clear. Many companies have been victims of significant data breaches in recent years. A typical breach costs a company \$197 per record, according to research from the

Ponemon Institute, a privacy and information management firm. That adds up quickly when loss events involve tens of thousands — or even millions — of records.

The "last bastion"

**"Encryption is like having a safe inside with two Doberman pinschers guarding it."
— Tom DeAgostino**

Encryption Security Solutions is creating offerings that are based on a modified version of the JUMBLE technology. That high level of encryption can be used by companies to employ a more "layered" approach to securing their data — one that goes beyond simply controlling access at the perimeter of their systems with firewalls. "I tell people to think of the front door and lock on your home as a firewall. Somebody is going to get past that door if they really want to," says DeAgostino. "Encryption is like having a safe inside with two Doberman pinschers guarding it.

"Encryption is the last bastion of protection for your data," says DeAgostino. "People will get through a firewall; and when they do, if the data itself is not protected, it's open. If it's fully encrypted, all they will get is garbled data."

Encryption:

The conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized users.

Between January 2005 and November 2007, some 215 million files of confidential information were stolen or lost from organizations in the U.S., according to the Privacy Rights Clearinghouse. "Since most of the data was lost from universities and governmental agencies, it was assumed those organizations had multiple firewalls," DeAgostino says. What's more, many data losses have been due not to hackers, but rather to lost or stolen laptops — which would not have been much of an issue if the data on them had been encrypted.

Encryption Security Solutions recently rolled out its first formal product, encryptoMail®, which can be used to encrypt e-mail. Other offerings in the pipeline include products that provide security for computer hard drives, Internet phone calls, video conferences, databases and remote access to corporate intranets.

Like Pure Entropy, Encryption Security Solutions is also taking advantage of partnerships to make JUMBLE technology available to other firms for use in their products. Target users, says DeAgostino, are companies that provide mobile telecommunications services. "If you're sending e-mail through your PDA, you want it to be encrypted because of the high risk of data loss through cell phone towers."

The Pure Entropy/Encryption Security Solutions team plans to introduce the JUMBLE technology into more and more products and applications — in both the private and public sectors — in the near future. Growth and revenue are, of course, part of this game plan, but so is something broader. DeAgostino says their technology is a "game changer" for security — one

that "saves data and information — but maybe more importantly, it can also save lives. Our plan is for JUMBLE to become the new standard for encryption."

For more information visit www.pureentropy.com.

Risky Business

Companies today house a great deal of electronic information about customers and, increasingly, that information is under attack by hackers and criminals.

In the past few years, organizations ranging from retailers and banks to government agencies and universities have suffered data breaches in which confidential information has been lost or stolen. Some events have made headlines, such as retail parent company TJX's reported loss of as many as 100 million records and the United Kingdom government's loss of information on 25 million residents. Numerous other breaches involving hundreds or thousands of records don't make the news, but are, nevertheless, damaging to companies and consumers. (For a list of breaches, visit www.privacyrights.org.)

Such breaches result from electronic intrusions, disgruntled employees and, especially, the fairly low-tech problem of lost and stolen laptops, USB drives and other devices. Indeed, according to the Ponemon Institute, an information and privacy management organization, 70 percent of data breaches result from the loss of such off-network equipment. That's one reason why many experts recommend the use of encryption, which renders the data useless to non-authorized people.

The cost of data breaches can be substantial because they can lead to everything from legal and consulting fees to lawsuits. In a study of 35 events, the Ponemon Institute found that the average incident cost \$6.3 million in 2007, up from \$4.8 million in 2006. And the impact can be far-reaching. A big part of the growing cost of data breaches was a 30 percent increase in the cost of lost business, which reflects the loss of customers' trust. As Dr. Larry Ponemon, chairman of the institute, points out: "Consumers seem to be less forgiving when their personal information is compromised."