Ovum
TMT intelligence | informa

On the Radar: Whitewood provides quantum-guaranteed entropy for random number generation

It offers on-premises entropy servers for a fee or entropy-as-a-service free from the cloud

Publication Date: 03 Jul 2017 | Product code: IT0022-001021

Rik Turner

Summary

Catalyst

Whitewood develops technology that applies quantum mechanics to the problem of generating perfect (i.e. unguessable) random numbers for use in encryption and other types of cryptography.

Key messages

- Whitewood offers its Entropy Engine to generate random numbers.
- Its netRandom software injects seed material into operating systems (OSs), virtual machines (VMs), and Internet of Things (IoT) devices.
- Whitewood also has a free entropy-as-a-service offering.
- It sees opportunities for service providers to offer their own entropy services for security-minded business customers.

Ovum view

Cybersecurity is a continual arms race between attackers and defenders, and the world of encryption is no exception. Using quantum entropy to help generate true random numbers for encryption keys represents a rare opportunity for defenders to get ahead of the game for existing applications. It will become an essential component of quantum-safe algorithms that are required before quantum computers become a reality.

Recommendations for enterprises

Why put Whitewood netRandom on your radar?

In the future, Whitewood's application of quantum mechanics to guarantee the perfect entropy of encryption keys will enhance companies' defenses against attacks from threat actors armed with increasingly powerful computers and, ultimately, crypto-cracking quantum computers. Customers have the opportunity to start using this technology now, in order to understand how to inject randomness into number generators in the OSs they use in their data centers, in the cloud, or in IoT devices.

Highlights

The rationale behind the creation of Whitewood is that all crypto-based security applications (encryption is the most well-known) rely on truly random numbers to generate keys that are unguessable, as any amount of predictability in keys creates a risk of attack. And yet in virtualized environments and low-power devices such as IoT, it is often hard to find sources of high-quality randomness (entropy). Furthermore, as quantum computing edges closer to becoming an affordable reality over the next decade, it will soon be possible to actually calculate, rather than crack, the keys used to encrypt data. This being the case, only the application of quantum-mechanical phenomena,

expressed in modules based on photonics, will be able to withstand such firepower by generating perfect random numbers.

Whitewood manufactures such modules and sells them as PCI cards for insertion into servers, as well as into appliances for installation in data centers as shared entropy sources. The technology can also be accessed as a cloud service, which Whitewood refers to as "entropy-as-a-service."

Software alone cannot generate true random numbers, but most OSs come with so-called pseudorandom number generators (PRNGs) or deterministic random bit generators (DRBGs), which are algorithms that can generate sequences of numbers whose properties approximate those of random number sequences.

These algorithms are "seeded" with real-world information, however, such as data from movements of the mouse or CPU timing, and as such they are not 100% random or perfectly unpredictable. Linux has two PRNGs built in, and takes in around half a dozen data sources to create the seed, which is a means of building entropy into the algorithm.

The approach runs into trouble when no such randomness is available, for example in a VM environment or an IoT scenario. There are academic studies that suggest that as many as 3% of all "randomly" generated keys are easily guessable or, in fact, the same, demonstrating an evident lack of entropy.

Whitewood's platform sets out to inoculate systems against generating predictable keys. Its two modules are

- a quantum entropy source known as the Entropy Engine, which is a purpose-built hardware component that runs at 350Mbps
- netRandom, which is server software that pulls random data from the Entropy Engine to deliver seed material to software agents within the OS, VMs, or devices (e.g. smart meters), establishing a network service to potentially thousands of endpoints, akin to the Network Time Protocol.

The Whitewood agent in the recipient system monitors the amount of entropy as it goes and requests additional entropy as required from the server, but otherwise requires no changes to existing hardware or software. The technology can run as a cloud service or a private service in a company's own data center.

Background

Whitewood was founded in 2014 and is a subsidiary of Allied Minds, an investment company that is listed on the London Stock Exchange.

The business model of Allied Minds is to bring research work done in academia and the US government sphere into the commercial realm, and Whitewood was created following a technology transfer arranged by the Department of Homeland Security from Los Alamos National Laboratories.

The technology that Los Alamos had been working on and then transferred to Whitewood involved the use of quantum mechanics for generating perfect (i.e. unguessable) random numbers and in key management technologies that are safe from attack by quantum computers.

Current position

Whitewood launched its Entropy Engine hardware and netRandom software products in 2016, and added the entropy-as-a-service offering in April 2017. The service is offered for free, while the on-premises software option, since it gives the customer control and a more granular view of the entropy it is injecting into its systems, is offered for a fee, with the preferred options being a perpetual license or a consumption-based model. In these cases, the size of the subscription is based on the number of systems to which the platform is delivering entropy. That said, Whitewood is also open to a revenue-sharing approach with partners and service providers.

The company targets the financial, healthcare, retail, and public sectors as potential customers, and seeks partnerships to embed its technology in devices such as routers, firewalls, and encryption platforms. It envisages a third route to market in the form of service providers that might want to launch their own entropy services. The company's entropy-as-a-service offering is designed to appeal to companies offering public key infrastructure (PKI) and email-signing technology.

Data sheet

Key facts

Table 1: Data sheet: Whitewood

Product name	netRandom Free (cloud-based entropy service), netRandom Enterprise (on-premises entropy server), Entropy Engine (quantum random number generator)	**Product classification**	Random number generation for cybersecurity
Version number	All products are new, so are v1.x	**Release date**	The quantum random number generator hardware was launched in late 2015, the entropy server in late 2016, and the cloud-based entropy service in April 2017
Industries covered	Typically those that handle regulated data or high-value IP, or are subject to privacy regulation (e.g. banking, retail, healthcare, high-tech, academia, government, and defense)	**Geographies covered**	Primarily developed countries, initially the US and now expanding into Europe and Asia
Relevant company sizes	Midsize to large organizations	**Licensing options**	Perpetual licenses, as well as recurring, consumption-based models in some cases. Revenue-shareing models are also available for partners and service providers
URL	www.whitewoodsecurity.com	**Routes to market**	Primarily direct, but recruiting channel partners and OEMs (security product vendors that embed the technology in their own solutions)
Company headquarters	Boston, Massachusetts, US	**Number of employees**	20

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

Cybersecurity and Encryption: Approaches to Obfuscating Data, IT0022-000263 (December 2014)

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum

TMT intelligence | informa

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo