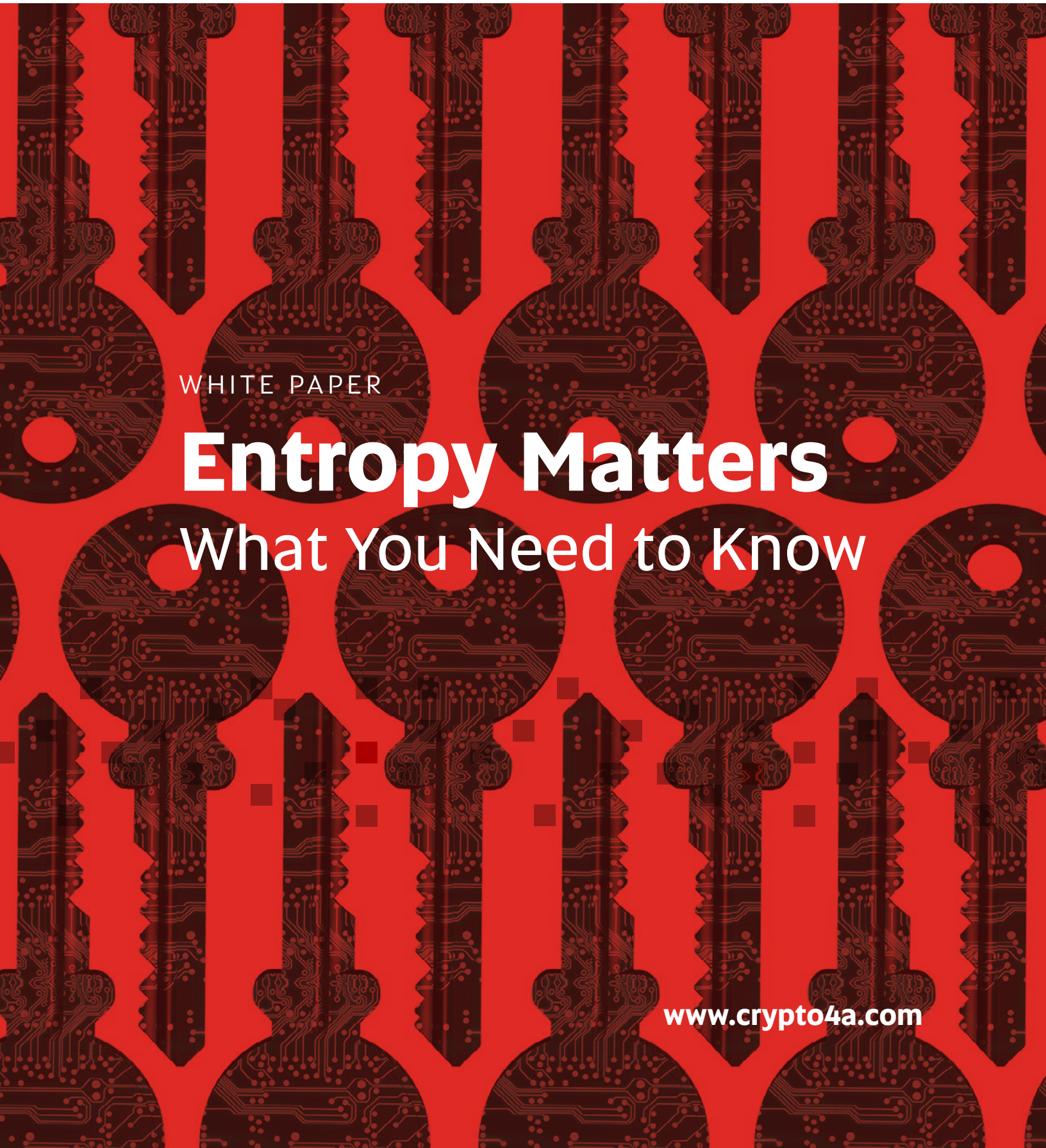
CRYPTO4A



WHITE PAPER

Entropy Matters

What You Need to Know

www.crypto4a.com

WHAT YOU NEED TO KNOW

Internet security is at risk. Quantum technologies, private and state-sponsored hacking, poor software maintenance practices and weak cryptography are on track to cost $2.1 trillion in data breaches globally by 2019.[1] Strong cryptography is required to secure the Internet, but it is less about the choice of algorithm and more about generating unpredictable keys and keeping them secure.

High quality entropy is required to generate the digital keys that provide organizations with the capabilities for secure transactions and storage of sensitive information. It is an important cornerstone of security in an era of complex cloud-computing deployments, machine intelligence which is coming on-line at an accelerating rate and the near advent of quantum computers.

Why Entropy is Important

Entropy can be thought of as a measure of unpredictability. The more unpredictable a system, the more entropy you can extract from it. In a general computing environment, entropy can be gathered from a variety of physical subsystems such as mouse movements, keyboard entries, disc drives or network activities which can be captured by an operating system. This widely unpredictable data can be transformed into random numbers used to generate cryptographic keys for encrypting information. Without strong entropy, there can't be strong cryptography; it's that simple! Traditional sources of entropy are no longer adequate for today's cryptographic needs.

Duplicate Keys are Not Random

In a landmark 2012 study entitled: "Mind your Ps & Qs: Detection of Widespread Weak Keys in Network Devices",[2] researchers became painfully aware that the scarcity of entropy in modern computing environments had reached distressing levels. While analyzing the public key systems securing the Internet at the time, they uncovered that as much as 5% of HTTPS and 10% of SSH public keys they collected were duplicates! To comprehend the magnitude of this result, imagine randomly picking a single atom from our known universe (there are an estimated 10^{82} of them). Now, further imagine that, contained within each atom of our own universe, there exists a further "mini-universe" that itself contains another 10^{82} "mini-atoms". Now, your final task is to randomly select one of these "mini-atoms". In other words, you have to ultimately pick an item out of a potential set of 10^{164} such items. Imagine your surprise if ten out of a hundred people who were asked to perform this same task, picked the same two "mini-atoms". That's how these researchers felt, too!

What is causing this apparent lack of randomness? Fundamentally, the demand for random data in day-to-day computing vastly increased with the rapid adoption of the Internet and the need to utilize security protocols. Early computing systems did a fine job extracting randomness from the entropy generated by human-machine interactions. However, access to these sorts of entropy sources has largely disappeared with the advent of embedded systems, Internet of Things (IoT) devices, and cloud-based computing environments. Hence, software functions such as Linux's /dev/urandom that were able to produce good random data derived from user interactions in the PC-era, fall drastically short when isolated in an embedded environment, on an IoT device, or in a cloud-based computing system.

To exacerbate the problem, IoT devices, while simple, are ultimately deployable connected computers or computing nodes. These devices, which include everything from smart light bulbs and security cameras to routers, server management cards, and beacons, were developed on the assumption of "good-enough" source of software-based entropy functionality. However, this assumption is flawed, as demonstrated in the 2012 study cited above. As seen with recent DDoS attacks, gaining access to the keys, or subverting a weakened key, allows for these devices to be quickly converted from positive assets to modern day digital pirates.

Today, it is even more difficult for application developers to find robust methods to generate high-quality entropy. It can be argued that while the need for strong entropy is growing exponentially in day-to-day software applications, finding such sources in modern computing systems has become a vanishing and elusive search. To that end, some efforts have been proposed to offer trusted external sources of entropy that can be shared by multiple applications in a production environment.

Entropy-as-a-Service (EaaS) to the Rescue

The United States' National Institute for Science and Technology (NIST) recently proposed the development of a new security service, Entropy-as-a-Service (EaaS), for procuring entropy. NIST's EaaS development proposal will utilize a standards-based approach to devise a universally available method to securely provide high quality entropy to cloud-based applications, embedded and IoT devices.

"The proverbial "Achilles' Heel" of the assurances from cryptographic security protection is the strength of the keys used to protect critical data."[3]

Entropy-as-a-Service greatly simplifies the development and deployment of modern applications or devices that require strong cryptographic capabilities; which is the vast majority of them nowadays. EaaS can be used to seed applications with high quality entropy generated from strong independent hardware sources.

Being 'as-a-Service' will allow developers to get their products to market in a timely manner while not having to worry about designing their own entropy sources. In other words, once deployed, their devices will be able to access true entropy from an Internet-based architecture. This will boost their product's cryptographic strength and security while minimizing the development overhead. And entropy can be refreshed to implement new keys as needed to further thwart attacks or take advantage of future cryptography requirements.

NIST's EaaS Reference Architecture

NIST's EaaS provides a secure method for devices and applications to seed their local RNG using strong entropy from an EaaS server. The protocol assures the confidentiality of the entropy data being returned to the requester as well as its integrity, authenticity and freshness. NIST further recommends that developers look to seed their applications or device's RNG by making requests to multiple EaaS servers. This is to further guarantee that the ultimate seed used by the application or device RNG will be very strong. NIST's intent in promoting EaaS is to make access to strong entropy data as ubiquitous and easy to obtain as time synchronization has become, thanks to the universal availability of Network Time Protocol (NTP) servers all over the Internet.

NIST's proposed reference architecture for their EaaS concept is described in "EaaS: Unlocking the Full Potential of Cryptography".[4] The architecture is built around a simple client-server interaction where a client can obtain a freshly generated entropy response in a confidential and authenticated manner. The "freshness" aspect of the response is achieved by the inclusion of a timestamp that the client can verify upon receipt and compare to a local clock. The response returned by the server is also digitally signed to provide the client a strong proof of the authenticity and origin of the seed being received. Finally, the EaaS server encrypts every single response under a unique key specific to each client.

The Crypto4A Solution

The Crypto4A EaaS product implements the complete NIST EaaS reference architecture in a single 1U server form factor. This product is built on Crypto4A's Security Processing Appliance (SPA). The SPA is based on the company's Next-Generation Hardware Security Module (NG-HSM) that implements multiple entropy sources and uses them to feed a NIST SP-800-90 random number generator design. The on-board NG-HSM provides all of the cryptographic confidentiality, integrity and authenticity services necessary to guarantee the secure delivery of the EaaS capabilities. For more detailed information about Crypto4A's offering, please visit www.crypto4a.com.

Bruno Couillard, P.Eng., co-founder of Crypto4A, is also the co-founder of Chrysalis-ITS (Gemalto) and was the Chief Technology Officer (CTO) that designed the Luna hardware security module (HSM). He served as a senior consultant for the Canadian federal government leading the security design and evaluation of multiple high assurance military security products, as well as occupying a lead role with the Canadian Cryptographic Modernization Program since its inception. Bruno earned his Electrical Engineering degree from the Royal Military College of Canada.

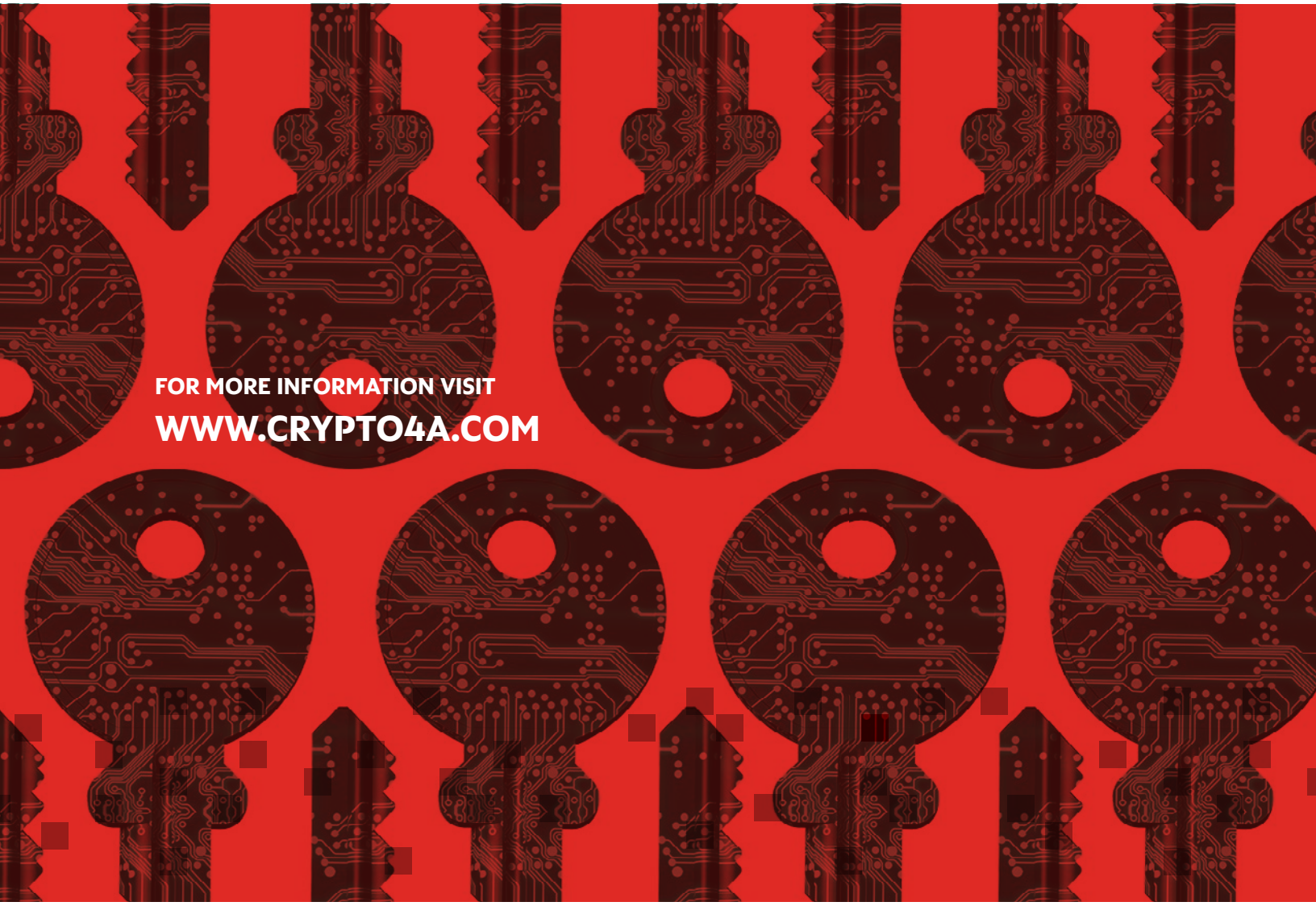
References

[1] Juniper Research recently predicted that the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015; https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

[2] https://factorable.net/weakkeys12.extended.pdf

[3] http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=920992

[4] http://csrc.nist.gov/projects/eaas/documents/pres_handout_final.pdf



CRYPTO4A

C4A-210-001-12092017