Redefining Randomness

Use Case: Managed Service Provider

Improving Randomness to Prevent Weak Keys and Ensure Availability

Quantis Appliance QRNG

Customer Profile: IT Company

Industry: Finance sector & Government

Country: Scandinavia

Business need	Solution	Results
Improve entropy generation to reduce delays in creating secure encrypted connections.	Quantis Appliance based on Quantum Random Number Generator (QRNG)	New revenue stream with secure high quality high availability services for customers

Business need

This Nordic-based IT company has a strong local and regional presence. The company provides IT solutions, business processes, financial services, internet banking services and business critical solutions to the finance sector and governments. These customers require a high quality, secure and easy-to-use service for both their employees and the clients that use their services. Each day tens of thousands of people access the banks' services for payment, money transactions, buying & selling stocks and other services.

In order to guarantee safe access to customers' applications, the company tried to improve security by implementing a PKI (Public Key Infrastructure) based on security certificates and by encrypting data transfers. But they realised that it took a long time (in some cases up to 10 minutes) to generate and assign a certificate. This had a direct impact on remote desktop applications e.g. applications that were running on the external server.

Since the IT company hosted core banking applications for banks and financial institutes that provided services to their own customers, these delays had a serious knock-on effect. The customers of the bank often experienced significant delays when they needed to link to banks' applications, especially at peak times.

After a careful investigation, the company realized that the reason behind the delay in receiving keys and certifications was that the calls to the randomness file/ dev/ random were blocked until enough randomness had been acquired to generate the cyptographic keys necessary for certificates and encryption material. In most cases the computers/servers pull the entropy from an external source, such as the movements of the mouse, disc interrupts, etc, but in isolated data

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com

centers or networks, such external entropy is limited. This phenomenon was particularly apparent in the morning around 8.30, when many of the users logged on at the same time.

The first users experienced fewer problems as the linux entropy pool had been replenished during the night, but later users had to wait a long time for the new entropy to be generated. The potential risk for losing customers' trust, and losing the customers due to mistrust, had a significant financial impact for the banks.

The company therefore realized that a hardware RNG was needed; to both resolve the delay in creating certificates & keys and to achieve a good level of encryption for mission critical banking applications; and also to upgrade the service to provide high availability.

Solution

The company looked for a partner to not only provide true random number generators but also to have the know-how and knowledge to help them implement the resulting solution securely.

One of the main requirements was to find the right true random number generator (TRNG). They knew that conventional algorithm and software based random number generators (called PRNG, Pseudo Random Number Generators) are deterministic, making their resulting entropy, or randomness, is untrustworthy. They also wanted to enter the new technological era by using TRNGs.

A true random number is a number generated by a process, whose outcome is unpredictable, and which cannot be subsequently reliably reproduced. Since the only way to achieve true randomness is via physical phenomena benefiting from the random nature of quantum physics, it was logical to search for a company that could provide true random number generators based on quantum technology called quantum random number gernerators, or QRNGs.

The case was discussed with ID Quantique (IDQ) which proposed its Quantis Appliance to solve the customer's problem. Quantis Appliance is a network-attached device, which securely generates and delivers high quality quantum random numbers for security and cryptographic applications in enterprise, data centers, government, gaming and cloud environments. Quantis Appliance is designed for environments, where high availability is necessary. It can be inserted in, or removed from, an operating network with no impact on any other appliance, such as servers, switches and Hardware Security Modules (HSMs).

IDQ helped the company measure the entropy level of their Linux servers' kernel pool and could demonstrate the low condition of entropy.

Results

The IT company deployed the Quantis Appliance in a redundant set up in their data centers. With the help of a software client installed on the server, the level and quality of entropy is measured, and – if required - more entropy is injected into the kernel pool. By injecting entropy at the level of the Linux kernel, the FIPS certification of the higher level crypto stacks is retained.

The delay in generating security keys and issuing the certificates was resolved, even during peak working hours. This allowed the banks and financial institutes to offer high quality and high availability services to their customers and it allowed the IT company to regain the trust of its clients. Moreoever, the provision of encryption and certificated issuance services allowed the IT company to generate a new revenue stream.

> *"We are pleased with the performance and the simplicity that the Quantis Appliance offers. Providing true random numbers based on the latest quantum technology, easy access and simple configuration are among the benefits that we gained by having Quantis Appliance."*
>
> Comment from IT Company CISO

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com