SOLUTION BRIEF

WHITEWOOD®

net / RANDOM™

HELPING SECURE THE INTERNET OF THINGS WITH NETWORK DELIVERED TRUE RANDOM NUMBERS

Centralized random number generation for IoT devices

The term Internet of things (IoT) spans such a wide variety of devices and markets, from light bulbs to artificial hearts, drones to driverless cars, that it becomes almost meaningless. The core tenant of the IoT is that the devices in question are intelligent compared to their non-IoT equivalents and that they communicate over networks. What this boils down to is that IoT devices understand data – they can collect it, process it and in the form of commands, act on it. Inevitably they become targets for data theft and subversion. What's more, they are vulnerable. They are out in the field – interacting with the real world not safely tucked away in a datacenter.

But it's easy to focus on the devices themselves. The IoT is a network, an ecosystem of control centers, hubs, data repositories, messaging gateways and concentrators, it's the only way IoT systems can scale and be resilient. Furthermore, they are constantly changing. Many IoT deployments will span decades and might be in constant transition as technologies evolve. What this means is that IoT security must always be looking ahead. It must be prepared for new threats before they emerge. The sheer scale and inertia in IoT deployments makes it impossible to have a reactive approach to emerging threats. IoT security must always try to be one step ahead.

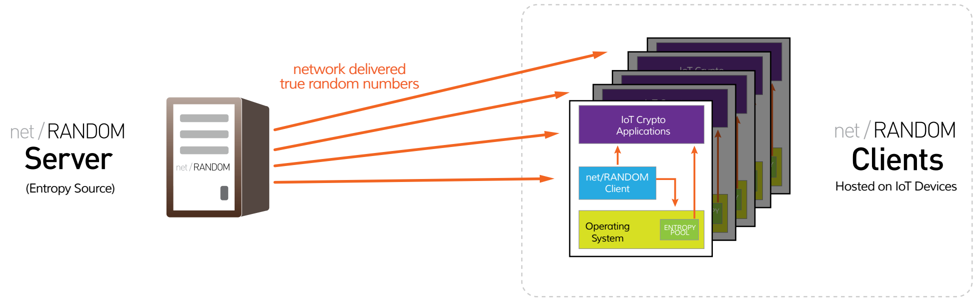
An area of constant evolution is cryptography. Not only is the use of encryption becoming ubiquitous but the underlying algorithms and key management practices are also being strengthened. This is to combat attackers with access to ever more powerful computers that one day, and potentially in the lifetime of IoT devices, might even include quantum computers with their ability to crack many of our current algorithms.

Cryptography underpins so much of IoT security. Everything from data at rest encryption to network encryption, device and server authentication, message integrity validation to securing firmware updates. All of these processes rely on random numbers to generate keys and perform crypto operations. If these random numbers are in any way predictable they weaken the security of the whole system. This is the reason by security certifications such as FIPS 140 are increasingly required in the IoT market. So, the big questions are – where do these random numbers come from and how do we know for sure that they are good enough?

Unfortunately, neither of these questions has a simple answer. Firstly, each IoT device typically uses deterministic software processes within the operating system to generate random numbers. These otherwise predictable outputs are randomized by capturing noise or other unpredictable events within the IoT hardware or by detecting apparently random behavior in the local environment. Inevitably the quality of random numbers will therefore vary from device to device. Secondly, measuring the quality of random numbers is notoriously unreliable and detecting when quality is insufficient is almost impossible.

These two issues are of growing importance across all application environments but are particularly prominent in the IoT where they are in direct conflict with ever-increasing security requirements. The cost structure for IoT devices is such that processing power is constrained and access to real-world entropy often are severely limited. The IoT manufacturer and operator are unlikely to have sufficient control over the physical environment to isolate the noise source from external influence and to depend solely on chip based noise sources places too much trust in manufacturing controls and lack of hardware degradation. Attesting to the security of any single device is difficult but to attest across a large distributed population of devices, some of which may have been in the field for many years, is untenable.

Whitewood's netRandom solution addresses both these critical issues of quality and consistency by delivering true random data over the network to reseed populations of IoT devices. Reseeding requirements can be as low as a hundred bits a day or even lower, but only by ensuring that those bits are truly random. A steady background supply of random seeds can transform the quality of random numbers available to applications running on the device. Furthermore, by supplying seeds from a shared central source can help ensure that the quality of random numbers is consistent, across all devices in the field, irrespective of their hardware capabilities or local environment.

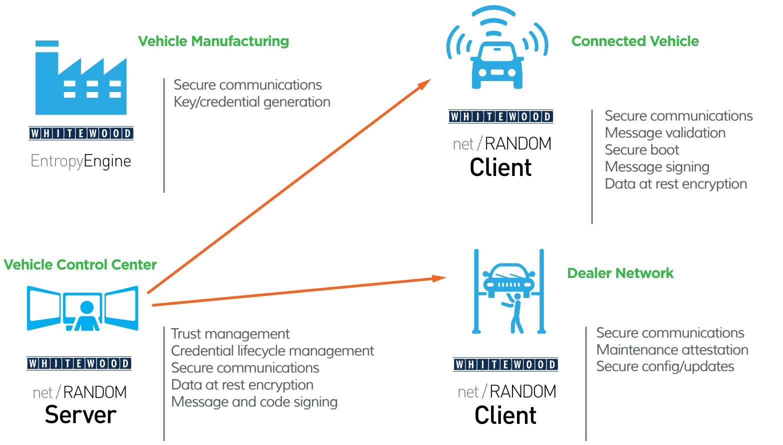


The netRandom solution comprises the netRandom Client and netRandom Server. The client is a small footprint agent that resides on the IoT device to request random seeds over the network and generate true random numbers for applications running on that same device. The netRandom Server is a shared entropy source and networked provider of random seeds. The Server would typically be co-located with other IoT management infrastructure items such as asset, security and configuration management systems and controlled by the system operator.

In addition to supplying the needs of individual IoT devices there is a broader requirement to strengthen the crypto based security across the entire IoT ecosystem that includes datacenter based systems, manufacturing facilities and maintenance services. For example, in the case of manufacturing, there is often a requirement to generate large quantities keys and credentials to be implanted in devices. This activity consumes large quantities of random numbers. To help address this requirement, Whitewood also provides a dedicated high-performance random number generator, the Entropy Engine. This hardware device employs the fundamentally random characteristics of quantum mechanics to generate entropy and random numbers that are truly random.

The diagram below illustrates a typical IoT ecosystem and the way that random number generation and delivery can play a critical role as the foundation to a wide variety of common crypto processes that protect data and overall system integrity.

DEPLOYMENT SCENARIO - CONNECTED VEHICLES



Security in general and cryptography in particular is hard to get right. In most cases, IoT developers rely on crypto experts to provide pre-tested and often pre-certified toolkits to incorporate in their designs. Whitewood has partnered with leading providers of crypto toolkits and supply chain security systems to enable developers to most easily take advantage of netRandom capabilities.