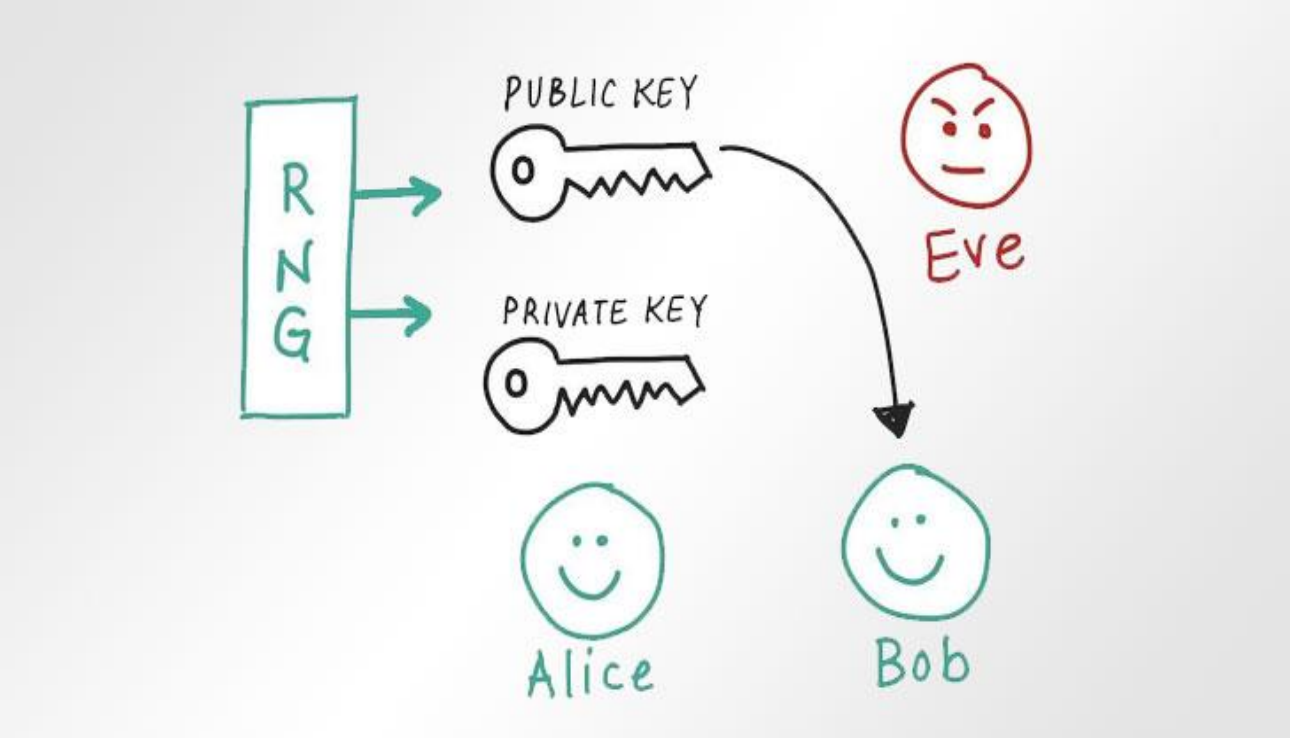
CYBERSPACE SECURITY GROUP
COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS SERVICE
ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo, Quezon City

A Critical Random Number Generator Flaw Affects Billions of IoT Devices



A critical vulnerability has been disclosed in hardware random number generators used in billions of Internet of Things (IoT) devices whereby it fails to properly generate random numbers, thus undermining their security and putting them at risk of attacks.

"It turns out that these 'randomly' chosen numbers aren't always as random as you'd like when it comes to IoT devices," Bishop Fox researchers Dan Petro and Allan Cecil said in an analysis published last week. "In fact, in many cases, devices are choosing encryption keys of 0 or worse. This can lead to a catastrophic collapse of security for any upstream use."

Random number generation (RNG) is a crucial process that undergirds several cryptographic applications, including key generation, nonces, and salting. On traditional operating systems, it's derived from a cryptographically secure pseudorandom number generator (CSPRNG) that uses entropy obtained from a high-quality seed source. When it comes to IoT devices, this is supplied from a system-on-a-chip (SoC) that houses a dedicated hardware RNG peripheral called a true random number generator (TRNG) that's used to capture randomness from physical processes or phenomena.

Stating that the manner in which the peripheral is being current invoked was incorrect, the researchers noted the lack of checks for error code responses across the board, leading to a scenario where the random number generated isn't simply random, and worse, predictable, resulting in partial entropy, uninitialized memory, and even crypto keys containing plain zeros.

"The HAL function to the RNG peripheral can fail for a variety of reasons, but by far the most common (and exploitable) is that the device has run out of entropy," the researchers noted. "Hardware RNG peripherals pull entropy out of the universe through a variety of means (such as analog sensors or EMF readings) but don't have it in infinite supply.

"They're only capable of producing so many random bits per second. If you try calling the RNG HAL function when it doesn't have any random numbers to give you, it will fail and return an error code. Thus, if the device tries to get too many random numbers too quickly, the calls will begin to fail."

The problem is unique to the IoT landscape as they lack an operating system that typically comes with a randomness API (e.g., "/dev/random" in Unix-like OSes or BCryptGenRandom in Windows), with the researchers highlighting the benefits of a larger entropy pool associated with a CSPRNG subsystem, thus removing "any single points of failure among the entropy sources."

Recommendation

Although the issues can be remediated with software updates, the ideal solution would be for IoT device manufacturers and developers to include a CSPRNG API that's seeded from a set of diverse entropy sources and ensure the code doesn't ignore error conditions, or fail to block calls to the RNG when no more entropy is available.

"One of the hard parts about this vulnerability is that it's not a simple case of 'you zigged where you should have zagged' that can be patched easily," the researchers said, stressing the need for implementing CSPRNG in an IoT operating system. "In order to remediate this issue, a substantial and complex feature has to be engineered into the IoT device."

References

https://thehackernews.com/2021/08/a-critical-random-number-generator-flaw.html

https://thecybersecurity.news/general-cyber-security-news/a-critical-random-number-generator-flaw-affects-billions-of-iot-devices-11818/

https://news.sodaiacademy.com/a-critical-random-number-generator-flaw-affects-billions-of-iot-devices/

https://alltech.news/cyber-security-news/a-critical-random-number-generator-flaw-affects-billions-of-iot-devices-40980