by KtioszDev

PS4 SAMU

Vol.1

What is SAMU?

The Secure Asset Management Unit (SAMU) is a separate processor from PS4.
Actually it’s not very easy hack into, and it is the reason why we don’t have crazy hacks/mods happening to the PS4. It operates a massive amount of information in there, and inside we find 3 contents:

- Spoofing ;
- Passphrase Keys ;
- Index.dat Spoofing

With Spoofing you can trick your system to allow you to go online with a modified console with an OFW (Official Firmware). Passphrase Keys protect private information and control all operation in PS4 that contain cryptographic system. Index.dat Spoofing are all information that comes from index.dat.
SAMU is an HSM (Hardware Secure Module), developed by the Semiconductor Company, Advanced Micro Devices. HSM is a very amazing typical piece of hardware that usually runs through firmware or software that binds itself to a computer or server.
Cryptographic Operations they contain are:

- Digital Signatures ;
- Hashing ;
- Encryption ;
- MAC

Digital Signatures are a type of electronic signature that encrypts documents with digital codes. Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Encryption is the process of converting information or data into a code, especially to prevent unauthorised access. MAC (Message Authentication Codes) is a cryptographic checksum on data that uses a session key to detect both accidental and intentional modifications of the data.
As previously mentioned, the Samu is difficult to hack, in fact the code says:

```
"Even with a kernel exploit, the SAMU processor is one of the few areas which we
don't have complete control over.
Although we can interact with it to decrypt almost everything
it is impossible to extract any keys so that decryption could be done externally."
```

In conclusion, we can say that SAMU is a strong processor that holds almost everything everyone in the PS4 Scene wants. If someone ever handles SAMU, modding has the chance to go online, but I don't know how things would work with the banning and the CIDs.