SS8 – Replacement for Insecure Signalling System No. 7 (SS7) Protocol revealed

Posted on **April 01,2017** by **lynx**

The ageing SS7 protocol has reached it's end of life. Security experts around the world have criticised vulnerabilities a long time ago. SS7 even facilitated unsolicited surveillance attacks. What's more, it has its own talks at the annual Chaos Communication Congress – which is a clear sign of fail if there is more than one presentation dealing with inherent design failures. It's time to put SS7 to rest. Since the 1970s the requirements for signalling have clearly changed. It's not only about telephones any more.

SS8, its successor, features a brand new design and fixes the many shortcomings of SS7. New technologies such as blockchain, artificial intelligence, crowd routing, social signalling, full "tapping", and deep state connections are now part of the core functions. Furthermore, SS8 is completely in harmony with Big Data, because it offers a compressed metadata format for long-time storage (thus accommodating requirements of different countries all over the world). It had been secretly tested, and the deployment is planned to start at the end of 2017. The upgrade will be seamless and will be over by Christmas, as usual.

New features of SS8 include

- zero-knowledge surveillance,
- in-band cyber defence by cloud algorithms,
- Big Data API for metadata backup to off-site storage,
- military-grade end-to-end obfuscation,
- wire "tapp" proof countermeasure heuristics,
- signalling transactions secured by a blockchain,
- multi-peer conversations (bidirectional and listening-only),
- attocells for PAN or NFC environments,
- integration with 5G networks, and
- backported 6G features.

The future of communication is looking bright again. An in-depth security analysis of SS8 will be given at DeepSec 2017 in November. If you regularly use telephones of any kind, then you might be interested in attending.

Posted in:High Entropy | Tagged:Mindset,Network | With 0 comments