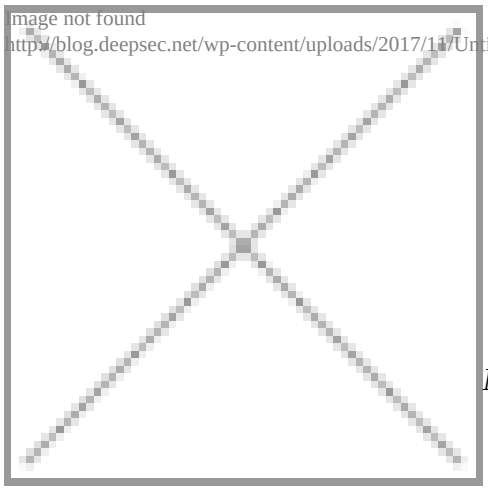
DeepSec2017 U21 Talk: Lessons Learned: How To (Not) Design Your Own Protocol – Nicolai Davidsson

Posted on **November 15,2017** by **sanna**

"One of the first lessons of cryptography is “don’t roll your own crypto” but we were bold enough to ignore it", says Nicolai. "Single Sign-On is so 2016 which is why we’d like to introduce its replacement, Forever Alone Sign-On – FASO. This talk will discuss one of the ugliest SSO solutions you'll ever see, its updated, slightly less ugly, iteration, and, ultimately, FASO.

We'll discuss the use cases, questionable decisions made during the planning process, the actual self-rolled, totally vulnerable, cryptography, and the even worse code architecture.

In all seriousness: The talk reflects on the design process of a SSO protocol and its first two iterations, going from a semi-functional workaround to an experimental OAuth-and-the-like alternative utilizing pre-shared keys, symmetric cryptography and implicit authentication."



Nicolai is a security researcher at zyantific and a graduate student at Ruhr University Bochum where he’s also an avid member of the FluxFingers CTF team. He likes burgers, buffer overflows and bad crypto.

Posted in:Conference,Development,Security | Tagged:DeepSec,FASO,SSO,Talk,U21 | With 0 comments