Summary of “The Sybil Attack”

Hou, Jue

[jue.hou@helsinki.fi](mailto:jue.hou@helsinki.fi)

In the article the article of this week, author introduced a special attack for large-scale distributed system, which is named as “Sybil Attack”. The mechanism of the Sybil Attack is that the faulty remote entities counterfeit and present multiple identities to the local entity so that it can defeat the effect of redundancy. The redundancy is originally used for reducing the dependence on entities which might be hostile. It is possible to challenge the identities to prove that they are legitimate under some conditions. However, these conditions can hardly be proved to be reasonable as assumptions. On the other hand, they cannot be practiced as system requirements in the real world as well. For example, all the identities must be verified by all the entities of the system in the exact same time. Obviously, it is not possible as well as practicable. As a conclusion, with the absence of certification authority, system is always very vulnerable to Sybil Attack. Thus, a logically-centralized and trusted certification authority is necessary.

The author used some trivial proofs to collectively justify his claim, which also, in my opinion, make the article quite straightforward.