

Title: Anonymous Single Sign-On With Proxy Re-Verification



Abstract: An anonymous single sign-on (ASSO) scheme allows users to access multiple services anonymously using one credential. In this talk, I will present a new ASSO scheme, where users can access services anonymously through the use of anonymous credentials and unlinkably through the provision of designated verifiers. Notably, verifiers cannot link a user's service requests even if they collude. The novelty is that when a designated verifier is unavailable, a central authority can authorize new verifiers to authenticate the user on behalf of the original verifier. Furthermore, a central verifier can also be authorized to de-anonymize users and trace their service requests. This scheme can be applied to smart ticketing where minimizing the collection of personal information of users is increasingly important to transport organizations due to privacy regulations such as general data protection regulations (GDPRs).

Short Bibliography: Jinguang Han is a professor at Nanjing University of Finance and Economics, China. He obtained his PhD degree from University of Wollongong in 2013. His research interests include cryptography, access control, cloud computing, network security, privacy-preserving systems, etc. He has published more than 60 academic papers in journals and conferences including IEEE TPDS, IEEE TC, IEEE TIFS, IEEE TDSC, ESORICS, etc. He was a program committee co-chair of ProvSec 2016, FCS 2019, SPNCE 2020, and served as a program committee member of over 100 international conferences including ESORICS'20, ACNS'20, ICICS'19, PST'18, CANS'17, GlobeCom'16, AsiaCCS'15, TrustComm'15. He is an associate editor of Soft Computing and an academic editor of Security and Communication Networks.