Full Name (English):	Rui Jiang	Recent Photo 
Affiliation (English):	Southeast University	

Biography+Email Address

Rui Jiang is now an associate professor at Southeast University, China. He received his Ph D degree at Shanghai Jiaotong University, China in 2005. He published more than 80 papers in *IEEE TPDS*、*TSC, Computers & Security, Journal of Computers*, respectively. He had authorized more than 30 national invention patents. He gained Second Prize of Scientific and Technological Progress for Shanghai. His current research interests include security of cloud computing and big data, AI system security, cryptanalysis and design of communication protocols, secure mobile network and systems communications, mobile voice end-to-end secure communications, and applied cryptography.
Email: R.Jiang@seu.edu.cn

Speech Title (English):

Cryptanalysis on TLS Protocol Based on Strand Space Model

Speech Abstract

In this report, we present cryptanalysis on TLS protocols, which includes TLS 1.2 and TLS 1.3, based on strand space model and authentication test. Firstly, we formalize TLS 1.2 and TLS 1.3 with strand space model theory. Then, according to the rules of authentication test, we make cryptanalysis on TLS 1.2 and TLS 1.3, respectively, and propose two kinds of attacks, which are server spoofing attack and user impersonation attack, on TLS 1.2 and TLS 1.3. Hence, we present detailed ways on these two attacks with experiments, in which the adversary may impersonate server to cheat users, and also impersonate users to cheat server without being detected. Finally, we may give some advices to remedy these two attacks on TLS 1.2 and TLS 1.3.