



A SECURITY MECHANISM FOR RFID WITH DEPENDABLE PROXY

JUN ZHOU^{1,2}, YONGJUN XU¹, XIAOWEI LI¹

*¹Institute of Computing Technology
Chinese Academy of Sciences
Beijing 100190, China*

*²Beihang University
Beijing 100190, China*

ABSTRACT—RFID (Radio Frequency Identification) is a non-contact auto identification technology widely applied in many fields nowadays, while its security issues also get much concern in practical applications. So far, experts from industry and academia have proposed a series of solutions, mainly including physical methods, security protocols based on cryptography, hardware encryption technique and so on. However, various defects still exist in all the three categories, which may lead to the failure to achieve the security requirements of RFID systems. Aiming to make a further improvement to these solutions, we propose a security mechanism designed with dependable proxy in this paper, which demonstrates a good fusion of physical methods and security protocols. In allusion to the new scheme, we use BAN logic to do the formal analysis to derive the security objectives of our mechanism. Subsequently, given the corresponding theoretic analysis and comparison, it is indicated that the new mechanism can efficiently defend RFID systems against monitoring, deception, tracking, replay attacks, and greatly decrease the possibility of suffering denial of service. The asynchronous problem that may arise on systemic information is also discussed to lessen the authentication failure of the legal tags.

Key Words: RFID, physical methods, security protocols, proxy, BAN logic