How to encourage cryptocurrency exchange to secure their systems

Shin'ichiro Matsuo[1], Yuta Takanashi[1,2], Pindar Wong[3], and Eric Burger[2]

[1] Georgetown University
[2] Japanese Financial Services Agency
[3] VeriFi Ltd.

Abstract. Huge number of low power devices, such as smart-card and RFID-tags, will be used around our life including in commercial and financial activities. A prime application of such devices is entity authentication in pervasive environment. The obvious concerns in this environment involves getting security against tag-forgery (even by adversary controlled readers) and, on the other hand, giving users privacy against linking of different authentication transcripts. Many cryptographic protocols have realizes such requirements. However, there is no scheme which realizes, both, forward-privacy and backward security right after some leakage is occurred. Since some devices among the huge quantity of expected devices will surely be compromised. it seems highly important, from an engineering point of view, to deal with limited damage of such exposures. In this paper, we propose the first scheme that realizes both requirements. It protects against partial leakage of tag-secrets and assures that forward-privacy is kept even if full information are leaked to an adversary.
Keyword: Cryptocurrency, Exchange, Information security management, standards

1 Introduction