

PREFACE

The security level of the authentication scheme using smart card is very important, especially the security level against offline password guessing attack. Even only the user of smart card knew the password, but with the special technique e.g. offline password guessing attack, the attacker can get the user's password. Therefore, the security level of the authentication scheme against offline password guessing attack has to be improved such that the attacker who conducts the offline password guessing attack needs to know another secret for succeeding in obtaining the user's password. This research proposed a method for overcoming the problem. Hopefully this method will be worth for securing the smart card transaction. This research has been added a random number as another secret in securing the user's password. The secret is only known by the smart card and used only once time in every authentication process. If the security level of authentication using smart card is high, then transaction using smart card for e-banking, e-commerce, e-health will be more secured.

Bandung, 25 Agustus 2017

DANI ARUMANEGARA