PIN and Security Code Hammer Protection

ISS

Intelligent Switched Systems
P.O. Box 65003
Nepean, Ontario
K2G 5Y3 Canada
Tel (613) 288 8493
Web www.iswitched.com

April 2006

Introduction

Account and PIN – Security Code protection of any service can be circumvented by a slow attack if adequate protection is not used. The method of the attack is to slowly cycle through the available PIN number space for each account.

The account number is the easy part of the information. There are many methods available to obtain valid account number for credit cards, calling cards, and other access cards. The only piece of information that is missing is the PIN – Security Code number.

PIN – Security Code numbers can either be fixed length or variable length. Variable length offers a higher degree of frustration as a larger number space must be scanned, but that is the only effect it has. For automated attacks this represents no real challenge.

To carry out the attack, an access point is needed. This can be a calling card service, an internet login to a banking service, or any other validation service such as a web store front. A data base is created for all the accounts to be cracked, and a thresh hold is set for the retry time. The retry is the key to the attack. The threshold is set to be long enough so as to appear to be a genuine attempt by the user that has failed. Elaborate selection of the PIN can also aide in thwarting detection.

Once the account has been compromised, two things happen. The vulnerability is open for exploitation until it is detected. Once the vulnerability is detected, the genuine customer is denied access to their service.

Protection

For any service the clients can be classed into two distinct groups. Casual users and constant users. This distinction is very important in understanding what protection can be implemented.

For casual users a leaky bucket algorithm is used to implement a set of alarm triggers. A heuristic is implemented to determine the history of activities on the account. For every access attempt (either successful or failed) a score is generated to determine the current state of the account. The scoring takes into account the number of successful attempts, the number of failed attempts, and the frequency of access. Typical alarming condition are suspected problem, genuine attack. A suspected problem would be when there is a certain percentage of bad PIN attempts, say 10%. Attack would be a higher level, possibly 30%. Actions of monitoring and protection can be automatically put into place as each level of alarm is reached.

This protection is aimed at services that desire to have a large penetration of their access mechanism in the marketplace, which will not all be in heavy usage. A typical example of this is a calling card.

Valued Customer Protection

PIN – Security Code hammer protection will not work for users that access the service frequently. The slow nature of the PIN hammer attack will only show up as normal failed attempts by the user if the thresholds are set low. If the thresholds are set high, then genuine failed attempts by the real user will alarm the system, and possibly deny them access to the service. Neither situation is acceptable.

Valued customers are the backbone of services as they generate the bulk of the transactions. In order to ensure that they have easy access without the possibility of denial of service, alternate authentication methods should be used. These methods must employ stronger authentication to eliminate any possible attack.

Stronger authentication can be audio smartcards for phone authentication, contact smartcards for physical authentication (point of sale, computer connection, etc.) phone authentication from GSM type devices.

The key is have a strategy which allows for a wide customer base penetration while only making the strategic investment in security for the customers that are actually generating revenue for the business.

Business Impact

Every customer wants to feel important, but for a business there are economic constraints to work with in the service they are providing. For a customer that has a healthy interaction with the business it makes sense to invest in their needs.

Customer loyalty is often rewarded in the marketplace. The airlines are a good example of this strategy. Customers will stay with a service if they feel there is value, and quality. In the case of a calling card, being certain that the card will not be deactivated while the customer is traveling is essential. The same holds true for a credit card.

Denial to either of these services leads to customer frustration and lack of confidence in the company that runs the service. In addition that frustration can lead to loss of the client because they feel the service provider is not providing the service at a level consistent with their needs.