Analyzing Preauthentication Timestamps To Crack Kerberos V Passwords

Ahmed Alazzawe, Anis Alazzawe, Asad Nawaz and *Duminda Wijesekera

*ISE Department, CSIS and C4I,
George Mason University,
Fairfax, VA 22030.

Abstract. Platforms, including Microsoft Windows 2000/2003 Servers, utilize Kerberos V for authentication services. Kerberos V introduced several improvements over its predecessor including a preauthentication scheme that authenticates KDC bound requests prior to issuing tickets. Timestamps are incorporated within the preauthentication scheme causing a weakness. The time needed to obtain a password is decreased by capturing and subsequently utilizing this timestamp. This paper examines the computational efficiency obtained by utilizing the timestamp in attacking Kerberos V preauthentication data. We developed a program that would parse the preauthentication data in an attempt to recover the client's password. It uses a well-known cryptographic library and one embodiment thereof omits the last HMAC computation used in the verification process. Instead a timestamp is used to determine the success of the decryption process. Our findings indicate that utilizing the timestamp saves considerable processing time.

1 Introduction

As users of computing devices in securely networked environments, we are often oblivious to the many interactions between numerous computing devices within the network that assist us in accomplishing our tasks. One of the many transparently executed tasks is the mapping and provision of services to each individual user. This seemingly simple task requires quite a bit of sophistication. For example, a user must first be authenticated to a server or service. Sometimes mutual authentication is required where the server is also authenticated to the user. Many protocols have been implemented to help accomplish this task. One such protocol is Kerberos. Kerberos provides a method whereby a trusted third-party authentication service is utilized in verifying user identities [1]. As with the advent of any technology, there will always be flaws and exploits to its weaknesses. In an effort to secure a network and its contents against such flaws and weaknesses, one must understand the root of the problem. Unfortunately, this requires an in-depth knowledge of the innerworkings of the authentication system. Hence, a brief overview of the origins of Kerberos, its components, its deployment, and comparison between released versions will be presented prior to a detailed discussion of the weakness exhibited by a Kerberos-utilizing system.

Alazzawe A., Alazzawe A., Nawaz A. and Wijesekera D. (2006).
Analyzing Pre-authentication Timestamps To Crack Kerberos V Passwords.
In *Proceedings of the 4th International Workshop on Security in Information Systems*, pages 267-277