Groups Order inside a PAC of Kerberos' Ticket in Active Directory

Abstract

Kerberos (KRB) is an AAA (authentication, authorization, accounting) protocol that is predominantly used in Microsoft's Active Directory environments. It uses a token system called Tickets, which are granted to entities so they can later use to authenticate to services. Because of KRB's vulnerable position in a lucrative target for hackers, there are many vulnerabilities and attacks to be wary of. One such attack is ticket forgery, where a hacker can make their own tickets to authenticate where and when they want. One way to detect a forged ticket is by examining the order of the groups the entity is a member of and find anomalies. In this project, you will find the algorithm Microsoft uses to order groups, and write your own ticket forgery tool.

Project overview

In this project you will:

a. Study how Kerberos works.
b. Reverse engineer a windows function.
c. Write a tool of your own that can perform a ticket forgery attack, while keeping the order of groups in the ticket correct.

Prerequisites

1. Network Security (236350).
2. Reverse Engineering (236496).

Instructors

Ori Shacham-Barr (s.ori@technion.ac.il)

Eran Tavor (tavran@cs.technion.ac.il)

References:

[1] Kerberos Authentication flow, only section A of the article
https://www.hackingarticles.in/deep-dive-into-kerberoasting-attack/

[2] What are forged Kerberos tickets
https://www.thehacker.recipes/ad/movement/kerberos/forged-tickets