Computer Security - Tutorial 1
Elevation of Privilege Game

Kami Vaniea

January 25, 2016

1 Introduction

Today in tutorial we will be playing a card game invented by Microsoft Research. The goal of the game is to enable software designers and network engineers to threat model their designs and identify potential security weaknesses while having fun.

In real environments doing a security evaluation is often considered annoying and delegated to the most junior member of a team who is least capable of accurately identifying security issues. Security professionals can come in and scan a system, but at that point it can be challenging to go back and fix all the issues. Security professionals also have less of an understanding of the system design than the developers who built it. Ideally a team would threat model in advance of building a system, but this is rarely the case.

In this tutorial you will be playing the Elevation of Privilege card game to encourage you to think about how a system might be attacked and defended. The goal is to both think about how security is done and to learn from your fellow class mates.

2 Elevation of Privilege (EoP) Card Game

The official version of Elevation of Privilege can be found on Microsoft's website: https://www.microsoft.com/en-us/download/details.aspx?id=20303

The language used in EoP is drawn from the STRIDE Threat Model which describes types of attacks that line up with the properties of Security we learned about in the first lecture.

Properties	STRIDE
Confidentiality	Information Disclosure
Integrity	Tampering
Availability	Denial of Service
Accountability	Repudiation
Authentication	Spoofing
All	Elevation of Privilege

The following rules are slightly modified from the original game to support easier play in a classroom setting. The game is loosely based on the rules of Hearts.

Play

- Select one of the two system diagrams based on the level of experience of your group.
- Shuffle deck.
- Deal 5 cards to each player.
- Play starts with the youngest player.
- Play progresses clockwise and each player in turn follows in the suit if they have a card in suit. If they don't have that suit, they can play another suit.
- After playing a card the player should take a new card from the top of the deck. Players should always have five cards in their hands.
- After all players have played a card, the high card played takes the trick, with the Elevation of Privilege suit taking precedence over the lead suit. Only Elevation of Privilege (EoP) or the lead suit can take a trick.
- To play a card, read the card aloud, and describe either:
  - How such an attack could be accomplished on the system diagram.
  - How such an attack could be defended against on the system diagram.
- Other players can ask for clarification or help brainstorm how the attack could be accomplished or defended against. However, the current player is discussion lead and should be given the first chance to speak.
- Threats and defences should be articulated clearly and include the part of the network or system that they impact.
- The person who collects the most tricks "wins" the game.

3 Other points for discussion

This card game was selected to highlight a number of things security professionals need to do regularly.

Threat Modelling is a common activity where a security professional has to think about all the possible threats that might impact a system.