



Practical Threat Analysis of Passport Security Protocol

Introduction

Passport is a protocol that enables users to sign onto many different merchants' web pages by authenticating themselves only once to a common server. Passport is notable as it is being very widely deployed by Microsoft.

In the following case study we present the PTA threat model of Passport which is based on the excellent article "[Risks of the Passport Single Signon Protocol](#)" by [David P. Kormann](#) and [Aviel D. Rubin](#). These authors thoughtfully examined the vulnerabilities and threats that were relevant to the protocol at the time of publication (2001).

Our aim is not to reanalyze the security of Passport (which may have been changed since 2001 and whose specifications are no longer publicly published) but rather to demonstrate the capability of PTA in representing the various ingredients and considerations relevant of a classical protocol cryptanalysis. Hence we have taken the content of the paper as-is and stayed as close as possible to its statements and conclusions. We believe that using PTA will help researchers in clarifying the interrelation between security entities and control the multitude of factors involved in this type of studies.

Representing a theoretical analysis through a real-life story

PTA methodology requires the assignment of financial values to assets and countermeasures and probabilities to threats. In order to transfer Kormann and Rubin paper to a PTA model we have decided to complement the academic cryptanalysis with a real life case data and have chosen the Passport-based solution for [Panhandle-Plains Student Loan Center \(PPSLC\)](#) to serve as the frame story of the analysis.

Preliminary assumptions on assets values

PPSLC, a Texas based student loans provider, decided to base its new user sign-in system on Passport's infrastructure. Although the PPSLC case study (presented at the case studies section of Microsoft site) is very instructive from a marketer point of view, it lacks the actual numbers relevant to the analysis, so we had to make some assumptions regarding the values of system assets as follows:

- The maximal damage that can be caused to a student due to forged purchases using her account is 1,000 \$ per year
- The maximal company's liability in case of a private information disclosure is 500 \$ per student per year

- The maximal damage that can be caused due to the unavailability of the online service is 50,000 \$ per year
- The maximal damage that may be caused due to decline in the system reputation and the trust of the students in the system security is estimated to be the 100,000 \$ per year

We further assume that the system serves 1,000 students. Note that these numbers are not sacred and were set only for giving a concrete example. PTA enables the user to easily modify such estimates at any time. Moreover, we recommend that you play with these values and see the effects for yourself.

Preliminary assumptions on countermeasures implementation costs

The majority of the proposed countermeasures deal with the leveraging of the Passport protocol. Since these tasks should be handled by Microsoft engineers we had to guess the cost of implementation of most the countermeasures. Again, for our purposes, the reality of these estimations does not really matter...

Compliance with Kormann and Rubin article

Both vulnerabilities of the Passport protocol and the potential threats to the system were extracted out of the discussion in the paper and were given a uniform level of description (with respect to the amount of details).

Some of countermeasures are already proposed in the article while other countermeasures were suggested by us. This is a natural consequence of the PTA's practical approach that associates countermeasures to vulnerabilities in order to provide an appropriate mitigation plan against the threats.

Threats probabilities, levels of threats' damages to assets and levels of mitigation of countermeasures were assigned by us. These assignments, which are not part of the paper, are subjective by their nature and crucially depend on the very specifics of the analyzed system. Therefore, they should be reexamined in real-life systems on a regular basis. PTA enables such dynamic changes of parameters' values with great ease.