

Tor Fingerprinting Attack: Project Plan

Nathan Dautenhahn

September 21, 2009

1 Introduction

This document will define the initial project direction and time-line. The general overview of our approach consists of several phases. Phase 1 will be to conduct general purpose research, in which the team will learn about the Tor architecture. Once a general understanding of the Tor architecture is gained the team will focus on an in depth analysis of the different modules that are directly related to the fingerprinting attack. In this way we will be able to understand Tor from the overall perspective, and then get in depth coverage where it matters most. This will allow us to get up to speed on Tor as quickly as possible allotting maximum time to perform implementation of the attack. Phase 2 will consist of the team brainstorming several attack vectors based upon our previous research. Once this phase is completed we will validate the options and start implementation.

2 Road Map

Meetings will be conducted weekly to allow for quick feedback to change the direction of the project if needed.

2.1 Tor Research (2 weeks)

- (1 week) Tor Architecture: read literature about how Tor works at general architecture level.
- (1 week) In Depth Research: read literature specific to the fingerprinting attack. At this point we will define three focuses for further research that will be given as a task to each member. In doing this we will cover more ground than if we all performed the same research.

2.2 Brainstorming (2 weeks)

This phase will consist of a brainstorming session in which we discuss the potential ways to implement our fingerprinting attack. We will come up with several ideas that we will then research in order to check the validity of each approach.

Some of the questions this phase should answer are:

- What type of signature will we use to fingerprint the websites?
- Where will we attempt to perform fingerprinting?
- Will we analyze encrypted packets?
- Any other questions???

2.3 Implementation (4 weeks???)

Self explanatory implementation period should extend from all prior research.

3 Meeting Agendas

1. Meeting 9.26.09 4:30pm CSL 221

- Identify specific areas to understand better that directly correlate to the fingerprinting attack
- Assign research for the next week

2. Meeting TBD

- Present research findings
- Brainstorm attack vectors based on findings
- Next week will consists of researching the possible attack vectors

3. Meeting TBD

- Present findings
- More brainstorming
- If prepared start testing out implementation opportunities