I Still Know What You Visited Last Summer

Introduction

In this paper the authors test an attack based on a target's Internet history. By deploying a set of methods, an attacker can determine the visitedness of links by a target without him realising he is even providing such information.

Though a defence has been deployed, preventing all known automated techniques for history sniffing, there has been no effort made towards blocking interactive attacks.

Automated attacks

There are three kinds of automated attacks described in the paper. The first, direct sniffing, is based on the computed JavaScript of an HTML document after a link is visited or not.

The second one, indirect sniffing, consists of two classes of techniques, the first making visited and unvisited links take different amount of space causing unrelated elements to move, so the attacker can inspect the position of those elements. The second indirect attack class makes visited and unvisited links cause different images to load and it does not even require JavaScript.

The third one is side-channel sniffing. Side-channel attack happens when a system leaks information without the intend to, bypassing the system security. Timing attacks are the most common attacks of this kind, eg. when a page takes longer to load if a link is visited.

By limiting CSSs ability to control the distinction between the visited and unvisited links, one can prevent most of the automated attacks.

Interactive attacks

Interactive is called an attack when a targeted person is asked to do some tasks when visiting the page, interacting with it, providing information to the attacker without his knowledge.

The tasks given to a target to accomplish by the attacker, are called CAPTCHAs and consist of a variety of methods to determine visitedness of a link. Those methods are
the word CAPTCHAs, the character CAPTCHAs, the chessboard puzzle and the pattern matching puzzle.

The authors of the paper conducted an experiment with volunteers, asking them to complete a set of tasks containing those methods for history sniffing. The results showed that such an attack is feasible, especially if the attacker is interested in a small set of links.

Side-channel attack

Furthermore, the authors conducted a second experiment, a side-channel attack using a webcam. Based on the idea that nowadays every computer has a webcam, they took control of it using third party programs that the user would allow to have access to his camera.

By changing the colors of the screen, according to visited or unvisited links, by the reflection on a human face or the wall behind it, an attacker is able to determine the actual internet history of the user at that time.