Chapter 5
2-ClickAuth: Optical Challenge-Response Authentication Using Mobile Handsets

Anna Vapen
Linköping University, Sweden

Nahid Shahmehri
Linköping University, Sweden

ABSTRACT
Internet users often have usernames and passwords at multiple web sites. To simplify things, many sites support federated identity management, which enables users to have a single account allowing them to log on to different sites by authenticating to a single identity provider. Most identity providers perform authentication using a username and password. Should these credentials be compromised, all of the user’s accounts become compromised. Therefore a more secure authentication method is desirable. This paper implements 2-clickAuth, a multimedia-based challenge-response solution which uses a web camera and a camera phone for authentication. Two-dimensional barcodes are used for the communication between phone and computer, which allows 2-clickAuth to transfer relatively large amounts of data in a short period of time. 2-clickAuth is more secure than passwords while easy to use and distribute. 2-clickAuth is a viable alternative to passwords in systems where enhanced security is desired, but availability, ease-of-use, and cost cannot be compromised. This paper implements an identity provider in the OpenID federated identity management system that uses 2-clickAuth for authentication, making 2-clickAuth available to all users of sites that support OpenID, including Facebook, Sourceforge, and MySpace.

INTRODUCTION
Today, Internet users have accounts on a wide variety of web sites such as social networks, blog sites, forums and multimedia sites, e.g. YouTube. Usually users log in to these sites using a username and a password (Mannan & van Oorschot, 2007). When a user chooses a strong password, which is difficult for an attacker to guess, they often write down the password and/or reuse the same password for every site (Yan, Blackwell, Anderson, & Grant, 2004). This creates a risk
since an attacker that captures a password for one site is likely to try the same password on other accounts belonging to the user.

For sites with higher security requirements, we have designed and implemented the authentication solution 2-clickAuth (Vapen, Byers, & Shahmehri, 2010) as an alternative to the standard password-based solution. It offers a higher level of security while retaining the simplicity of passwords.

2-clickAuth is an optical challenge-response solution that uses a camera-equipped mobile phone as a secure hardware token together with a web camera to provide fast, simple, highly available and secure authentication. 2-clickAuth combines text-based and imaged-based data representations with real time video capture of data, in order to provide fast, multimedia-based authentication. Data is transferred both to and from the phone using Quick Response (QR) codes, a two-dimensional barcode type invented by Denso Wave Inc. It has been proven that QR codes can be reliably captured using mobile phone cameras.

To demonstrate and evaluate 2-clickAuth, we have implemented an identity provider for the federated identity management system OpenID, which uses 2-clickAuth for authentication.

The purpose of identity management is to solve the problem of users having many passwords and usernames to remember. One approach to identity management is federated identity management, in which participating sites form a circle of trust, so that if the user is authenticated to one site the other sites will automatically log the user in if the user visits them. A variation on this method uses a third party, often known as an identity provider, which holds information for the user and is responsible for authentication. Such systems are secure if the third party can be trusted (Shim, Bhalla, & Pendyala, 2005).

OpenID is a federated identity management system that uses trusted third parties called OpenID providers. Anyone can start an OpenID provider and the provider decides which login method to use. Some well-known OpenID providers are Google, Microsoft Live and Yahoo (OpenID Foundation, 2010). Web sites that allow users to log in using OpenID are called relying parties. Some well-known relying parties are Facebook, Sourceforge and MySpace (OpenID Foundation, 2010). The number of relying parties in OpenID is constantly increasing (JanRain, 2009).

A related problem is that of untrusted computers. All computers are potentially untrusted since they can contain malware such as key loggers that are capable of capturing user input, including passwords. Even a laptop that is owned and trusted by the user may be attacked if used in an untrusted environment, e.g. an unsafe network. Since computers and the environment may not always be trusted, mobility can create security problems.

When accessing web sites from untrusted computers or in untrusted environments, there is a need for more secure authentication than passwords can provide. This is especially true in federated solutions where the user’s password at the identity provider is a valuable asset that can give an attacker access to all web sites where the user has an account. An alternative to passwords should be as easy to use as passwords and should require no special software on the computer, so that it can be used anywhere, including places where the user cannot install software, such as at Internet kiosks or cafés.

2-clickAuth is designed to meet the above requirements concerning security, availability and ease of use.

The remainder of this paper describes the 2-clickAuth solution and its implementation in OpenID. Firstly, we discuss the current state-of-the-art and the design choices made for 2-clickAuth. After that we describe the 2-clickAuth system in detail and the performance of 2-clickAuth. Then we present an evaluation method based on the Electronic Authentication Guideline from NIST (Burr, Dodson, & Polk, 2008) that can be used to evaluate and compare authentication solutions for mobile phones. To conclude this paper we discuss