PHBooth

PHBooth

<series>draft-hallambaker-phbooth

<status>informational

<stream>independent

<ipr>trust200902

<author>Phillip Hallam-Baker

<surname>Hallam-Baker

<initials>P. M.

<email>phill@hallambaker.com

<keyword>Cryptography

<keyword>PKI

<keyword>OpenPGP

<also>http://prismproof.org/Documents/draft-hallambaker-phbooth.html

Cameras on mobile phones have become a major nuisance at public events. Half the audience wants to take photographs or video of the event with the result that at least a quarter of the audience ends up watching the spectacle through the screen of their phone. Cameras are cheap and QR codes provide a simple method of sharing URIs.

PHBooth is a protocol and implementation that allows an event host to provide still and video cameras that create a shared public record of the event that audience members can acquire by simply scanning a QR code.

This document describes the implementation and the security concerns arising from the scheme.

Introduction

Definitions

This section presents the related specifications and standard, the terms that are used as terms of art within the documents and the terms used as requirements language.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

## Defined Terms

## Related Specifications

## Implementation Status

# User Interactions

The PHBooth

Shared Code

A static QR code posted prominently at the event refers attendees to a Web site where photographs and videos taken at the event are made available for download.

This mode of interaction has the benefit of requiring least effort by subjects. Since the access code is static, users can scan it before or after taking a picture. They can even email it to other participants who took photographs but forgot to 'collect them'.

Dynamic Code

A photo booth is set up at the event with a fixed camera. Photographs are taken by pressing a button placed in or near to the subject and collected by scanning a QR Code generated after the picture is taken.

This mode of interaction has the benefit of allowing subjects to take private pictures but requires subjects to have some understanding of the process. For this reason, it is probably not best suited to applications in which high throughput is required.

Personal Device

In this variation of the Dynamic Code interaction, the user uses their personal mobile device in place of a fixed button. To begin the interaction, the subject scans a static QRCode which refers them to a Web site which presents a button for them to press to take a photograph. They are automatically redirected to the download site after the picture is taken.

This mode of interaction has the benefits of the Dynamic Code interaction without the need for a button device to be provisioned separately from the camera. The chief disadvantage is that the process is rather more complicated for the user. For this reason, it is probably not a mode of interaction that users will be comfortable with unless they have time to understand it.

Personal App

Use of a dedicated mobile app allows a considerably better user experience and additional security controls such as encrypting images and videos so that they are not exposed on a public server. The chief disadvantage of this approach is that the users must download the app.

Implementation

Image Acquisition

Upload Task

Control Pad

Authentication

Security Considerations

Human Subjects

Since this is private research and not funded by any government agency, Human Subjects board approval is not required by law. The moral obligations of such work still apply however. The following controls are to be observed:

* Subjects MUST be clearly informed of the distribution scope of the images before images are captured.
* Booths SHOULD NOT be erected in spaces unless either subjects have given clear consent to be photographed or are in a public space where such consent is implicit.
* The field of view of the camera SHOULD be limited to avoid unintentional encroachment.
* Images MUST be deleted on request of a person clearly identified in it or request by a guardian thereof.

Privacy

Consent

Access

IANA Considerations

None