S-SPAN: Secure Smart Posters in Android using NFC

Jason Wu, Lin Qi, Nishant Kumar, Ram Shankar Siva Kumar, and Patrick Tague
Carnegie Mellon University, Electrical and Computer Engineering
{jasonwu, linq, nkumar1, ramshans, tague}@andrew.cmu.edu

Abstract—**Smart posters are a promising new use case for NFC-enabled mobile devices, but to date there has been a general lack of security mechanisms for NFC smart posters. We present S-SPAN - a secure smart poster system consisting of three parts: an administrative web interface for managing posters, a backend server for storing and serving data, as well as an Android application for end-users. S-SPAN enforces confidentiality and integrity of smart poster data as well as authentication/authorization of administrators and end-users, thus ensuring that only authorized users can access the content.**

I. Introduction

Smart posters, which allow businesses or other organizations to disseminate information to end-users in a more interactive fashion than standard posters, are an increasingly popular application of NFC tags. Such tags store small amounts of read-only (or less commonly, rewriteable) data. A typical use case for NFC smart posters is to provide users of NFC-enabled smartphones with quick access to a URL related to the poster content; for example, a user interested in a product advertisement might swipe her phone over the ad poster to open a webpage containing detailed specifications and a link to purchase the item.

There are also situations that call for smart posters to contain sensitive information only privy to specific users. For example, a museum may wish to use NFC smart posters in tandem with a custom smartphone application, to provide additional information about exhibits on the condition that the content should only be available to users who have paid for admission on a given day. S-SPAN aims to provide a framework for secure active-passive pairings between NFC tags and Android devices in a smart poster setting.

This project was motivated by the Report on Smart Posters by the NFC Forum: "The benefit of signing tags is that they become secure - they can't be changed to direct users to other content" [1]. Like any security analysts, our group recoiled in horror, when we read that the caretakers of NFC believe that signing tags make it secure. In particular, NFC tags are very low-cost and have no processing power, so smart posters containing sensitive information and based on NFC tags must be carefully designed with security in mind.

Within this context, NFC tags are vulnerable to spoofing as well as cloning [2], and the RF channel, like any wireless channel, is susceptible to data modification or man-in-the-middle attacks [3]. Furthermore, the NFC protocol as currently defined has some weaknesses, e.g. the standardized NFC Data Exchange Format (NDEF) does not guarantee integrity and authenticity, even in the presence of a digital signature [4]. The main goal of S-SPAN is to secure smart posters against attacks on tags, end-user devices, the RF communication channel, as well as the NFC protocol, thus ensuring confidentiality and integrity of poster data as well as authentication of poster administrators and end-users.

Summary of Contributions

With the unimpeachable notion that smart posters need to be secure, S-SPAN is carefully designed to overcome a subset of the above-mentioned attacks and, at the same time, enhance the user's tryst with the poster. We believe that this combination of resilience and experience makes S-SPAN a holistic, usable and off-the-shelf solution for securing smart posters. On the security front, S-SPAN is designed to overcome Tag Spoofing, Tag Cloning, Eavesdropping attacks and also provide avenues for auditing and revocation of posters. At the core of the application is the authentication framework that the application is interfaced with, which in our case is Carnegie Mellon's WebISO framework, but can be any such generic system. In order to read from any of the applications services, one must be 'logged in.' Our approach to eliminating tag spoofing and cloning is to store no information other than a string of random bytes in the tag. This is different from the conventional approach of storing the complete resource in the tag itself. Thus, if an attacker attempts to clone our tag, all he gets is a bunch of random numbers, from which no information can be gleaned about the resource. These random numbers function as the tag ID, and an authenticated user queries the database using an HTTPS connection thereby thwarting any possibility of eavesdropping. The administrator, a trusted member, whose only responsibility is to register the tags, has access to the audit logs of the posters and can revoke any poster, if malicious activity is suspected. The Implementation section elucidates on the complete architecture and workings of the poster.

II. Implementation Details

A. Backend Server

The backend for the smart poster application consists of two major components, namely a web interface for administrators as well as an API for the mobile application.

Only specific authorized users within CMU are allowed to access the administrative web interface. This policy is enforced

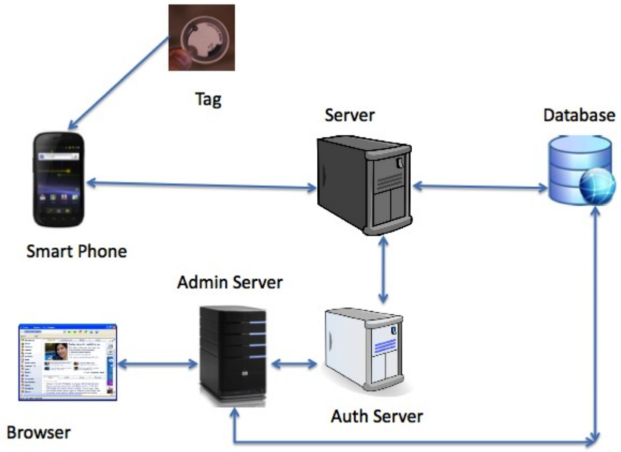
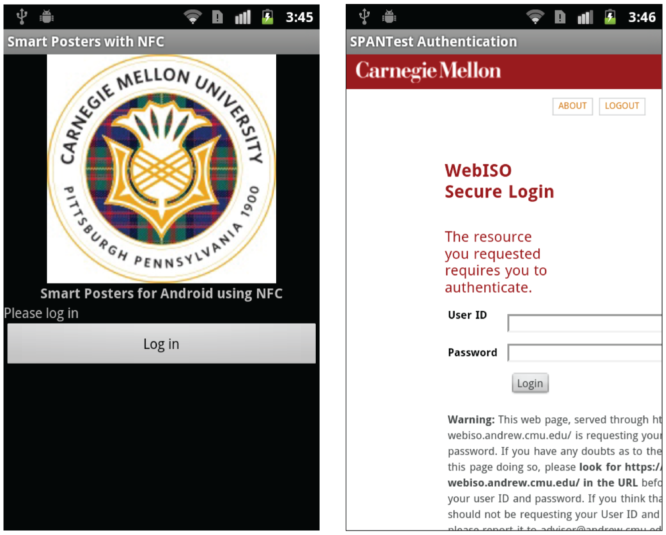


Fig. 1. Application architecture block diagram



Smart Posters with NFC

Smart Posters for Android using NFC

Please log in

SPANTest Authentication

WebISO
Secure Login

The resource you requested requires you to authenticate.

User ID

Password

Warning: This web page, served through ht
webiso.andrew.cmu.edu/ is requesting your
password. If you have any doubts as to the
this page doing so, please **look for https:/**
webiso.andrew.cmu.edu/ in the URL befo
your user ID and password. If you think tha
should not be requesting your User ID and
please report it to advisor@andrew.cmu.ed

Fig. 2. Authentication screens

through WebISO, the CMU single sign-on system which has the ability to limit webpage accesses to specific users. Once logged in, an administrator can add two types of smart posters: link posters or poll posters. A link poster contains a brief description and a URL to the web version of the poster or a related webpage. A poll poster contains a question as well as up to ten choices, from which the user can choose. These responses are sent to a URL that the administrator specifies. When adding a poster, the administrator also has the option to set an expiration date; the poster will be automatically disabled after that date. If the administrator discovers that a poster contains undesirable content or simply wishes to stop using a particular poster, she can use the web interface to manually disable the poster so that users of the mobile app will no longer be able to access the content. In addition, for auditing and accountability reasons, all actions performed on the administrative web interface are logged.

After an administrator adds a poster, the server generates a pseudorandom 39-byte (312-bit) tag identifier for that poster. The reason for this tag identifier size is compatibility, as certain types of NFC tags, such as the MIFARE Ultralight C, can only store 46 bytes of data, including about 7 bytes of metadata and padding. Tag IDs are never reused so as to prevent accidental or malicious reuse of an old, possibly disabled, poster to point to new content. The administrator should write the tag ID into an NFC tag and affix it onto the poster so that users of the smart poster app can see the additional content.

Our API provides the mobile app with read-only access to the database of tag IDs. For security reasons, all API requests must be made via HTTPS, and all input is validated before being acted on. Furthermore, WebISO integration ensures that a requestor must be authenticated in order to access the API at all. If the requestor has not yet logged in or has passed the 12-hour limit imposed by WebISO, then he or she is redirected to the WebISO Secure Login page. The main API request, *get_poster*, takes a tag ID for a particular poster and returns an XML file containing the poster content. If the tag ID is not in the database or the poster has already been disabled, then the XML file instead contains an error code. The mobile app can appropriately parse the XML file to retrieve the poster contents and display them to the user.

B. Authentication

S-SPAN treats the authentication mechanism as a module, so any cookie-based authentication system can be adapted to secure the administrative interface as well as the Android application. For our initial implementation, we have chosen to use WebISO, a cookie-based single sign-on authentication solution for web pages within the Carnegie Mellon domain.

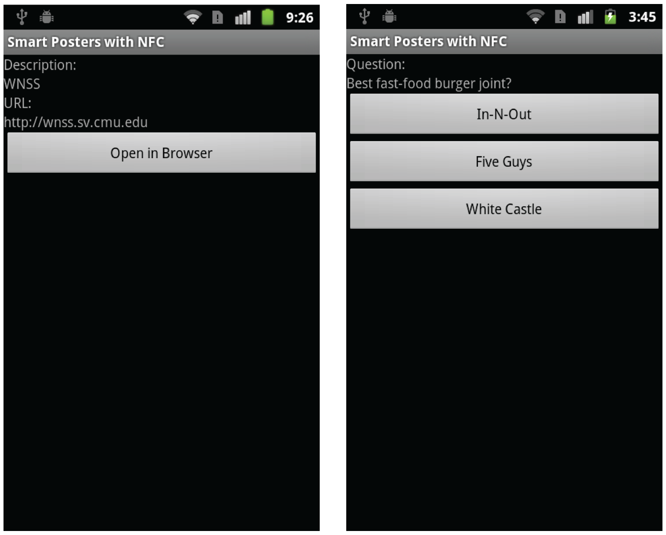
All pages and scripts on our backend server are WebISO-protected, so the Smart Poster app must check the user's authentication status on each request to the server. To perform this check, the app takes advantage of the fact that WebISO will automatically redirect requests with invalid cookies to the WebISO login page; if the check fails, then the app asks the user to once again provide credentials, as shown in Fig. 2. The app can easily be modified to accommodate authentication systems that treat invalid requests differently, e.g. by serving a standard error page or returning a specific HTTP status code.

C. Displaying Poster Contents

When a user scans an NFC tag, the app calls *get_poster* with the poster/tag identifier stored on the tag. The server will return an XML file containing either an error code or the poster contents. In the case of the former, the app will parse the error code, which could be indicative of a nonexistent tag ID or revoked poster, and inform the user. Otherwise, the app displays the poster contents, i.e. a link or a poll (Fig. 3).

III. Application Demo

Though we intend to bring our own phones for the demonstration, any NFC-enabled Android phone with the app is all



Description:
WNSS
URL:
http://wnss.sv.cmu.edu

Question:
Best fast-food burger joint?

Fig. 3. Link poster (left) and poll poster (right)

that is required to enjoy the experiment. The user can assume the role of an administrator or the role of an end-user. As an end user, one can enjoy the following features: *Vox Populi*, *ShareIt!* and *Contextual Presentation*. The Access Control and Revocation features are the perks of assuming an administrator role.

A. Vox Populi

Smart Posters can not only be used for displaying content from the poster creator but also receiving feedback/inputs from the viewers. For example, consider a use-case where a smart poster creator would like to show the viewers a questionnaire/poll for the poster. When registering the NFC tags in our system using the Admin UI, the poster creator would provide the questionnaire/poll, which would then be entered into our database and linked with the tag's ID. Now, when a viewer of the smart poster scans the NFC tag, he is shown the corresponding questionnaire/poll and can select one of the options to send his response to the server. Once the server receives the response, it stores the response in the database associated with each tag ID. The poster creator can view all the responses and statistics associated with the responses. There is also a *V-Like* feature, wherein a poster would have a like button when the content of the smart poster displayed. This helps the poster creator to know how many viewers liked the idea displayed on the poster. The application also supports a feature wherein the users could provide comments or feedback.

B. Contextual Presentation

In the context of smart posters, Contextual Presentation refers to displaying different 'additional' content for the same poster based on the user-group of the viewer. For instance, if a college recruiter would like to announce a seminar, but the teams meeting the CS students are different from those of the ECE students, there is no need to create two different posters. Instead, one poster can be created, and 'presented' differently, based on the 'context' of the user.

When an administrator registers tags for the smart poster, instead of providing a single content item for the poster's tag ID, he would provide multiple content items for the same poster tag ID, along with the group name/ID for each content item by which he wants the viewers to be distinguished. Since we require the user to authenticate to view the content for the poster, we would be able to distinguish between different viewers based on their group membership and present the appropriate content.

C. ShareIt!

Using the ShareIt feature the posters can be shared with social networking groups as the application has been integrated with third party APIs such as Google Calendar, Facebook and Twitter. If a user scans a poster which has an event associated with it and registers to attend it, then the application would automatically create an event in their Google Calendar.

D. Fine-grained Access Control

One essential requirement is that only an authenticated and authorized user should be shown the content associated with the poster; depending on the use case, an administrator can exert fine-grained control over poster access via a user whitelist/blacklist. Also, for the Admin UI, an administrator needs to be authenticated and would be able to see and edit only entries created by him. Although we use WebISO, this fine-grained access control mechanism is designed and implemented in the application in such a way that it would be able to support multiple authentication mechanisms.

E. Revocation of Smart Posters

This feature would provide an ability to measure the usage of the smart poster tags and would help in amortizing the application. The idea behind revocation of tags is that a user would register a poster content with the tag in our database. While registering the tags, he will also provide a time till when the tag/tag ID should be active. So, once this time period has ended the tag ID would be revoked by our database. If a viewer scans a revoked tag, he will not see the content originally associated with the tag. So a user could be charged based on the duration the user registers the tag. Also, revocation of the tags could be done manually by an admin through the Admin UI. This feature provides users and admins a way to revoke a tag which might be incorrect or has been tampered.

References

[1] NFC Forum, *Smart Posters*, April 2011

[2] A. J. Jara, A. F. Alcolea, M. A. Zamora, and A. F. G. Skarmeta, *Evaluation of the security capabilities on NFC-powered devices, in Smart Objects: Systems, Technologies and Applications (RFID Sys Tech)*, 2010 European Workshop on, 2010, pp. 19.

[3] B. Mohamed and M. Abd, *Strengths and Weaknesses of Near Field Communication NFC Technology*, Global Journal of Computer Science and Technology, vol. 11, no. 3, 2011.

[4] M. Roland and J. Langer, *Security Vulnerabilities of the NDEF Signature Record Type*, 2011 Third International Workshop on Near Field Communication, 2011.