A Study on Overcoming Security Problems of Two-dimensional Barcode in Web Applications

Lifen WANG, Liping HAN, Jingfeng ZHANG, Xiaohong HU

Beijing Polytechnic Telecommunication Engineering Institute, Beijing 100176, China.

Abstract — With the ever growing popularity of smart phones, two-dimensional barcode security of Web applications has become a matter of concern. Through security vulnerabilities analysis of two-dimensional barcode Web applications, we found the root of the problem being the use of two-dimensional barcode storage in web sites: simply to continue using this application model it is difficult to avoid attacks. We discuss the issues involved in proposing a new application model for two-dimensional barcodes.

Keywords - HTML5; Web App; 2D barcode; Security

I. INTRODUCTION

With the rapid development of the growing popularity of smart phones, mobile telecommunications enter the 3G and 4G era, the demand for an application on the smartphone are abnormal high. Smart phones and other mobile devices have constituted mobile services platform. This emerging mobile applications combined with powerful devices, have brought great convenience for people's lives.

Types of Web applications are also increasing, from the initial Games, Videos, and now the WeChat, Alipay, especially with the development of e-commerce, people have grown accustomed to online shopping, direct payments have become a Web application normal. Especially in recent years, the combination of Internet and financial industries, have a large number of Web applications with a payment function. I believe that in the near future, Web applications with payment function will be more and more. But here in particular should be noted: Most Web applications with payment function have two-dimensional barcode scanning capabilities, and will function as one of the means of payment. So these two-dimensional barcode Web applications secure? How to protect their safety, which is a topic worthy of attention.

In fact, news reports from some users often use the event to see the phone scan two-dimensional barcode has been fraud, liar. For example: "According to the Evening News report, because recently Ms. Chen Yongkang a stranger sent by scanning the two-dimensional barcode, cheated 5,000 yuan." Similar incidents had not poor, if you enter on Google. "Two-dimensional barcode fraud" as a keyword, it will search out approximately 4.39 million results, which shows a two-dimensional barcode scanning as a means of payment, this feature there is a huge security risk. In particular, March 13, 2014 the central bank issued a suspended two-dimensional barcode Alipay payment service, making two-dimensional barcode related Web application security issues become a remarkable problem.

With the growing popularity of smart phones, people demand the application of the mobile device for constantly rising, but how to design and develop mobile applications, mobile applications are using is safe, we will face what kind of security challenges? What are the security risks exist two-dimensional barcode scanning? How to design more secure Web applications? Below we conducted a preliminary analysis.

II. MOBILE APPLICATION DEVELOPMENT MODEL ANALYSIS

In the traditional sense, the application have defined as software running on the computer to help user perform a specific task. With the definition of smart phones applications has been extended to on smartphones and tablet computers run the software. Developing mobile applications for a variety of models, divided into body language and the web-based.

Body language usually refers to mobile devices supported languages, such as iOS system uses Objective-C, which is a variant of C++. Android system used by the body language is Java. Use body language development program run with high efficiency, speed and safety advantages. However, the difficulty of the development of relatively large, long development cycle, the development cost is relatively high. Especially Android system, due to the adaptation has some incompatibilities between multiple devices, different devices, therefore, the development and testing of the workload is very large, higher development cost.

As in [1] described, Web development approach is mainly used HTML5, the basic method development are: the use of HTML5 and CSS3 design language user interface, using JavaScript to achieve various functions. Because HTML5 is running on the browser, so you can be independent of the platform. Whether iOS device or Android device, as long as it's browser supports HTML5,
Web applications can work properly. This greatly save development costs. However beneficial to have disadvantages, the same HTML5 security issues can cause security problems of Web applications.

As a new generation of Web language, HTML5 applications with rich API, cross-platform, etc. is recognized as the future direction of web technology. However, no matter how powerful HTML5 have, it is always a description of the page markup language, it must perform its functions through the browser. HTML5 security will also affect the security of Web applications.

III. HTML5 SECURITY ANALYSIS

HTML5 is recognized as the next generation of Web language, which greatly enhance the Web's ability, especially in the rapid development of mobile terminals and mobile Internet background, HTML5 has been a profound change in the current application service model and the entire Internet ecosystem. As the most recent huge leap WEB standard, HTML5 standard has been IE, Chrome, Firefox, Safari, Opera and other major mainstream browsers support the rapid growth of the number of applications HTML5-based Web development prospects are generally all aspects of HTML5 good.

However, the new features of HTML5 Web application development in promoting, but also introduces new security issues, increasing the chances of an attacker to launch attacks, expanded the range of attacks, as well as the severity of the consequences. Early in August 2011, the European Union Network and Information Security Agency ENISA has published a security document analyzing HTML5, HTML5 specification announced the discovery of 13 of the 51 security issues, this is the first time an institution from a security point of view to the overall analysis of this specification. Since HTML5 standard start, its security mechanisms, frameworks and technologies are not yet mature, so as HTML5-based Internet applications and Web applications large-scale promotion, security issues will gradually expose and raises concern.

While HTML5 there are many security risks, but this article will focus on the client-side storage, cross-site scripting and other security issues.

A. Client Store Security Issues

In previous versions of HTML language, only allow Cookies store information as a local and relatively small allocation of space. Often only stored on the client's session ID and other simple little information, when users need to access the same data multiple times, you need to send a request to the server repeatedly obtain, therefore, greatly reducing the Web application access performance.

With Web applications increasing complexity and amount of data access performance has become an important bottleneck restricting the development. To this end, HTML5 introduced a LocalStorage, allows the browser to store large amounts of data at the client, and allows the use of new types of data. This adjustment, although greatly improved access performance, but at the expense of the expense of safety, and the resulting security risks are enormous. Under this mechanism, the sensitive data will be stored on the client, the attacker only needs a simple way to access the client or other damage by physical, you can easily get sensitive data. Cookies do instead of using LocalStorage authentication, Cookies have HTTPONLY protection, but LocalStorage without any protection mechanism, if a site XSS vulnerabilities exist, then the data is stored in localStorage where it can easily be acquired.

An attacker by entering the following code, you can get all the information using localstorage stored locally.

```javascript
var i = 0;
var str = "";
while (localStorage.key(i) != null)
{
    var key = localStorage.key(i);
    str += key + "=" + localStorage.getItem(key);
    i++;}
document.location="http://your-malicious-site.com?stolen=" + str;
```

B. Cross-site Scripting Attacks

Cross-site scripting (Cross-site scripting, commonly referred to as XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Such attacks often contain HTML5 and Javascript and other scripting languages.

Basic methods of attack: the use of Web applications and interactive text input window, enter a script contains malicious attacks, the malicious script masquerading as a link, when the information entered on the display window again, click on the link to other users it is possible to be attacked. In public interactive applications, such as WeChat, Alipay and other Web applications, it is vulnerable to this type of attack. Example: "June 28, 2011, Sina Weibo appear a relatively large XSS attacks." Specific methods of attack are: An attacker with a short connection issued a Sina url: http://weibo.com/pub/star/g/xyyyd”/>? type = update. When the user clicks on the url when the string Sina will be processed into a similar http://weibo.com/pub/star/ph p?g=xyyyd”/> ? type = update. Normal should return an error page, but because the application did not make...
adequate filtration parameters $g$, the parameter values are written directly to return to the page, resulting in the script is executed.

In fact, the realization of all Web attacks are needed to run some attack code on the user's own equipment, but the attacker used a variety of means to deceive, enabling users do not realize it. [2] lists many Web security testing tools and methods, such as a fan detection means closed the window of network attacks, however, the use of mobile phones to scan two-dimensional barcode, but for the network opens the door to the attacker. Many two-dimensional barcode scanning results of its scan Web applications without any safety testing, thereby producing a large number of security vulnerabilities, and has produced serious consequences.

IV. TWO-DIMENSIONAL BARCODE SECURITY VULNERABILITIES

The popular two-dimensional barcode is the QR Code, Japanese Denso Corporation in 1994 to the invention. Compared with the conventional one-dimensional barcodes, QR codes can store more data, and data type can be arbitrary binary data. QR Code was first track for auto parts, with the development of 3G mobile networks, mobile Internet gradually developed, but at the time the popular mobile phone is very difficult to enter the URL. Thus, the Japanese mobile phone companies started on a mobile phone with a camera added QR code reading software, thus reducing difficulties for user to enter the URL on the mobile phone. Later, using QR codes to store more and more popular in Japan URL magazines and advertising, by scanning the QR code on the Internet gradually called a popular application mode.

However, with the birth of the advent of the Apple iPhone mobile phone, as well as the subsequent Android operating system, smart phones gained rapid development, intelligent phone features also received a great deal of wealth. In this environment, two-dimensional barcode by scanning into the Internet and downloading software, although convenient for the majority of users, but also for criminals engaged in illegal activities to open the door.

As the literature [3] described, with the application and promotion of two-dimensional barcode technology, two-dimensional barcode has become the main channel on the mobile phone to the spread of the virus. Criminals two-dimensional barcode generated by the free tools and sites, the preparation of false information, phishing sites, mobile phone viruses site into a two-dimensional barcode, and published in a number of media and advertising, when consumers scan barcode via the phone, if you do not plus screening could become a victim of these attacks. Faced with this problem, how to solve? We can see from the two-dimensional barcode generation, reading these two directions to consider solutions.

First, we consider the two-dimensional barcode is generated. In theory, as long as the two-dimensional barcode generation software, you can generate a two-dimensional barcode that contains any information. Although the authorities proposed a "two-dimensional barcode registration management center was established to provide credible two-dimensional barcode of public services" and other measures, but in order to completely eliminate the use of two-dimensional barcode of cybercrime is unrealistic.

Secondly, from the aspect of two-dimensional barcode reader. Mobile phone softwares which QR codes can be read have reached a hundred variety. The software can be divided into two categories. The first is a simple two-dimensional barcode reader, use the URL obtained directly online or download software. Another is the two-dimensional barcode reader integrated into the software system, the two-dimensional barcode reader as an input means. For example: WeChat, Alipay.

For the first type of application which two-dimensional barcode reading software, I recommend adding a set up for two-dimensional barcode, display the content, allowing users to download software before directly to the Internet or have a chance to choose, although this does not completely solve the problem, but at least it can prevent some of the offenses occurred.

For the second type of application, the results of the two-dimensional barcode scanning can actually be seen as a text input. In order to prevent malicious attacks, scan results must be strict checks and filters, similar to prevent XSS vulnerability approach. However, due to the two-dimensional barcode information may be either included in the URL, it can be arbitrary text, so check the filter does not solve the problem. The biggest problem is: the face of a network address, we can only be addressed through a browser accessible way, but in the course of the visit, we may have suffered a cyber attack. In fact, in order to secure Web applications using two-dimensional barcode, the only way is to change currently using two-dimensional barcode storage web site application mode.

V. SECURE APPLICATION MODE OF TWO-DIMENSIONAL BARCODE

Change the use of two-dimensional barcode can better address the security issues of web applications. In many applications integrated two-dimensional code, such as WeChat, Alipay, two-dimensional barcode is mainly used to identify the different accounts or users, these accounts has a unique identification in the application system, is stored only if in the two-dimensional barcode uniquely identifies not include URLs in the application uniquely identifies converted to the corresponding Web site, so Web application security can be greatly improved. Below an
example to illustrate this new two-dimensional barcode application mode.

In the circulation of goods are goods barcode traceability of product in China has a huge demand. If we print a two-dimensional barcode on the product, the information it contains are: product barcode, date of production, goods unique serial number. Web applications through the two-dimensional barcode, we can build a simple traceability system.

The first step, using the Web application scanning the two-dimensional barcode that can be resolved by the two-dimensional barcode scan results: product barcode, date of production, a unique serial number; the second step, product barcode contains three messages: country, manufacturers number, product number; the third step, according to the manufacturer's serial number corresponding to the vendor's site; the fourth step, the product number, production date, a unique serial number as an argument to the manufacturer's website, query and traceability.

Such established web application security can be guaranteed. First, two-dimensional barcode that we use contains only a series of numbers, the results of the scan resolution is a very simple task, if the scan results do not meet our requirements, you can exit the system, thus guaranteed safety. Although our Web applications also need access to information through the network, but because the application site is our internal structure in the Web, which ensure that we will not have access to a dangerous site. In addition, such Web applications are not against a vendor established for all manufacturers, we can use, we only need to update Manufacturer ID and vendor URL correspondence table, you can expand the system.

VI. CONCLUSION

For Web applications including two-dimensional barcode scanning capabilities, both from the user's point of view and from a designer's point of view, it is vital to improve safety awareness, and only gradually abandon storage sites using two-dimensional barcodes of this application model, only then can the real improvement begin in the security of Web applications.

REFERENCES