Spamming the Internet of Things: A Possibility and its probable Solution

Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 10 (2012) 658 – 665

Procedia Computer Science

The 9th International Conference on Mobile Web Information Systems

Spamming the Internet of Things: A Possibility and its probable Solution

Faisal Razzak

Politecnico di Torino, Italy

Abstract

The Internet of Things (IoT) enabled users to bring physical objects into the sphere of cyber world. This was made possible by different tagging technologies like NFC, RFID and 2D barcode which allowed physical objects to be identified and referred over the Internet. Due to less complexity and low development and deployment cost of 2D barcodes, they have become modus operandi for building an IoT system. This paper explores the possibility of spamming the Internet of Things. It tries to establish that web spammers can use 2D barcodes to flood the physical side of the IoT, trick users to see or reach unsolicited and unrelated content over the Internet and possibly destroy the legitimacy of correct content. Preliminary results from an experiment establishing the possibility of the problem are outlined. This paper also proposes the use of digital signatures (ECDSA) to address the problem of spamming the IoT. A prototype implementation of the solution and its experimental results are given in this paper.

Keywords:
Spamming, Internet of Things, 2D barcodes, QR Code, Digital Signature, ECDSA, Spamming Solution, elliptic curves

1. Introduction

In our cyber lives, we all have encountered Spamming at some stage, ranging from getting uninvited emails to the mischievous alteration of web pages by Web spammers. The objective is to prey on unsuspecting users and undermining search engines by subverting search results to increase the visibility of some web pages and possibly have monetary benefits [1]. Formally, Spamming is the act of spreading unsolicited, anonymous and unrelated mass content [2] over the Internet. The emergence of Internet of Things (IoT) has provided an initiative to link our cyber lives with the physical ones by exploiting low-cost embedded tags, i.e., RFID, NFC, 2D barcode. Due to less complexity and low development and deployment cost of 2D barcodes, they have become the primary tool to create a linkage between physical objects and their cyber representations. The availability of smart phones having 2D barcode scanning facility has also provided the stimulus to this physical-cyber linkage. Plethora of applications exploiting the physical-cyber linkage have spawned in research [3, 4, 5] as well as in the real world. The basic principle governing the physical-cyber linkage is the ability to encode public data into a 2D barcode and place it on a physical object or space which

Email address: faisal.razzak@polito.it (Faisal Razzak)

1877-0509
doi:10.1016/j.procs.2012.06.084

Fig. 1. Example 2D barcode (Website referral) in a public space

can easily be decoded by ordinary mobile phone users. Since the encoded data in 2D barcodes is always public and the generation of new 2D barcodes is cheap and easy, it can make the physical side of the IoT an easy target to spam for less scrupulous people.

This paper is a preliminary work exploring the possibility of Spamming the Internet of Things and putting forwards a probable solution to address the problem. It tries to establish that Spammers can use 2D barcodes to flood the physical side of the IoT and mislead users to reach unsolicited and unrelated content over the Internet (increasing traffic for certain pages). Thus, possibly destroying the legitimacy of correct content. Preliminary results from an experiment which establishes the possibility of the problem are outlined. Moreover, a possible solution to the problem is also defined along with its implementation details and experimental results.

The paper is divided into five sections. Section 2 defines the problem addressed in this paper, the result of the preliminary experiment to see the possibility of such a problem and outlines some scenarios where the problem might exist. Section 3 put forward a probable solution for the problem defined in the paper and explains developed applications implementing the probable solution. Section 4 discusses approaches already existing in the literature and Section 5 concludes the paper.

2. Problem: Spamming the Internet of Things (IoT): A possibility

The main driving factors behind spamming are monetary benefits, religious or political agendas [1], attempting to convince people into buying some products online or generating more online traffic for certain pages etc. So, the question is that where exactly the Internet of Things fits in this picture?

As explained earlier, Internet of Things works on the physical-cyber linkage. In physical space, 2D barcodes are placed on objects or places to point toward resources over the Internet. Spamming in the Internet of Things means - creating new 2D barcodes or modifying legitimate 2D barcodes pointing towards unrelated content over the Internet and flooding physical space with them to increase traffic for certain web pages. Public spaces like tourist spots, train stations, movie theaters, transportation system are the most vulnerable to such form of spamming but semi-private spaces like universities, offices or industries can also become victims of this form of spamming.

The following section outlines possible techniques to spam and example domains that may become victim of spamming.

2.1. Public Spaces and Website Referrals

Using a 2D barcode to refer towards resource on the Internet has become the modus operandi. The companies providing services on the Internet create 2D barcodes which point towards their online services. These barcodes are then distributed across different physical spaces enabling users with the mobile to access online services ubiquitously. Such 2D barcodes and physical spaces are the most vulnerable to spamming pointing to unsolicited content over the Internet.

Consider a public transportation company which places 2D barcodes at different bus terminal (refer to Figure 1) pointing to its online services. These services provides the timing of bus arrival, departure,

or information about different routes[1]. The user could decode the 2D barcode to access the company's online services. It represents a typical Internet of Things scenario where the 2D barcode placed at different terminals represent the physical side of company's system and online services represent the cyber side of the company's system.

The spammer could utilize following two methods to spam such environments.

2.1.1. Mass Flooding

Mass Flooding deals with flooding the physical side of an IoT system with many 2D barcodes making it difficult for users to determine which 2D barcode points to a service that the users are looking for. In above defined scenario, the spammers could easily generate numerous website referrals pointed towards unintended content over the Internet and place them in such public spaces (bus terminal). Since the location will have multiple 2D barcodes, the user especially tourists might easily be confused and start decoding 2D barcodes placed in the location to search for a legitimate service over the Internet. Since the terminal has multiple 2D barcodes, the chances of user being exposed to unrelated content increases. Moreover, it also undermines the credibility of the company as it hinders the services provided by the company. Therefore, on one hand the mass flooding of such environments could easily destroy the reputation of legitimate websites and will generate additional traffic for spammer's link.

2.1.2. Redirection Hiding technique

Given a spammer knows the content (URL) of a legitimate 2D barcode placed by the company, the spammer could easily generate a corresponding 2D barcode which points towards a spammer web page. The spammer's web page employs re-direction hiding technique to eventually route the user to the correct content of the legitimate 2D barcode. It is referred as *Redirection hiding technique* [1] in this paper. For example, imagine a legitimate 2D barcode at a public location pointing to a legitimate web address (http://correctAddress.com). The spammers could easily decode this address, create a 2D barcode that points to the web address (http://spammerAddress.com) and replaces it on the environment. On the Internet, the web address (http://spammerAddress.com) uses the redirection mechanism (either using meta-tags or javascript) to eventually point to (http://correctAddress.com). When the user decodes this spammer's 2D barcode, the user is eventually re-routed to correct address but not before visiting the spammer's web address. This technique may easily be employed in public spaces as compared to semi-private or private spaces. The main feature of this technique is that in fact, the spammer does not need to mass flood the environment. Placing a silent tag like this will eventually enable spammer websites to have more hits over time. The experiment conducted to establish the possibility of Spamming the Internet of Things in this paper, employs this technique.

2.2. Business/Contact Cards

Business cards carries information about an individual or a company. They are shared during formal introductions as a convenience and a memory aid. Encoding Business cards with 2D barcodes (especially QR code) has picked pace in recent years and number of online services are available[2], offering people easy and innovative ways to embed 2D barcodes with their business cards. Figure 2 shows an example of such a business card. Such cards can become an easy target for spammers to copy and distribute them with modified embedded 2D barcodes. Figure 3 shows an example of a business card that points to a modified QR code. For an unacquainted user it will be very difficult to differentiate between a valid and an invalid business card. Both spamming techniques (Section 2.1.1 and Section 2.1.2) can be employed for business cards.

[1]The scenario is not imaginary. Many transportation companies across Europe are in fact placing bar codes at different bus terminals to point towards their legitimate websites for more information. For example, GTT (GRUPPO TORINESE TRASPORTI) in Torino, Italy does employ this method and uses QR code to encode information in order to assist users

[2]http://businesscards.tec-it.com,

Fig. 2. Correct Version.

Fig. 3. Spammed Version.

Record	Spammer Link	Real Link	Spammer Hits	Real Hits
1	/site/elitefaizal	/site/elitefaisal	20	48
2	/site/referralS	Not Given	19	unknown
3	/site/referralA	Not Given	32	unknown
4	/site/referralU	Not Given	26	unknown

Table 1. Experimental statistics for establishing the possibility of spamming the Internet of Things.

2.3. Preliminary Experiment

To establish the possibility of spamming the IoT, an experiment has been conducted. The experiment does not intend to capture the effects of such form of spamming on the overall system but the focus is to establish the possibility of spamming the IoT. Table 1 shows preliminary results of the experiment which has been carried out. The spamming technique employed for the experiment is redirection hiding technique (Section 2.1.2). "Spammer Link" points to the spammer's web page containing unrelated and unsolicited content. For the experiment, the spammer web pages only have hit counters, counting the number of online hits received. "Real Link" refers to legitimate websites that actually host any service that the user is interested in. "Spammer Hits" and "Real Hits" contains the number of hits received by the *Spammer Link* and *Real Link* respectively. QR Code is chosen to encode spammer and real links. QR code or Quick Response code is a 2D matrix bar code, created by the Japanese corporation Denso-Wave in 1994. It has been chosen because they were developed by keeping in mind a quick decoding process and many modern mobile phones are by default equipped with software to decode information in QR codes[3]. The experiment was carried out for six days and five 2D barcodes were placed for each spammer and real link at different locations. On the first day, QR codes pointing to real links were placed at different locations. The next day, some of the QR codes were replaced with QR codes pointing to spammer's link.

For record number 2,3 and 4 the Real Link was supposed to point to real world websites. Therefore, their actual addresses have not been provided and their total number of online hits are not known. However, their corresponding spammer link hits are documented. For record 1, a web page is created acting as a real link. The real web page has an embedded hit counter, counting the number of total hits received.

2.3.1. Discussion

From Table 1, it is evident that the web spammer can create or modify QR codes to mislead users to open unrelated content over the Internet. The "Spammer Hits" column points to this fact. Another interesting fact is by placing only 5 QR codes, such number of hits were observed. In future, the author intends to observe effects of controlled mass flooding techniques.

To avoid such form of spamming, we require a technique which could ensure us to track the identity of QR code creator (the content creator) so that people trying to trick users into viewing some unrelated content can be identified. Moreover, the technique should allow legitimate content owners to create QR codes for which the integrity of the original message can be kept. In author's view, the problem defined in this Section can be avoided by technique(s) ensuring both the integrity of the original content and the authenticity of the content creator.

[3]From this point, QR code are used to refer to 2D barcodes and vice versa.

3. A Probable Solution

In order to ensure the integrity of the content and establish the identity of the content creator (to address the problem defined in Section 2) the author proposes the use of Digital Signatures [6, 7] to digitally sign the content inside 2D barcodes. The science of digitally signing the content to ensure the integrity of the message and the identity of the content creator (Digital Signatures) has been well studied in the field of cryptography and it naturally makes sense to use existing tools and technologies to address a problem. A digital signature or digital signature scheme demonstrates the authenticity of a digital content. It helps ensure authentication of the user and integrity of the content. Embedding digital signature inside the 2D barcode will naturally ensure integrity of the content[4] as well as will help identify the correct identity of content creator.

To help embed and verify digital signatures in QR code two important elements are needed, i.e., a digitally signed QR Code Generator and an application to verify the signed QR code.

Figure 4 shows the basic elements of the proposed solution and their interaction. Firstly, a QR Code generator is needed that can digitally sign the content and encode it in the QR code. It takes the content, the public-private key pair (public-key cryptography) and certificate information and generates a digitally signed QR code and relevant certificates. The modified QR code is embedded with three pieces of information, i.e., original content/message (C), digitally signed content (DS) and the public key (PK) of the content creator. Considering the content is a website referral, the certificates verifying the identity of the creator are placed at the URL. The second element is a mobile application that scans the QR code and has the ability to check the integrity QR code content and validate the certificate chain.

The interaction among different elements of the proposed solution is explained below:

1. Given a content and the identity of the content creator (public-private key pair and certificate), the "QR Code generator" generates a QR code embedded with the original content (C), its digitally signed version (DS) and the public key of the content creator.
2. This step is optional. If the content creator does not have certificates verifying the identity of the content creator, the "QR Code generator" generates self-certified certificates encoding the identity of the content creator.
3. Given the content is a website referral, the certificates are places at the URL referred by the the content(C).
4. The "mobile application" decodes the QR code to extract the original content (C), the digitally signed version (DS) and the public key of the creator (PK).
5. The "mobile application" ensures the integrity of the QR code by verifying the content and comparing it against the digitally signed content (DS) using the content creator's public key.
6. The "mobile application" verifies the certificate/ certificate chain and ensures that the root certificate is entrusted by the user of the mobile application.
7. The referred website is opened.

3.1. Developed Applications and their Testing

The author implemented different elements of the solution to evaluate the feasibility of the proposed solution. The 2D barcode chosen for generation is the Quick Response code (QR code). A "QR code generator" application is implemented in Java. It uses the ZXing library[5] to generate QR Codes. ZXing (pronounced "zebra crossing") is an open-source, multi-format 1D/2D barcode image processing library implemented in Java, with ports to other languages. Since NIST [6] recommends the use of elliptic curves for encryption and digital signatures for future applications, the developed "QR code generator" uses elliptic curve (EC) based public-private key pair for signing the content. Elliptic curves based cryptography and

[4] In this paper, the content refers to a website referral like http://www.bing.com

[5] http://code.google.com/p/zxing

[6] http://csrc.nist.gov/groups/ST/toolkit/digital_signatures.html

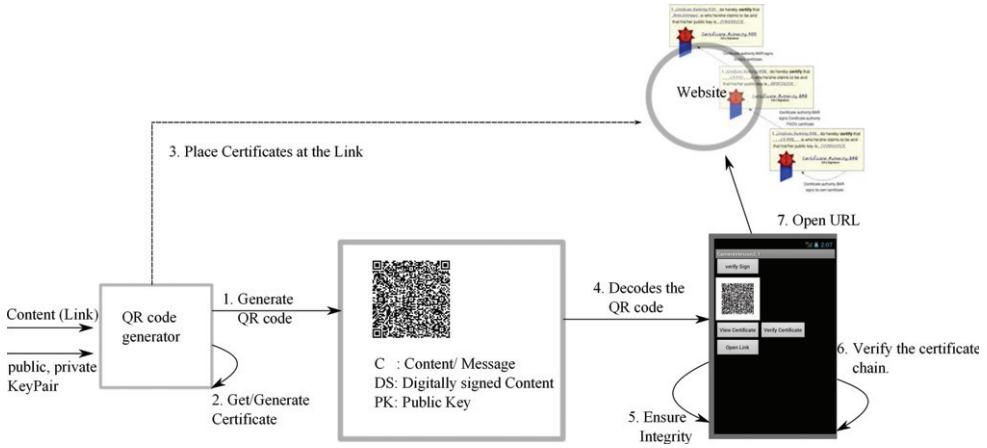

Fig. 4. Elements and their interaction inside the proposed solution

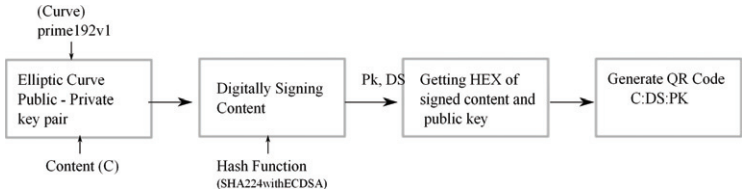

Fig. 5. QR code generator steps

digital signatures are increasingly being used by organizations to encrypt and digitally sign data because it uses smaller key lengths than those of the older schemes (RSA, DSA) to achieve same security level. It forms the basis for the next cryptographic standard for U.S. government use, known as Suite B [7].

Given the content, the "QR code generator" uses Elliptic Curve private-public key pair to digitally sign the content and (if needed) create certificates. Conceptually, the Elliptic Curve Digital Signature Algorithm (ECDSA) [8] is utilized and practically Bouncy castle Java Security provider[8] is used to generate public-private key pair on Elliptic curves and sign the content digitally. However, both the digitally signed content and the public key are converted into their hex-decimal representations and then embedded in the QR code. The steps are depicted in Figure 5.

The mobile application to verify the integrity of the QR code and the identity of the content creator is developed on the Android platform[9]. It gives the user an ability to decode a QR code by using a barcode scanner. After getting the decoded message of the QR code, the application provides users the ability to verify the integrity of the content, ensure the authenticity of the content creator and option to open URL in

[7] http://www.nsa.gov/ia/programs/suiteb_cryptography
[8] http://www.bouncycastle.org
[9] http://www.android.com

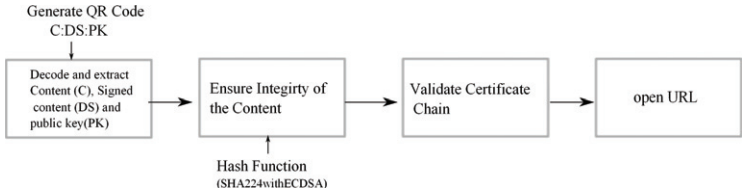

Fig. 6. Verification steps of the generated QR code

Elliptic Curve	Curve (Bits)	cryptographic hash functions	Dimensions of QR code	Message Size (byte)	Verify Time (seconds)
prime192v1	192	SHA224withECDSA	256 x 256	296	2.46
prime239v1	239	SHA224withECDSA	256 x 256	342	3.31
prime256v1	256	SHA224withECDSA	256 x 256	360	3.36
P-224	224	SHA224withECDSA	256 x 256	322	3.21
P-256	256	SHA224withECDSA	256 x 256	361	3.29
P-384	384	SHA384withECDSA	512 x 512	482	7.3
P-521	521	SHA512withECDSA	512 x 512	629	9.0

Table 2. Experimental statistics of the solution.

the browser. The steps are depicted in Figure 6.

3.2. Experiment

To assess the generation and verification of digitally signed QR codes, an experiment has been performed which uses different elliptic curves to generate public and private keys and cryptographic hash function for content signing. In future, it will help provide observations outlining different possibilities, give some initial recommendations for readers (if they intend to use it) and observe any weakness (if any) in the proposed solution.

Seven iterations were performed in the experiment (Table 2). In each iteration, a different elliptic curve was used to generate the public and the private keys (*Elliptic curve and curve (bits)*) and a different cryptographic hash function was chosen (*cryptographic hash function*). The *Dimensions* show dimensions of the generated QR code. The *Message Size* column shows the size of the generated QR code in bytes and it was averaged for 50 QR codes. The *verify time* shows the average time taken by the mobile application to successfully decode the QR code and verify the integrity of the message. It is averaged over 50 QR codes for each iteration.

The time taken to authenticate the identity of the content creator (certificate chain) is not shown in Table 2 because it mainly depends upon the length of certificate chain and is not the focus of this paper. The time will vary depending upon the certificate chain length, and will be in addition to the time taken to verify the integrity of the QR code.

3.3. Discussion

Table 2 outlines the results obtained by performing the experiment using the developed applications. It proves the feasibility of the solution and the solution's implementation. However from the results following points are observed.

1. From Table 2, it is evident that the mobile application takes time in seconds to verify the integrity of the content. To establish the identity of the content creator will take additional time (validate the certificate chain). Therefore for higher curves, robustness of the solution needs to be improved.
2. The content assumed in the solution is a website referral and therefore certificates are assumed to be placed on the website. But for cases where the content refers to other than website, the placement of certificates ensuring the identity of the content creator is not clear. A possible solution might be to encode the QR code with the web address where the certificates are located.

4. Literature Review

This paper has preliminarily explored the possibility of Spamming the Internet of Things and proposed a probable solution of using Digital Signatures to address the problem. The literature on the identification of the problem (Spamming the IoT) and possible techniques is rare but the use of digital signature in signing documents and 2D barcode is not new and has been employed by many researchers to address separate problems in literature.

Katsunori Seino et al. [9] proposed a system to identify a fishery product by giving it a unique serial ID (generated by a server) printed in to 2D QR code and attached to the product. The main focus of the paper was to generate a unique product-identification and encrypt it using public-key encryption method. Since encoding the product-identification into QR code makes duplication easy, therefore to maintain the integrity the use of digital signature is recommended. However, the paper does not outlines the steps to digitally signed the QR code and the placement of certificates. The current paper addresses a different problem and describes in details the process and different components of making Digital signatures work in QR code.

Yung-Wei Kao et al. [10] proposed an efficient and safe authentication procedure for access control system by using common equipments, i.e., mobile phone and QR code. It generates a secret by using OTP (One Time Password) technique and stores that secret into a QR code. The paper did outline the architecture but the details of the overall approach and its implementation seems to be missing. The issue of the integrity of the information encoded in QR code and the authenticity of the QR code has not been addressed.

In order to bind an electronic document with its printed version, a printable digital signature scheme derived from the Korean Certificate-based Digital Signature Algorithm (KCDSA) for secure transaction was proposed in [11]. It utilizes the QR code for printing out the signature in a small area within a printed document. The details of the procedure are outlined in [12]. The QR code acts as a digital signature for the printed document, but in the domain of Internet of Things (IoT), the QR code acts as the main carrier of information and provides a linkage from physical to cyber world. In short, the current paper outlines in detail the implementation and the experimentation carried out for the IoT domain.

5. Conclusion

This paper discusses and establishes the possibility of spamming the IoT and proposes a probable solution. Results from the preliminary experiment establishing the possibility of spamming the IoT are also presented. This paper also proposes the use of digital signatures to address the problem of spamming the IoT. The implementation of the solution and its experimental results are given in this paper.

References

[1] Z. Gyongyi, H. Garcia-Molina, Spam: it's not just for Inboxes anymore, Computer 38 (10) (2005) 28 – 34.
[2] P. Hayati, V. Potdar, A. Talevski, N. Firoozeh, S. Sarenche, E. Yeganeh, Definition of Spam 2.0: New spamming boom, in: Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on, IEEE, 2010, pp. 580–584.
[3] F. Razzak, D. Bonino, F. Corno, Mobile interaction with smart environments through linked data, in: Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on, IEEE, 2010, pp. 2922–2929.
[4] J. Gao, L. Prakash, R. Jagatesan, Understanding 2d-barcode technology and applications in m-commerce-design and implementation of a 2d barcode processing solution, in: Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International, Vol. 2, IEEE, 2007, pp. 49–56.
[5] T. Liu, T. Tan, Y. Chu, 2d barcode and augmented reality supported english learning system, in: Computer and Information Science, 2007. ICIS 2007. 6th IEEE/ACIS International Conference on, Ieee, 2007, pp. 5–10.
[6] W. Diffie, M. Hellman, New directions in cryptography, Information Theory, IEEE Transactions on 22 (6) (1976) 644–654.
[7] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key crypto systems, Communications of the ACM 21 (2) (1978) 120–126.
[8] D. Johnson, A. Menezes, S. Vanstone, The elliptic curve digital signature algorithm (ECDSA), International Journal of Information Security 1 (1) (2001) 36–63.
[9] K. Seine, S. Kuwabara, S. Mikami, Y. Takahashi, M. Yoshikawa, H. Narumi, K. Koganezaki, T. Wakabayashi, A. Nagano, Development of the traceability system which secures the safety of fishery products using the QR code and a digital signature, in: OCEANS'04. MTTS/IEEE TECHNO-OCEAN'04, Vol. 1, IEEE, 2004, pp. 476–481.
[10] Y. Kao, G. Luo, H. Lin, Y. Huang, S. Yuan, Physical access control based on QR code, in: Cyber-Enabled Distributed Computing and Knowledge Discovery, 2011 International Conference on, IEEE, 2011, pp. 285–288.
[11] J. Lee, T. Kwon, S. Song, J. Song, A model for embedding and authorizing digital signatures in printed documents, Information Security and CryptologyICISC 2002 (2003) 465–477.
[12] C. Teoh, Two-dimensional barcodes for hardcopy document integrity verification (2008).
URL http://eprints.utm.my/9467