Phishing detection model using the hybrid approach to data protection in industrial control system

To cite this article: E A Mityukov *et al* 2019 *IOP Conf. Ser.: Mater. Sci. Eng.* **537** 052014

IOP Conf. Series: Materials Science and Engineering **537** (2019) 052014 doi:10.1088/1757-899X/537/5/052014

Phishing detection model using the hybrid approach to data protection in industrial control system

E A Mityukov, A V Zatonsky, P V Plekhov and N V Bilfeld

Perm National Research Polytechnic University, 29, Komsomol ave., Perm, 614990, Russian Federation

E-mail: zxenon@narod.ru

Abstract. Phishing is the procedure of tampering with sites, login and password forms, emails and so forth which simulate a legitimate analogy using methods and means of social engineering to deceive the victim in order to obtain his or her confidential information. We have conducted a statistical analysis of unique phishing attacks and the attacked areas. Today, there is an increase in attacks aimed at the manufacturing sector, in particular at industrial control systems (ICS). This area is the least protected today from external threats, including phishing. Taking this fact into account, we have investigated the features of an ICS in terms of possible phishing attacks. A comparative analysis of existing methods of protection against phishing, which are potentially applicable to ICSs, has been carried out. We have developed a method of combating phishing, consisting of 3 main modules: the module of obtaining the URL of the visited webpage, the filtering module based on white-list, the login form search module. The experiments resulted in true positive rate equal to 90.41%, false positive rate equal to 7.24%, precision and f1-measure being equal to 95.17% and 92.72%, respectively.

1. Introduction

Phishing is a threat to cybersecurity that can be implemented by various methods of social engineering to fraudulently obtain the Internet users' confidential information. Today, detection and prevention of phishing attacks is a serious and complex task, as attackers are using increasingly sophisticated approaches, so the existing methods of combating phishing require improvement.

Kaspersky Lab ICS CERT published statistics (figure 1) from October 2017 to June 2018. It is evident that phishing emails with malicious attachments are actively sent to large industrial companies [1]. The peak of the attacks was in May 2018, when 265 companies were attacked in Russia. The industrial sector is becoming a priority target for fraudsters [1, 10], industrial control system (ICS) users are also attacked.

A lot of anti-phishing techniques have been designed [9], but no any "open-the-box" solution that can guarantee full protection [8]. However, properly applied security technologies along with user training significantly reduce the risk of the theft of confidential information [2], 3].

The purpose of this research is to develop the system for protection of ICS against phishing attacks. We suggest a hybrid approach adapted specifically for ICS. The first module of ICS protection receives the URL requested by the user, the second and the third modules for legitimacy check act as primary and secondary filters. They decrease false positives (FP) and improve performance by excluding already checked pages or that without registration forms. The availability and validity of records older than 30 days are also periodically checked.

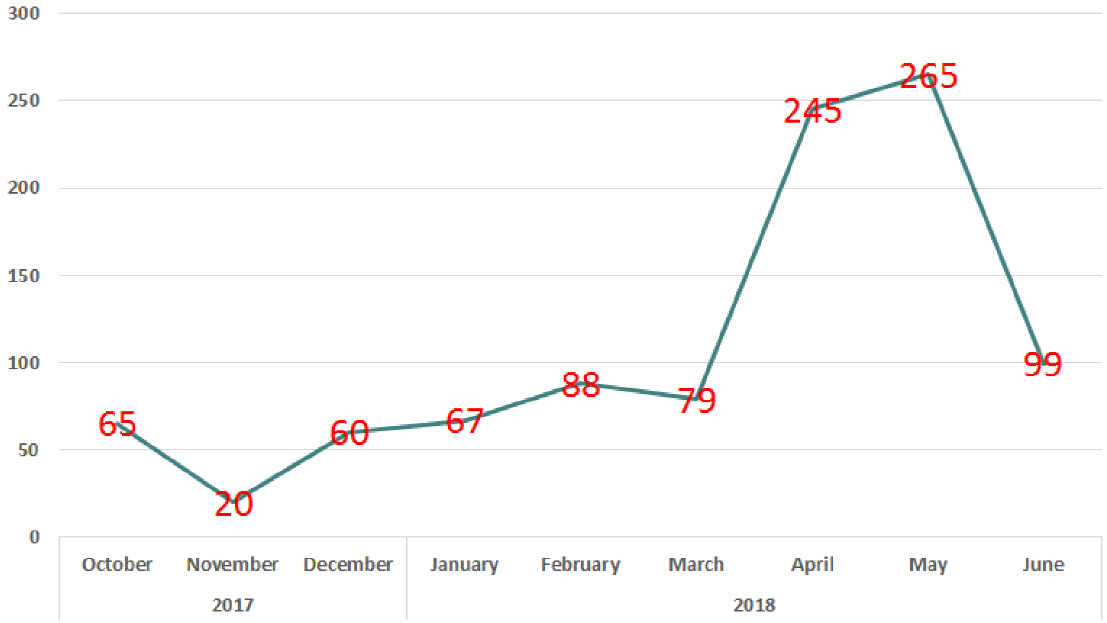

Figure 1. The number of companies attacked by intruders from October 2017 to June 2018.

2. Literature review

In recent years, more and more research has focused on the solution to the phishing problem. Kang and Lee (2007) proposed a general approach based on white-lists [7]. The approach denies access to explicit phishing sites by mapping the IP address to a domain name. When a user visits any website, his URL and the IP-address of the website are transferred to Access Enforcement Facility (AEF), to verify the legitimacy of the site. If the URL passed to AEF matches the entry in the white-list, then the analogy of the IP address to that of the entry is checked. If the address also matches, the site is legitimate; otherwise, the site is considered as phishing. In our approach, we use the white-list as a secondary filtering module, which, along with a bundle of IP-address and domain name, also contains the time of the resource visit.

Han et al. (2012) considered a method of "automated individual white-lists" (AIWL) [4]. According to this approach, users independently maintain their own white-list, which contains known legitimate websites visited by the users. Application of this approach significantly increases the speed of white-list scanning, as the lists are stored locally for each user. They also contain functions of web pages, such as URL of the widgets on the page, etc. In this case, the bottleneck is the local storage of the list as, if the list is compromised, the user becomes vulnerable. This problem can be solved in two ways: 1) list encryption; 2) remote server storage. We decided to use a similar but more secure approach as, for any ICS, it is important to eliminate process downtime which can occur as a result of any phishing attacks. We create a list for each user, which is stored separately on the server.

As a result of phishing page studies, Jain and Gupta (2016) proposed a model which uses an auto-updatable white-list of legitimate sites and notifications for users in case the URL is not in the white-list [5]. The validity of a web page was checked on the basis of two components: 1) matching the domain name and its IP address; 2) examining the features of hyperlinks from the source code. The key point was that the site was automatically added to the white-list as a result of the checks. Since attackers often create new sites and domain names, it is necessary to keep even white-lists up to date. We add a resource to the white-list in case of passing all checks, but after 30 days since the date of adding, we check the resource again. If the domain name is unavailable or missing, and the name is available for registration, the resource is excluded from the white-list, otherwise the date of the visit to the website is updated.

Zhang et al. (2007) proposed an approach based on CANTINA functions, which uses the TF-IDF (term frequency and inverse document frequency) algorithm to determine keywords and tags from the web page content [6]. The words found are checked using Google search engine. If the information from the examined page is found in the resulting pages of search queries, the page is considered legitimate. As a result of the CANTINA method development, Xiang et al. (2011) created a new version of CANTINA+. We use an algorithm taken from CANTINA+ to search for login forms. The algorithm is adapted to the keywords of the login search forms, which are most common among ICS users.

3. System architecture

The main purpose of this system is to identify threats and notify information security officers when ICS users visit phishing sites. The architecture of the system and its filtering modules is shown in figure 2.

First, you need to get the URL of the visited webpage using a full-fledged deep packet inspection solution (DPI-solution), which is the first module of the system. After that, the second module checks if the site is in the white-list, which is automatically updated, and the third module checks if the page can potentially retrieve sensitive user data. If the web page is not in the white-list and has a login form, the URL is legitimate. Otherwise based on the results of each module, the security officer decides if it is necessary to intervene in the workflow. If necessary, it is possible to manually block user's access to the Internet, using the DPI-solution mechanisms.

Automatic blocking is not provided. This is due to the peculiarity of the technological process, as it can affect the ICS operation as a whole (for example, the transmission of technological data over the Internet can be interrupted).

The filtering module based on a white-list is a personal white-list that contains legitimate websites. It includes the web page URL, the IP address of the host where the web page is located, date of the visit. Before the whitelist is updated with a new record, the IP-address is checked. The IP address is compared by nslookup via a local DNS server, then using remote root DNS servers (1.1.1.1 and so on) to verify legitimacy. If the addresses match, the record can be added to the white-list. This approach protects the list from “dns poisoning” attacks.

When a user attempts to visit a website, the white-list based filtering module checks whether the current URL and the IP address of the website are in the white-list. If so, the website is considered to be legitimate. Otherwise, it is unknown. The URL is then redirected to the next module for further verification.

This module also checks the availability of the resource after 30 days from the date it was added. If the site is accessible and the IP address matches the URL, the date is updated. If the site is unavailable, the entry is removed from the list. When the site is available but the IP address has changed, the URL is sent to pass all checks again. The filtering module improves system performance and accelerates the resource scanning speed, as personal white-lists, which constantly contain relevant records and are automatically updated, are used.

Filtering module based on login form search module. At present, the sites use user registration and authentication systems to ensure users' identity. Attackers usually attempt to steal the registration data of users with a bogus login form. We have developed a module to check the page for the presence of at least one login form. If there are no registration/authentication forms, the resource is considered to be legitimate, since the users do not enter their data anywhere. It improves system performance with respect to resources that do not have any registration forms. For implementation, we used an algorithm for checking the presence of the login form from CANTINA + (2011).

We used 20 keywords for entrance (for example: login, password, email and etc.). These keywords are used to determine the type of the page to be checked. The algorithm for determining the form is in the table 1.

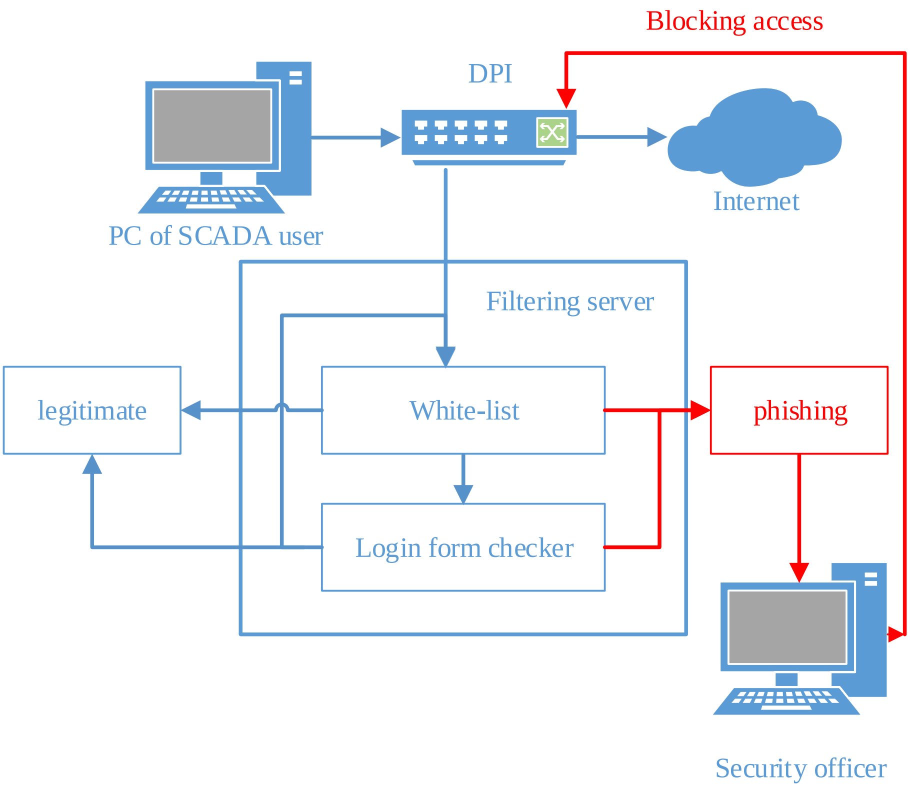

Figure 2. System architecture.

Table 1. Algorithm for determining the form

```
Input: HTML of the web-page;
a. Check the current page for the form tags and input tags availability, if they exist, then:
b. Search for keyword in tags form to check if it is a search page, if they exist, continue step “b”, if not, move into the next step “c”.
c. Search for keyword «login» in tags form to check if it is a login form. If it is, return the result «1», if not, move into the step “d”.
d. Follow the URL on the page to the depth of «2», search for keywords on those pages. If the words are found, return the result «1», if not, move into the step “e”.
e. Search for images on the page and their size, if they exist, return the result «1», if not, move into the step 1.1 for the next form. If no page with a login form found, move into the step “i".
f. Check the current page only for the input tags availability, if they exist, then:
g. Search for keyword «login», search for login words to login the domain tree. If they exist, return the result «1», if not, move into the step “h”.
h. If there are images to login the domain tree, return the result «1», if not, return the result «0».
i. If the page has no form tags and input tags, return the result «0».
Output: (1: login form exists; 0: login form does not exist).
```

4. Results and discussion

To assess the performance of the system in the experiment, we took the following two metrics: true positive rate (TPR) and false positive rate (FPR). Also we used standard measures such as accuracy and F1-measure.

The TPR is calculated by the ratio of the identified phishing pages to the total number of phishing sites that should have been identified (1):

$$TPR = \frac{TP}{P} = \frac{TP}{(TP + FN)} \tag{1}$$

TP is the quantity of correctly classified phishing pages; *P* is the quantity of phishing pages equal to the sum of correctly classified pages (TP) and missed phishing pages (FN).

False Positive Rate (FPR) is the percentage of phishing sites that are classified as legitimate ones of the total number of phishing websites. (2):

$$FPR = \frac{FP}{L} = \frac{FP}{(FP + TN)} \tag{2}$$

where *FP* is the number of legitimate web pages which are incorrectly classified as phishing, *L* is the total number of appropriate pages.

Precision (PR) is a relation between the number of actual phishing web pages and the total number of web pages identified as phishing ones (3):

$$PR = \frac{TP}{(TP + FP)} \tag{3}$$

F1-measure is the average between *PR* and *TPR*, as shown in formula (4):

$$F1 = 2 \cdot \frac{PR \cdot TPR}{(PR + TPR)} \tag{4}$$

We conducted two experiments to assess the effectiveness of the approach proposed. In each experiment, we used the same set of data obtained from public sources. As a result, we had 1439 phishing sites and 911 legitimate ones. Initially, the adequacy only of the white-list based filtering module was evaluated. We got TPR equal to 87.42%, FPR was equal to 8.34%, while F1 and Precision were 94.30% and 90.73% respectively. Obviously, these values are not enough to effectively identify phishing sites. In the second experiment, we tested the efficiency of the whole system. We managed to increase TPR by 2.99% and reduce FPR by 1.1%. Precision and F1-measure of the second experiment allowed us to estimate the overall performance of the system. We got Precision equal to 95.17% and F1-measure equal to 92.72%.

5. Conclusion

In this paper, we propose an effective method against phishing in ICSs, which is based on DPI solution, the white-list based filtering module, and the login form search module. The general architecture of the system has been developed. We have modified 4 existing methods and adapted them to the features of the ICS. Then we conducted a practical study of the developed approach in two variants. As a result, we got TPR equal to 87.42% and FPR equal to 8.34%, using only the whitelist based module. Application of two modules allowed us to increase TPR by 2.99% and FPR by 1.1%. Further work will include the development of additional heuristics methods to improve the accuracy of phishing detection.

References

[1] Paganini P 2018 *Industrial Sector targeted in surgical spear-phishing attacks* Available from: https://securityaffairs.co/wordpress/75033/hacking/industrial-sector-spear-phishing.html

[2] Romansky R A 2017 Survey on Digital World Opportunities and Challenges for User's Privacy *International Journal on Information Technologies and Security* **9(4)** 103-14

[3] Yoana A I 2018 Assessment of the Probability of Cyberattacks on Transport Management Systems *International Journal on Information Technologies and Security* **10(4)** 99-100

[4] Cao Y, Han W and Le Y 2008 Anti-phishing based on automated individual white-list *Proceedings of the 4th ACM Workshop on Digital Identity Management* (New York, USA:

ACM) pp 51–60

[5] Tewari A, Jain A K and Gupta B B 2016 Recent survey of various defense mechanisms against phishing attacks *Information Privacy and Security* **12(1)** 3–13

[6] Zhang Y, Hong J and Cranor L 2007 CANTINA: a content-based approach to detecting phishing websites *16th International World Wide Web Conference* (Banff, Alberta, Canada) pp 639-48

[7] Kang J and Lee D 2007 Advanced white list approach for preventing access to phishing sitesn *Convergence Information Technology International Conference* pp 491–6 doi:http://dx.doi.org/10.1109/ICCIT.2007.50

[8] Zatonsky A V 2013 *Software of global optimization of automatic control systems* (Moscow) pp 4-16

[9] Mityukov E A 2018 Phishing in Industrial control system *Decision* 171-4

[10] Mityukov E A 2018 The practice of using reverse-proxy to protect corporate applications on the Internet *Automated Control Systems and Information Technologies* 288-92