

A Design of Access Control Model for Information Leak Detection based on Inference in Smart Device

Junho, Choi¹, Chang Choi², Htet Myet Lynn², Byeongkyu Ko², Ilsun You³, and Pankoo Kim^{2*}

¹Division of Undeclared Majors, Chosun University

Gwangju, South Korea

xdman@chosun.ac.kr

²Department of Computer Engineering, Chosun University

Gwangju, South Korea

{enduranceaura, htetmyet, byeongkyu.ko}@gmail.com, pkkim@chosun.ac.kr

³School of Information Science, Korean Bible University

Seoul, South Korea

isyou@bible.ac.kr

Abstract

The rapidly growing number of users in the smartphone market has increased the variety of emerging issues. In particular, smartphones store user private information, thus highly needing security techniques because losing data and malicious code may lead to significant monetary damages or loss. In this paper, we propose an intelligent access control model based on ontology inference, which prevents personal information leakage in Android platform with dynamic security level access. The proposed model analyzes the permission by category of application services and detects new malwares through context ontology inference of API resource information and permission. It is shown that the proposed model achieves both more precise and practical malware detection.

Keywords: Android Security, Access control model, Information leakage detection, Ontology Inference

1 Introduction

The Android platform is an open and free software stack of Google that includes an operating system, middleware and also key applications for use on mobile devices including smartphones[7]. Android OS is released by Google under open source licenses, although most Android devices ultimately ship with a combination of open source and proprietary software[2]. In 2013, Android grew to a very large number: 87% of its share of the global smartphone market. It also grew to an even larger one: 97% of Android's share of global mobile malware[1].

The personal information is stored on a smartphone. Clearly, user information can be leaked when a user launches an application, which contains malicious code with damages. Therefore, there is a high need for a method, which can detect and control access to a user's personal data in a smart device. Typical approaches to tackle this challenge include signature detection, virtualization in mobile devices, mobile cloud service, and so on. Recently, there has been considerable attention to the context-based authentication and authorization[12, 3].

This paper introduces an intelligent access control model for detecting leakage of personal information including device information, location information, address book, message and so on. In the

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 1, Article No. 15 (January 15, 2015)

*Corresponding Author: Chosun University, No. 8111, Computer Engineering, 309, Pilmun-daero, Dong-gu, Gwangju, 501-759 Rep. of Korea, Tel:+82-62-230-7636, Web: <http://iclab.chosun.ac.kr>

proposed model, the permission by category of application services is analyzed as well as new malwares are detected through context ontology inference of API resource information and permission. Especially the proposed model enables dynamic security level access.

The remainder of this paper is organized as follows: Section 2 describes related work of android security type and access control model. In section 3, we propose an intelligent access control model for information leak detection based on ontology inference. We performed the experiment and evaluation of the proposed method in section 4. Finally, in section 5, we present the conclusion and future study direction.

2 Related Work

2.1 Security Type based on Android Platform

This section describes information leak route and cases in smartphone environment. Table 1 shows information leak route and cases. The most common leakage of user information has been caused by malicious code and it occurs from a variety of sources. Typical methods are being introduced through SMS phishing or social engineering techniques, intelligent detection technologies. Detecting malicious code is a difficult task because there are new malicious code emerge as improvement in detecting technology[13].

Table 1: An example of information leak in android platform

Type	Path	Threat Case
Smishing (SMS+Phishing)	URL connection Inducement using SMS	<ul style="list-style-type: none"> · Malware infection · Charge-induced · Spamming exposure
Social Engineering Method	Malware using email, SMS and etc.	<ul style="list-style-type: none"> · Address Book Information Disclosure · Media Information Disclosure · Messages Information Disclosure · Moving the storage medium information disclosure
Physical Factor	Loss of smart device	<ul style="list-style-type: none"> · Moving inside the storage medium Personal / Company Information Disclosure · Secondary security threat

Trojans and PUP type malicious code are the highest proportion of malicious code in recent Android platform. Typically, Android-Trojan/FakeInst in an application spoofs IMEI information of the device and send the personal information via SMS. Android-PUP/Airpush is an advertising framework that aggressively pushes ads to the devices even the user doesn't run its application[6], [15].

Most of the malicious code has been deployed using the repackaging in the following way Figure 1, malicious developers download an application from Google Market and includes their malicious code into the package (Decompile) before upload the specific application, which contains malicious code, to a 3rd-party market. If a user downloads the application from that 3rd party market, the application runs in background state and gets the user information.

Repackaging the APK of application with malicious code requests the unnecessary least privilege of the application and the user information has been collected by this route. However, The conventional malicious behavior detection techniques still have low accuracy because they only navigate the malicious application which reacts malicious behavior based on the presence or absence of the permission[11], [14].

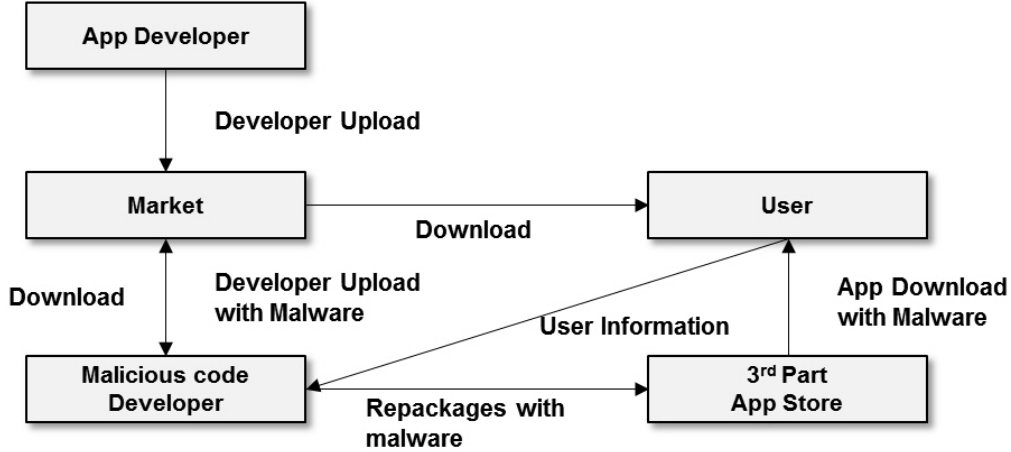


Figure 1: A processing of the malicious code deployment using the repackaging method

2.2 Access control model of the Android platform

Sensitive information in accordance with the increase of the data stored in the internal smartphones have leaked by an unauthorized user, the risk of modulation was increased. The need for access control is required in order to access the information for the rights according to this role. Access Control means a user or 'Subject' of processor is able to reading, writing and execution the database with user information or file 'Object' which contains the private information[8], [5].

The file system access in Android environment uses DAC(Discretionary Access Control) method, which is able to add or delete the user's access rights based on user identification. That allows a user to access to a random file to read, write and execute privileges so that the malicious user can easily obtain unauthorized access to data file and app resources acquired the DAC permission[10], [9].

In random access control policy, the access control can be changed because the user who owns the object can set the set of access control to the subject and object units. However, because of the control access to kernel resources, the random access control based on the particular application environment cannot be executed.

3 Inference-based access control model designed for information leakage detection

3.1 Inference-based access control framework and implementation process

Configuration of the overall framework of the inference-based access control for personal information leakage detection is made, as shown in Figure 2. Frist, model the ontology of the specific permission analyzing the permission of application category, then extract the package name of current running service and analyzing the classification category of the application from the information of Google market to analyze the category of current running application.

It consists of Access Control Module to manage Context Analysis Engine, User Authentication, security services such as access control according to the status information from a smartphone environment for collecting and managing the status information requested by the application module and to classify the categories.

Android system provides the provider for each database to obtain the accessible security and flexi-

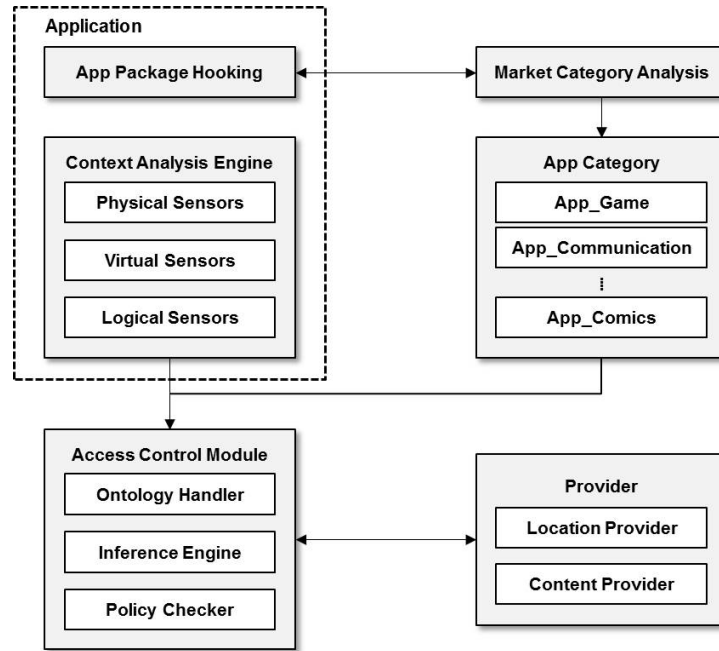


Figure 2: A framework of access control based on inference

bility of the application of internal database. Figure 3, shows the determination of the access provider.

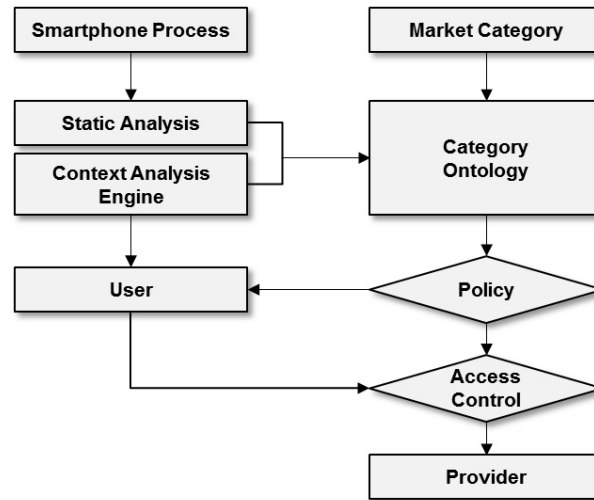


Figure 3: A processing of access control based on inference

First, extract the package name of the foreground service that is currently running on the Android environment, and then parse the registered category information from Google market using the extracted package name in order to analyze the category of the current running application.

To study the characteristic pattern of the classified application category, analyze the major credentials of specific appropriate category using static analysis and define a policy to build the context category ontology[4]. At this point, ask the user to confirm if the user is in breach of an application for a security policy through the reasoning of when to request an internal database of the authority to request the information by category of applications that can lead to malicious actions based on the permissions and

malicious via API to allow or block access to the resource through.

3.2 Classification and Permissions of Android application category

Category through the Google market to analyze the main Permission information by category of Android applications analysis of the top each 50 most popular free and measures a total of 1,200 APK file permissions entries. Some of the major authority list classified Specific category are as follows Table 2. More than 90% application access the internet from INTERNET permission information and ACCESS_NETWORK_STATE permission information, to determine the network status, and 60 70% of specific appropriate application category learn the characteristic permission privileges based on requested permission pattern information respectively.

Table 2: A request pattern of category permission

	Game	Health	Education	Transportation	Financial	Weather	News	Decoration
ACCESS_COARSE_LOCATION	14	26	8	39	17	37	18	17
ACCESS_FINE_LOCATION	6	15	7	38	22	48	47	11
ACCESS_GPS	-	-	-	27	-	-	-	-
ACCESS_LOCATION	-	-	-	28	-	-	-	-
ACCESS_LOCATION_EXTRA_COMMANDS	10	-	-	-	8	-	-	-
ACCESS_NETWORK_STATE	50	50	42	50	45	50	-	45
INTERNET	50	48	47	49	50	48	50	38
ACCESS_WIFI_STATE	36	19	7	27	13	36	14	18
CAMERA	-	8	9	-	14	-	8	4
CHANGE_NETWORK_STATE	22	-	-	-	5	-	-	-

3.3 Inference-based access control model design

Through analysis by category of application permissions, learning about the relationship between the main characteristics of each category permissions request privileges and privileges on information disclosure, and use the Protege ontology modeling constructs. The following Figure 4 indicates a context specific ontology modeling app category.

Combinations that can lead to malignant behavior through the inference in the class with respect to the personal information related to spill over through the access privileges by using the relationship between the built ontology running the application requires that the resource rights and application category for the resource access request the judgment, and ask the user to the user when using the least privilege access control through access control model. The following Table 3 represents the permission to disclose the personal information on the combination of malware.

New malicious code of the category of an app can be inferenced by performing ontology inference.

4 Experiments and Evaluation

Implement the access control model for the leakage of personal information to detect and check the results in order to verify the accuracy of the detection of the leakage of personal information from the

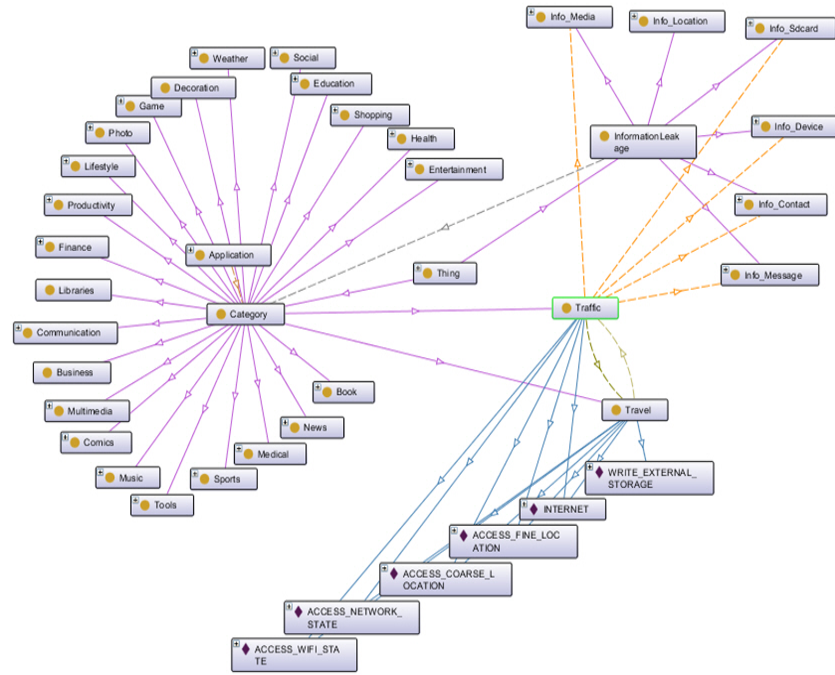


Figure 4: A ontology modeling of App category

Table 3: Permission combination of the personal information leak

Category	Permission	Description
Info_Device	INTERNET READ_PHONE_STATE	Read the cellphone transmitting information via the Internet
Info_Device	SEND_SMS + INTERNET READ_PHONE_STATE	Read the Mobile Phone Information SMS, sent via the Internet
Info_Location	INTERNET ACCESS_FINE_LOCATION ACCESS_COARSE_LOCATION	Reading the location information and transmit

intelligent inference based access control model. Intelligent access control model based on rights management and the importance of personal information disclosure is required, and to ask for permission for each API function relationships by setting intelligent access control model offered in the Smartphone environment.

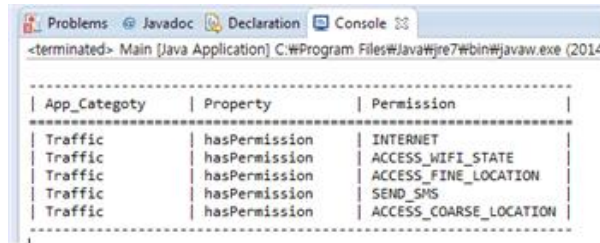
Personal information leakage detection system applications in the Android environment caused by device information, address book information, text messages, notes, call history information for the prevention of leakage of personal information, and access control. In the experiments to verify the performance of the intelligent access control and security requirements of the access control model in consideration of the category-specific conditions Table 4 authorized by category, such as to define with the result of executing the proactive approach control according to the situation check.

Application related to 'traffic' category mainly used the Internet-related applications subject to status inquiries, internet access, Wifi access, through a combination of private information and examine on the

Table 4: Security policy of the personal information leak

Circumstances	Security Requirements
Terminal information	<ol style="list-style-type: none"> 1. Terminal directory 2. Information transfer device
Message information	<ol style="list-style-type: none"> 1. Terminal inside the SMS message directory 2. Writing SMS messages 3. SMS messages sent 4. SMS messages
Call Information	<ol style="list-style-type: none"> 1. Terminal view call status 2. The information recording device address book 3. The terminal contacts information contact
Location Information	<ol style="list-style-type: none"> 1. Terminal position directory 2. Send the terminal location information

authority to request prior authorization to receive requests and GPS information to be leaked by SMS, performed by an application that includes five permissions information of SEND_SMS permission rights.



```

<terminated> Main [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (2014.

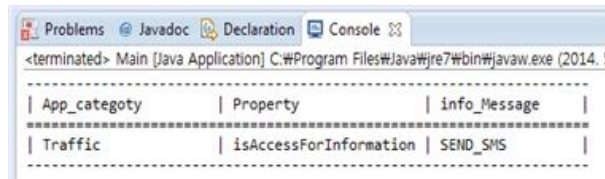
```

App_Catagoty	Property	Permission
Traffic	hasPermission	INTERNET
Traffic	hasPermission	ACCESS_WIFI_STATE
Traffic	hasPermission	ACCESS_FINE_LOCATION
Traffic	hasPermission	SEND_SMS
Traffic	hasPermission	ACCESS_COARSE_LOCATION

Figure 5: A result before inference rules applied

While one of the categories of applications, 'traffic', is running, check the result of the resource information of requesting the application related to 'traffic' through the relationship set of its ontology modeling. While one of the categories of applications, 'traffic', is running, check the result of the resource information of requesting the application related to 'traffic' through the relationship set of its ontology modeling Figure 5. The Authorization requested information of the application can be confirmed because the application results does not apply the inference.

The experiments 'traffic' result using the Jena inference engine for context information leakage that may occur in related applications applying the inference rule is as follows Figure 6.



```

<terminated> Main [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (2014. 5

```

App_catagoty	Property	info_Message
Traffic	isAccessForInformation	SEND_SMS

Figure 6: A result after infernece rules applied

Although, In the specific permission element of the application like Transportation, INTERNET element, to access the internet, ACCESS_COARSE_LOCATION to obtain GPS information, and ACCESS_FINE_LOCATION element are included, the location information disclosure can be occurred via

SMS transmission of GPS information using SEND_SMS element. Detection the personal information leakage resources can be found according to analyzing the malicious code. Once the granular permission privileges and the relationship set of API function have been built, there will also be a high accuracy in detection of new malicious acts.

5 Conclusion

This paper studies not only the characteristics and behavior of malicious code to steal personal information from smartphones, but also presents the inference-based access control model, which detects the outflow behavior of personal information and controls access to information resources. According to the evaluation, the proposed model shows an improvement in detecting both the existing malicious code and new unknown malware infection compared to the existing detecting method. In further future studies, we will use APK data file to analyze the detail features by category, perform ontology modeling, and finally increase the detection accuracy through the complex testing procedure composed of several steps according to the research access.

Acknowledgment

“This research was supported by ‘SW master’s course of a hiring contract’, through the Ministry of Science, ICT and Future Planning(HB301-14-1006) and Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning(2014R1A1A1005915).

References

- [1] Report: 97safe. <http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/>, 2014.
- [2] R. Amadeo. Google’s iron grip on android: Controlling open source by any means necessary. <http://arstechnica.com/gadgets/2013/10/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/>, 2013.
- [3] M. Bourimi, S. Scerri, M. Planaguma, M. Heupel, F. Karatas, and P. Schwarte. A two-level approach to ontology-based access control in pervasive personal servers. *University of Siegen Catalogue for internal publications*, pages 1–16, November 2011.
- [4] C. Choi, J. Choi, and P. Kim. Ontology-based access control model for security policy reasoning in cloud computing. *Journal of Supercomputing*, 67(3):711–722, March 2014.
- [5] D. F. Ferraiolo, J. A. Cugini, and D. R. Kuhn. Role-based access control (rbac): Features and motivations. In *Proc. of the 11th Annual Computer Security Applications Conference (ACSAC’95)*, New Orleans, Louisiana, pages 1–8. IEEE, December 1995.
- [6] C. Gibler, J. Crussell, J. Erickson, and H. Chen. Androidleaks: Automatically detecting potential privacy leaks in android applications on a large scale. In *Proc. of the 5th International Conference on Trust & Trustworthy Computing (TRUST’12)*, Vienna, Austria, LNCS, volume 7344, pages 291–307. Springer-Verlag, June 2012.
- [7] G. Inc. Android platform. http://www.webopedia.com/TERM/A/Android_platform.html, 2009.
- [8] M. J. Moyer and M. Ahamad. Generalized role-based access control. In *Proc. of the 21st International Conference on Distributed Computing Systems (ICDCS’01)*, Arizona, USA, pages 391–398. IEEE, April 2001.

- [9] R. Sandhu, D. Ferraiolo, and R. Kuhn. The nist model for role-based access control: towards a unified standard. In *Proc. of the 5th ACM workshop on Role-based access control (RBAC'00)*, Berlin, Germany, pages 47–63. ACM Press, July 2000.
- [10] R. S. Sandhu, E. J. Coynek, H. L. Feinstein, and C. E. Youmank. Role-based access control models. *IEEE Computer*, 29(2):38–47, February 1996.
- [11] B. P. Sarma, N. Li, C. Gates, R. Potharaju, C. Nita-Rotaru, and I. Molloy. Android permissions: a perspective combining risks and benefits. In *Proc. of the 17th ACM symposium on Access Control Models and Technologies (SACMAT'12)*, Newark, USA, pages 13–22. ACM, June 2012.
- [12] H. Shen and Y. Cheng. A semantic context-based model for mobile web services access control. *International Journal Computer Network and Information Security*, 3(1):18–25, February 2011.
- [13] J.-M. You and I.-K. Park. Android storage access control for personal information security. *Journal of The Institute of Internet, Broadcasting and Communication*, 13(6):123–129, December 2013.
- [14] Y. Zhong, H. Yamaki, and H. Takakura. A malware classification method based on similarity of function structure. In *Proc. of the 12th International Symposium on Applications and the Internet (SAINT'12)*, Izmir, Turkey, pages 256–261. IEEE, July 2012.
- [15] Y. Zhou and X. Jiang. Dissecting android malware: Characterization and evolution. In *Proc. of the IEEE Symposium on Security and Privacy (S&P'12)*, San Francisco, USA, pages 95–109. IEEE, May 2012.

Author Biography



Junho Choi received a doctoral degree in the department of computer science at Chosun university of Korea in 2004. Currently, He is a assistant professor in the department of division of undeclared majors. His research interests include computer security, semantic information processing, ontology engineering and semantic web.



Chang Choi received a doctoral degree in the department of computer Engineering at Chosun University of Korea in 2012. Currently, He is working as a research professor at the same university. His research interests include semantic information processing, semantic web and Multimedia.



Htet Myet Lynn is a student for the Master Degree in Computer Engineering from Chosun University of Korea. His reasearch interests include Natural Language Processing, Automatic Text Summarization.



Byeongkyu Ko is a student for the doctoral degree in computer engineering from Chosun University of Korea. He received a master degree at the same university in 2012. His research interests include web documents classification, Natural Language Processing, semantic information processing and semantic web.



Ilsun You received his MS and PhD degrees in Computer Science from Dankook University, Seoul, Korea in 1997 and 2002, respectively. Also, he obtained his second PhD degree from Kyushu University, Japan in 2012. In 2005, he joined Korean Bible University, South Korea as a full time lecturer, and he is now working as an associate professor. Dr. You has published more than 110 papers as well as edited more than 20 special issues with focus on the topics including internet security, mobility management, cloud computing, pervasive computing, and so forth. Dr. You is IET Fellow and IEEE Senior Member.



Pankoo Kim received his M.S. and Ph.D. degrees in computer engineering from Seoul National University, Korea in 1994. He is a full professor in the department of computer engineering at Chosun university. He is in the editorial board for International Journal of IT CoNvergence PRActice. His specific interests include semantic web techniques, semantic information processing and retrieval, multimedia processing and semantic web.