Research and Application of Device Fingerprint

Xinming Yin [a], Zhengliang Hu, Guoliang Chen, Haiye Huang, Zhiwei Cao

Information Security Technology Division, The Third Research Institute of Ministry of Public Security, Shanghai 201204, China

[a]yinxm6@163.com

Keywords: Access detection of video dedicated network, Device fingerprint, Decision tree, Information entropy.

Abstract. Because many acquisition equipments of video network are deployed in public areas, they face many security issues. It is very important to connect the video equipments to the video dedicated network safely and efficiently. In this paper, we propose a decision tree classification algorithm of device fingerprint to solve the problem. According to the characteristics of video equipments, we design the device fingerprint on the basis of the operating system fingerprint. Meanwhile, we also propose the collection and storage methods of device fingerprint. The decision tree classification algorithm of device equipment can detect the untrusted devices in the video dedicated network, and can also prompt the system to send alarm information. In a word, this project can effectively prevent the illegal intrusion and keep the data in video dedicated network from leaking.

1. Introduction

With the development of video surveillance technology, video dedicated network plays a more and more important role in the actual business of various industries. But many video dedicated network video collection equipment deployment in a public area, their securities and reliabilities can't be well protected. Once the intrusion events, the safety of the video dedicated network resources will not be protected, and thus may lead to serious problems, such as citizens' privacy, the reliable video dedicated network net detection technology has important significance and value.

2. Device fingerprint in the video network

Dedicated or generic devices in the video dedicated network have their own specific operating system, which contains the basic features of a common operating system.

2.1 Design of device fingerprint in the video network

Most of the domestic market IP cameras support the SNMP protocol. For the cameras which don’t support the SNMP protocol, device fingerprint feature is only contains the operating system of fingerprint part; For the cameras which support the SNMP protocol, we only need to deploy SNMP agent on the device, it resides in the workstation in device, can respond to the request of the network monitoring server and provide the device data information for the request.

Research of network fingerprint technology [7-10], we can refer to the fingerprint of operating system and relevant content of SNMP network equipment management information, which can help design equipment fingerprints of IP surveillance camera. DEV_fingerprint contains the following several dimensions of features, and reserve some expand options (Table 1).

2.2 DEV_fingerprint acquisition in video dedicated network

Figure 1 shows the position of the device fingerprint network detection server in the dedicated network system, its role is to scan the video network equipment. For the existence of abnormal behavior or replacement of the equipment is in a timely manner alarm. Video dedicated network DEV_ fingerprint acquisition is divided into the two ways of active polling acquisition and boot polling acquisition.

Table 1. The features of DEV_fingerprint

feature	meaning	For example
IP_Address	IP address	192.168.1.99
MAC_Address	MAC address	D4:3D:7E:AC:F7:B8
Device_type	Device type	General
OS_type	Operating system category	Linux 3.X
SW_InstalledName	The list of software installed on the device	Mysqld telnet ...
Using_port	The port on the device that is being used	23/tcp 80/tcp ...
Using_service	The service is running on the device	rtsp Pwgpsi ...
Port_for_service	The port of the service that is running on the device	http 80/tcp Rtsp 554/tcp ...
Net_distance	Network spacing	2 hops
OS_details	Operating system version information	Linux 3.8 - 4.5
CPUInfo	Average CPU usage per unit time	HOST-RESOURCES-MIB::hrProcessorLoad.768 = INTEGER: 42 ...
DSK_Used	Disk usage information	Filesystem Size Used Avail Use% tmpfs 4.0G 1.0 3.0G 25% ...
Memory_Used	Memory usage information	MemTotal: 8267896 kB MemFree: 6026888 kB

netIFInfo	Network interface information description	IF-MIB::ifDescr.1 = STRING:eth0
		ifHCInOctets.1 = Counter64: 210400
		fHCOutOctets.1 = Counter64: 83501

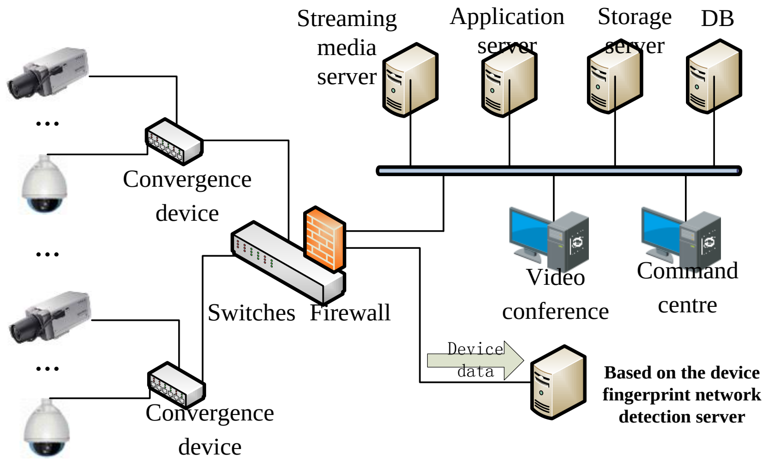

Fig. 1 Network detection server based on the device fingerprint

Figure 2 is active polling acquisition process of DEV_fingerprint in video dedicated network, which describes the monitoring the active devices in a video dedicated network information process.

Polling acquisition will lead to the problem which the information data is not real-time. Here, we introduce access guide and Trap guide when polling technique. Access to guide the acquisition or when a camera and dedicated network communications for the first time occurs, by giving notice to the net in figure 2 switch or firewall test server, to guide the company server of the devices for information collection. In the configuration of the SNMP agent on the device opens the SNMP Trap lead to each SNMP polling techniques agent to Trap report to management workstation exception events news report, news station found the Trap when it reports on an exception report of network scanning equipment for real-time information.

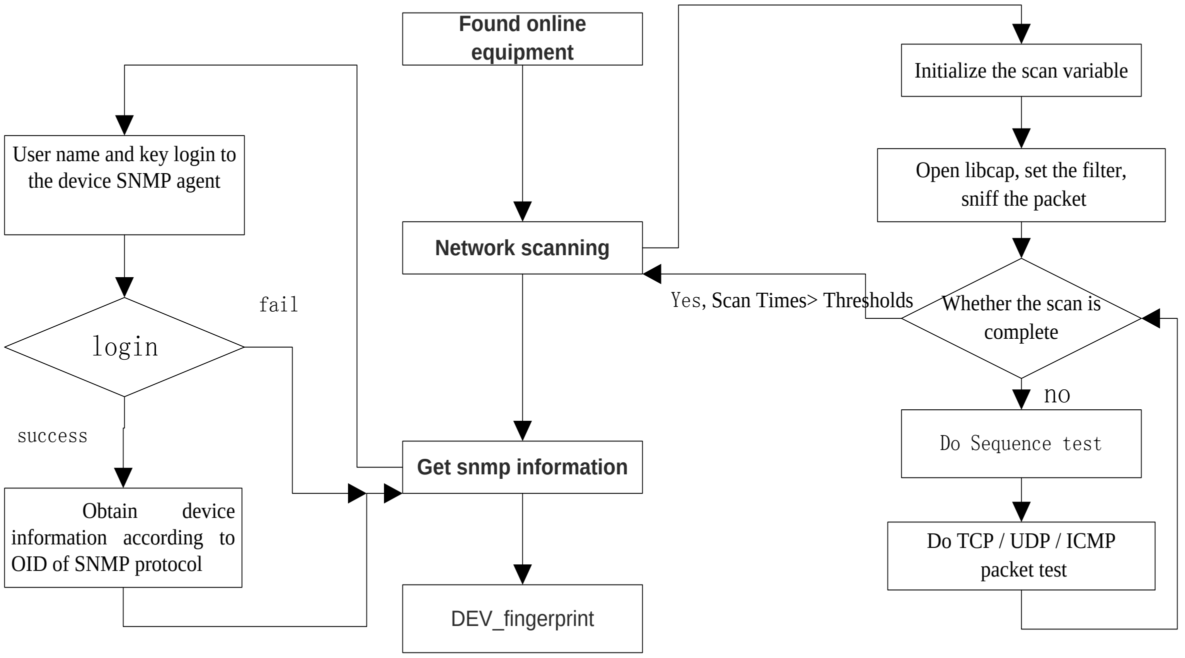
Found online equipment
Initialize the scan variable
User name and key login to the device SNMP agent
Open libcap, set the filter, sniff the packet
Network scanning
fail
Yes, Scan Times> Thresholds
Whether the scan is complete
login
no
success
Do Sequence test
Get snmp information
Obtain device information according to OID of SNMP protocol
Do TCP / UDP / ICMP packet test
DEV_fingerprint

Fig. 2 Active polling acquisition process of DEV_fingerprint in video dedicated network

3. Intrusion detection of video dedicated network

The detection of video dedicated network is to use the equipment DEV_fingerprint acquisition technology, which can find signs of dedicated network intrusion behavior, or be attacked in control equipment. The illegal invasion can be timely found, and the corresponding warning to take emergency measures.

3.1 Decision tree algorithm

Decision tree algorithm to deal with the data classification accuracy is high, the noise data on the anti-interference ability. The frequently-used decision tree algorithms mainly include ID3, C4.5, CART algorithm, the data space for processing is based on information entropy, information gain and so on.

1) Information entropy

The information entropy is used to solve the system information on the measurement of quantitative problems, and can be understood as the amount of information. The uncertainty of information can only reflect the symbol, and the information entropy can be used to measure the uncertainty of the entire source X overall.

Set something to have n kinds of independent possible states: $x_1, x_2, \cdots, x_n$, The probability of each state is $P(x_1), P(x_2), \cdots P(x_n)$,and

$$\sum_{i=1}^{n} p(x_i) = 1 \tag{1}$$

Then, the information entropy of the thing is:

$$Entropy(X) = p(x_1)I(x_1) + \cdots + p(x_n)I(x_n) = -\sum_{i=1}^{n} p(x_i)\log_2 P(x_i) \tag{2}$$

2) Information gain

Information gain is for each feature attribute. For a property A, the system has it and it is not the amount of information when the amount of the difference between the two is the property to the system to bring the amount of information that is information Gain. The information gain Gain (X, A) of a property A relative to the sample set X is defined as:

$$Gain(X, A) = Entropy(X) - \sum_{v \in V(A)} \frac{|X_v|}{|X|} Entropy(X_v) \tag{3}$$

Where V (A) is a set of all possible values of attribute A, X_v is a subset of the attribute A of v in X,| X_v | and | X | represent the number of records in the collection, respectively. Gain (X, A) is the information gain about the target value due to the value of the given attribute A.

3.2 Video dedicated network intrusion detection based on device fingerprint decision tree algorithm

In this case, the decision tree algorithm is used to segment the dynamic information DB of the dynamic fingerprint of the device, and the fingerprint of the device in each leaf node will be more and more similar. Dynamic fingerprint DB dynamic collection of fingerprint library for the training data is set D, security rule DB in each rule as a property, the use of decision tree algorithm to create a decision tree.

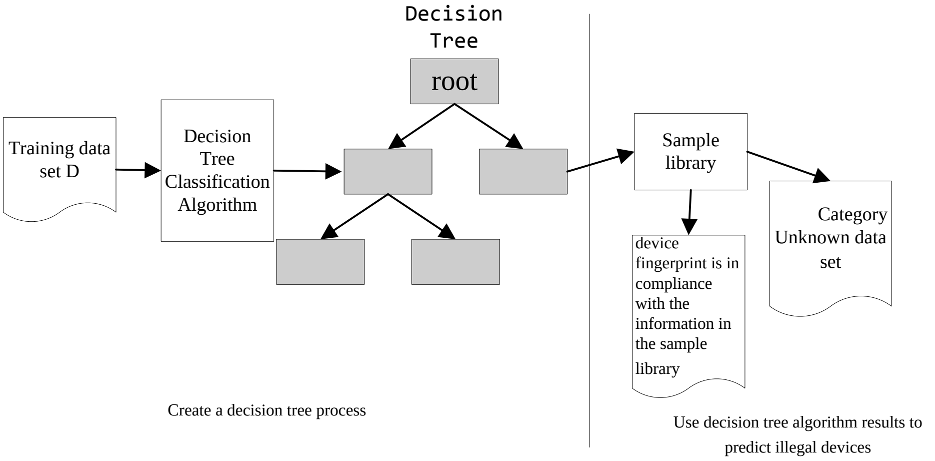
Decision Tree
root
Training data set D
Decision Tree Classification Algorithm
Sample library
Category Unknown data set
device fingerprint is in compliance with the information in the sample library
Create a decision tree process
Use decision tree algorithm results to predict illegal devices

Fig. 3 Process diagram of the decision tree classification algorithm model

The figure 3 is a dynamic DEV_fingerprint repository decision tree classification algorithm model, the specific process is as follows:

Definition:

1) Decision rules($rule_1, rule_2, ..., rule_m$), The device fingerprint record feature set A consists of all the likelihood values of the decision rule;

2) Training data set is dynamic_DB($data_1$, $data_2$,..., $data_n$), $data_i$ is a fingerprint record, Initializes the record class of the same attribute of k : C_k ,k=1,2,...,k;

3) One or more records($data_i$,..., $data_j$)in a leaf nodeHave the same or similar characteristic attributes;

4) Information gain threshold ε .

Created DEV_fingerprint Decision Tree with decision tree classification algorithm:

1) If all records in dynamic_DB belong to the same class C_k , Then T is a single node tree, And the class C_k as the node class tag, return T;

2) If A= Φ , then T is a single node tree, and the class C_k with the largest number of instances in dynamic_DB is the class tag of the node, return T;

3) Otherwise, according to the formula (4-3) to calculate the characteristics of the A dynamic_DB information gain, select the information gain of the largest characteristics of A_g ;

4) If the information gain of A_g is less than the defined threshold ε , then T is a single node tree, and the class C_k with the largest number of instances in dynamic_DB is the class tag of the node, return T; else, for each possible value a_i of A_g , according to $A_g = a_i$, Dynamic_DB is divided into several nonempty subsets dynamic_DB[i] , Mark the largest number of records in dynamic_DB [i], Constructs a child node, T Consists of nodes and their child nodes, return T;

5) For the i-th sub-node, use dynamic_DB [i] as the training set, with $A - A_g$ as a feature set, recursive call 1) step-4) step Get the subtree T_i, return T_i To a layer of recursive call.

4. Conclusion

In this paper, we study an intrusion detection system of video dedicated network, which is based on decision tree classification of device fingerprint. This system can effectively help us find anomalies of devices in video dedicated network. The accuracy of decision tree classification algorithm depends on the sample library of richness. In the future, we will continue to research the "incremental learning" decision tree learning algorithm, which is based on video dedicated network environment. And we will design an intrusion detection system of video dedicated network with higher accuracy.

References

[1]. GB/T 28181-2011,Security and protection video monitoring network system technical specification for information transport, switch and control

[2]. MA zhuo, Ma Jian-Feng, LI Xing-Hua, et al. Provable Security Model for Trusted Network Connect Protocol. Chinese Journal of Computers, 2011(9):1669-1678.

[3]. ZHANG Ming-de, ZHENG Xue-feng, LV Shu-wang, et al. Research on Trust Degree of Authentication. Computer Science, 2011, 21(11):43-47.

[4]. Mao Yuxin,Hao Zhenwu, Jiang Jiaren.A Network Architecture Based on Trusted Identity and Its Application. ZTE Technology Journal, 2016(3).

[5]. CAO Zhi-wei, SHAO Xu-dong, FAN Zhi-jie, LIU Yang, et al. Response Mechanism of Road Emergency Based on Video Security Access. Computer Technology and Development, 2015 (7): 166-169.

[6]. LIU Xiao-Wu, WANG Hui-Qiang, LÜ Hong-Wu, et al.Fusion-Based Cognitive Awareness-Control Model for Network Security Situation. Journal of Software, 2016(8):2099-2144.

[7]. Keaton Mowery, and Hovav Shacham. Pixel perfect: Fingerprinting canvas in HTML5. Proceedings of Web 2.0 Security and Privacy.2012.

[8]. Nick Nikforakis, Alexandros Kapravelos, Wouter Joosen, Christopher Kruegel,Frank Piessens, and Giovanni Vigna, Cookieless monster: Exploring the ecosystem of web-based device fingerprinting. Proceedings of 2013 IEEE Symposium on Security and Privacy. Berkeley, CA, 2013: 541-555.

[9]. Ramandeep Kaur, Parvinder S. Sandhu, Amit Kamra. A Novel Method for Fingerprint Feature Extraction, IEEE Networking and Information Technology, 2010:1-5.

[10]. CHENG Shu-bao, HU Yong. Operating System Recognition based on Singular Value Decomposition and DAG_SVMS. China Information Security, 2013(9):66-68.

[11]. NMAP. Network mapper [EB/OL].[2015-12-20]. http://nmap.org/.

[12]. LI Hong-cheng, WU Xiao-ping, YAN Bo. Research on distributed genetic k-means for anomaly detection in MANET. Journal on Communications, 2015(11):1-7.

[13]. ZHANG Li-ping, LEI Da-jiang, ZENG Xian-hua. System Calls Based Intrusion Detection Method with Frequency Feature Vector. Computer Science, 2013(S1): 330-334.

[14]. Li Yongzhong, Chen Xingliang, Yu Hualong. ntrusion detection technologies based on improved evidence fusion of DS and ELM. Application Research of Computers, 2016(10).

[15]. GUO Qibiao, LI Bingjian. Network Intrusion Detection Based on Akaike Information Criterion and BP Algorithm. Journal of Jilin University: Sci Ed, 2015(4):715-719.

[16]. LIU Yaqiu, LI Haitao, JING Weipeng. Implementation of decision tree algorithm dealing with massive noisy data based on Hadoop. Journal of Computer Applications, 2015(4): 1143-1147.