Internet Protocol Cameras with No Password Protection: An Empirical Investigation

Haitao Xu[*], Fengyuan Xu[†], and Bo Chen[‡]

[*]Northwestern University, Evanston, IL 60201, USA
`hxu@northwestern.edu`
[†]National Key Lab for Novel Software Technology, Nanjing University
Nanjing, China
`fengyuan.xu@nju.edu.cn`
[‡]Michigan Technological University, Houghton, MI 49931, USA
`bchen@mtu.edu`

Abstract. Internet Protocol (IP) cameras have become virtually omnipresent for organizations, businesses, and personal users across the world, for the purposes of providing physical security, increasing safety, and preventing crime. However, recent studies suggest that IP cameras contain less than ideal security and could be easily exploited by miscreants to infringe user privacy and cause even bigger threats. In this study, we focus on the IP cameras without any password protection. We conduct a large-scale empirical investigation of such IP cameras based on *insecam.org*, an online directory of IP cameras, which claims to be the largest one in the world. To this end, we have monitored the site and studied its dynamics with daily data collection over a continuous period of 18 days. We compute daily number of active IP cameras and new cameras on the site, and infer people's usage habit of IP cameras. In addition, we perform a comprehensive characteristic analysis of IP cameras in terms of the most used TCP/UDP ports, manufactures, installation location, ISPs, and countries. Furthermore, we explore other possibly existing security issues with those cameras in addition to no password protection. We utilize an IP scanning tool to discover the hidden hosts and services on the internal network where a vulnerable IP camera is located, and then perform a vulnerability analysis. We believe our findings can provide valuable knowledge of the threat landscape that IP cameras are exposed to.

Keywords: IP camera; IoT security; Vulnerability analysis

1 Introduction

An Internet Protocol (IP) camera refers to a video camera which is attached to a small web server and allows the access to it via Internet protocols. Along with the growing security needs and the development of `IoT` technologies, IP cameras are being widely used to monitor areas such as offices, houses, and public spaces. However, recent reports [8, 10, 11] and studies [12, 16] have shown that IP cameras contain less than ideal security, and could be exploited and fully controlled by miscreants to infringe user privacy and even launch large-scale DDoS attacks [4, 9, 14].

Username and password is the most widely used form of authentication in practice to prevent unauthorized access. However, an incredible number of IP cameras are found to have no password protection (or more exactly, with password of null or empty) and are having their live video feeds streamed on *insecam.org*, a popular website with hundreds of thousands of visitors daily.

Most previous works mainly focus on summarizing various vulnerabilities of IP cameras and making suggestions on potential mitigation solutions. In this paper, based on the data provided by the site *insecam* about its listed IP cameras, we conduct an in-depth, large-scale quantitative evaluation of vulnerable IP cameras with no password protection. Specifically, we performed daily collection on *insecam* over a continuous period of 18 days. As a result, we observed 28,386 unique IP cameras, from 31 timezones[1], 136 countries, and 25 manufacturers, streaming their live video feeds on *insecam* without awareness of IP camera owners. In addition to those currently active IP cameras, we managed to exhaust and collect all the history records of IP cameras ever streaming on *insecam*, with a total number of 290,344. We then performed a comprehensively characteristic analysis of those IP cameras and also conducted vulnerability analysis of the internal networks where those IP cameras reside with an attempt to identify more vulnerabilities.

Our work is the first measurement study on IP cameras using *insecam.org* as a possible data source. Based on the assumption that all the information posted on *insecam* about the IP cameras is correct, we highlight the following findings: 1) there are about 20,000 to 25,000 active cameras shown on insecam each day and 215 new cameras are added daily on average; 2) 87.4% IP cameras on insecam are from the three geographic regions - `Europe`, `East Asia`, and `North America`, while `United States` alone contributes 22.5% of those cameras; 3) monitoring the on/off state of IP cameras could reveal usage habit of IP cameras; 4) more than a half of cameras are from the two manufacturers, `Defeway` and `Axis`; 5) a third of IP cameras use the port 80 to communicate to their administrative interface; 6) about a quarter of hosts where an IP camera resides have remote access ports 22 (`SSH`) and 23 (`Telnet`) open, which make them more vulnerable to attackers; 7) nearly all those cameras were running extremely old and vulnerable web server software, most of which are found to bear tens of `CVE` (Common Vulnerabilities and Exposures) vulnerabilities. We believe our findings can provide valuable knowledge of the threat landscape that IP cameras are facing.

[1] There are 39 different timezones currently in use in the world [6].

2 Background

In this section, we briefly introduce IP cameras and the site *insecam.org* where we collected data.

IP cameras. An IP camera contains a CPU and memory, runs software, and has a network interface that allows it to communicate to other devices and be remotely controlled by users. Different from CCTV cameras (closed-circuit television cameras), IP cameras have the remote access features for administration and video monitoring. However, the remote accessibility can be exploited by a hacker, especially when users adopt default settings and credentials for the web administrative interface.

insecam.org. This site is reported to have existed since September 2014. It is claimed to be the world largest directory of network live IP video cameras. The first time the site attracted media attention was in November 2014 [8, 10, 11], when journalists reported that the site provided a directory for countless private IP cameras which streamed privacy-sensitive live video feeds. Since then, the site administrator seems to have enforced strict policies that only filtered IP cameras can be added to the directory. However, there are still hundreds of thousands of IP cameras listed on the site without their owners' awareness. In addition, all IP cameras on *insecam* are accessible without any authentication (i.e., no password protection) and the live video stream can be directly viewed by any visitors across the world.

3 Measurement Methodology and Dataset

insecam.org collects a large set of currently active IP cameras that have no password protection. And those cameras seem not to be remotely controlled or interfered by *insecam.* According to the policy described on the homepage of *insecam* [7], anyone could request the site administrators to add an IP camera to the directory by providing the IP and port of the camera. For each active IP camera, *insecam* streams its live video feeds on the site for visitors to watch and also provides relevant metadata information including the camera IP, port, manufacturer, geolocation information (country, city, and timezone), and a tag describing the subject of the video feed (e.g., animal, street) if available. An IP camera turned off by its owner cannot be accessed on *insecam*, and thus the total number of active cameras shown on *insecam* is always changing. In addition, each IP camera is assigned a unique ID by *insecam* and the ID of an IP camera could usually lead to a webpage displaying the IP camera metadata information.

Our general goal is to evaluate the seriousness of security issues with vulnerable IP cameras through the study on *insecam.* Our measurement methodology is driven by three specific goals. First, we wish to examine the dynamics of *insecam* in terms of daily number of active IP cameras and new cameras on the site. Second, we want to characterize those IP cameras without password protection in terms of their manufacturers, installation location, ISPs, and countries. Third, we want to explore the possibility that a vulnerable camera could be leveraged as a pivot point onto the internal network.

We built a Python crawler that allows us to automatically collect the information about the IP cameras posted on *insecam.* Considering the always changing number of active cameras due to turning on or off, we ran the crawler at least four times each day at six-hour time interval. The collected information suffices for our purposes of examining *insecam* dynamics and characterizing IP cameras, except the information about what ISPs are hosting those vulnerable IP cameras. We then queried the IP addresses of *insecam* cameras in an online IP geolocation database [5] to obtain the corresponding ISP information.

In addition, based on the observation that the camera IDs on *insecam* are all integers and the camera IDs in our collected dataset have many missing values, we assume that *insecam* assigns *sequential* IDs to its cameras, and conjecture that those missing camera IDs correspond to the IP cameras which were ever collected on *insecam* but are currently not accessible due to either no longer working or password setup. We ran the crawler to request the corresponding web pages for the camera metadata information. In this way, we believe we are able to exhaust or at least very close to collect all the history records of IP cameras ever appearing on *insecam.*

We also utilized an IP scanning tool [1] to discover the hidden hosts and services which co-reside with the vulnerable IP cameras in the same internal network. We paid special attention to the services (e.g., `SSH` and `Telnet`) which are often probed by attackers as the starting point for further attacks. We then performed vulnerability analysis based on the collected co-residing information.

Dataset. Through daily data collection over a continuous period of 18 days, from September 25, 2017 to October 12, 2017, we have observed 28,386 unique, active IP cameras listed on *insecam*, which are from 31 timezones, 136 countries, and 25 manufacturers. For each of them, we collected its metadata information displayed on *insecam*, and probed it several times a day in the following days to determine its on/off state at that time. In addition, based on the observation that the minimum and maximum values of the IDs assigned by *insecam* for still active IP cameras are 1 and 560,293, respectively, we queried all camera IDs falling within $[1, 570, 000]$ one by one in *insecam*, and finally were able to collect the metadata information for 290,344 IP cameras (28,386 active ones included), for each of which *insecam* still maintains a webpage. We conjecture that *insecam* at least has posted 560,293 unique, vulnerable IP cameras in the past three years since the website was created; currently 290,344 (51.8%) of them still left "crumbs" for us able to track, and the reason why the information about the rest 48.2% cameras is totally missing on *insecam* is still an open question; the currently active IP cameras only occupy at most 5.1% (28,386 out of 560,293) of all IP cameras ever disclosed by *insecam.*

Ethical Consideration. In our study, we collect data from *insecam*, a publicly available website, for 18 days. During our data collection, we did not receive any concerns or get warnings from *insecam.* In addition, we anonymized the collected metadata information before using it for study. We strictly abide by the copyright licenses if present. Therefore, our work will not introduce any additional risk to *insecam* or the owners of the IP cameras listed on *insecam.*

4 Dynamics of *insecam*

We examined the dynamics of *insecam* based on collected data and present the findings as follows.

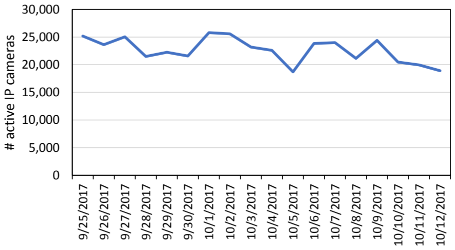

Fig. 1: Daily active IP cameras with dates.

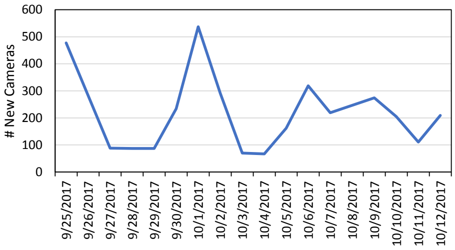

Fig. 2: Daily new IP cameras with dates.

4.1 Daily Active IP Cameras Listed on *Insecam*

Figure 1 shows the number of daily active IP cameras in the time period during which we ran our crawler. We can see that there are about 20,000 to 25,000 active cameras shown on *insecam* each day. Those cameras only represent the tip of the iceberg, since the site administrator claimed to have filtered out all cameras which may invade people's private life. Furthermore, any visitors to *insecam* have direct access to the live video feeds of those cameras from across the world, which suggests a very serious privacy issue caused by IP cameras with no password protection.

4.2 Daily New Cameras Added on *Insecam*

The number of daily new cameras reflects the popularity of *insecam*, to some extent. We also examine how many new cameras are added to *insecam* daily. By new cameras, we mean the cameras which IP addresses are not seen before in our current dataset. It is possible that an IP camera could have a different IP address if `DHCP` is enabled. Considering the claim made by *insecam* that all IP cameras are manually added, we assume that the use of `DHCP` would not cause the same IP camera to be given a new camera ID. We reached out to the site admin to confirm but received no response.

Figure 2 shows the number of daily new cameras on *insecam* in the time window we monitored. The daily new camera number varies greatly with date, with the maximum of 537, the minimum of 67, and the average number of 215. Thus, *insecam* seems to have developed quite well since November 2014, at the time *insecam* was rebuked by many medias [8, 10, 11].

4.3 Top Timezone with Most Cameras Collected on *Insecam*

IP cameras on *insecam* are well organized by timezone. We would like to know which geographic areas contribute most cameras to *insecam*. We confirmed that

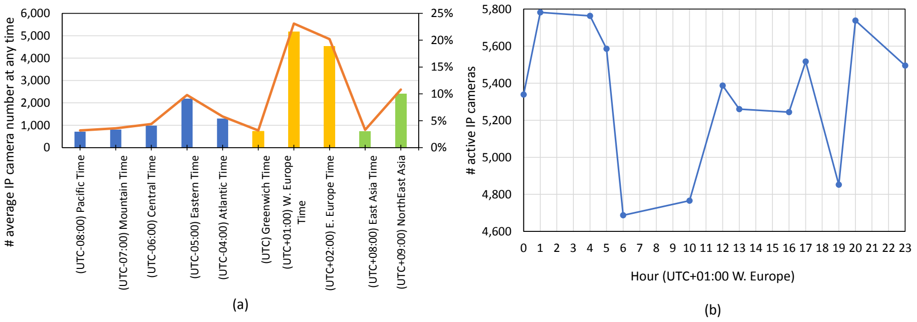

Fig. 3: (a) Top timezones with the most cameras posted on *insecam*. (b) The average number of active IP cameras in the hour (local time) of a day in UTC+01:00, West Europe.

the geolocation information provided by *insecam* is correct by comparing the geolocation information shown on *insecam* with the information returned by `Maxmind` for the same IP. Figure 3(a) depicts top 10 timezones with the most IP cameras disclosed on *insecam*. The timezone `UTC+01:00`, mainly representing `Western Europe`, contributes the most cameras and has 5,186 active cameras listed on average at a time, occupying 23.1% of all active cameras worldwide. The timezone `UTC+02:00`, mainly referring to `Eastern Europe`, comes second, with the average number of 4,522 cameras. The third and fourth timezones are `UTC+09:00` (`Northeast Asia`) and `UTC-05:00` (`Eastern America`), with 2,414 and 2,186 active cameras on average, respectively. In summary, the three geographic regions - `Europe`, `East Asia`, and `North America` - contribute the most IP cameras on *insecam*, 87.4% in total.

4.4 Usage Habit of IP Cameras within a Day

During our several times of polling of an IP camera within a day, we always observed that a proportion of IP cameras become inaccessible within some time period. We conjecture that the IP camera owners may often turn off their cameras during some time period in a day. Thus, we would like to examine the diurnal pattern of usage of IP cameras within a day.

We analyze the change in the average number of active IP cameras per hour within a single day throughout the 18 days for the timezone `UTC+01:00`, the one with the most IP cameras on *insecam*, and illustrate the results in Figure 3(b). It clearly shows that the number of active IP cameras[2] does change with the hour of the day. Specifically, there are more IP cameras to be on during the nighttime period from 17:00 in the afternoon to 5:00 in the next early morning, except the time 19:00, probably an outlier. And the active IP camera number peaks at 1:00am. In contrast, there are fewer IP cameras on in the daytime, from 6:00 to 16:00 in the figure. The finding seems reasonable given that the main purpose of IP cameras is to increase safety and prevent crime.

[2] Active IP cameras refer to the IP cameras whose video feeds are accessible online.

5 Characterization of *Insecam* IP Cameras

In this section, we examine various characteristics of the IP cameras listed on *insecam*. We want to answer the following questions: 1) what countries are having the most vulnerable IP cameras without password protection, 2) what organizations are hosting those cameras, 3) where are they being installed, 4) what are the manufacturers of those cameras, and 5) what TCP/UDP ports are used by IP cameras for communication to its administrative interface.

5.1 Top Countries and ISPs Contributing *Insecam* IP Cameras

As mentioned before, the currently active IP cameras on *insecam* are from up to 136 countries, that is, 209 IP cameras on average per country. Figure 4(a) shows the top 10 countries which contribute 61.2% IP cameras on *insecam*. `United States` tops the list and has more than 4,500 IP cameras listed on *insecam*, 22.5% out of all *insecam* cameras. `Turkey` and `Japan` come second and third, with 1,604 and 1,303 IP cameras, respectively. It seems that all the top 10 countries are either developed countries or countries with large populations.

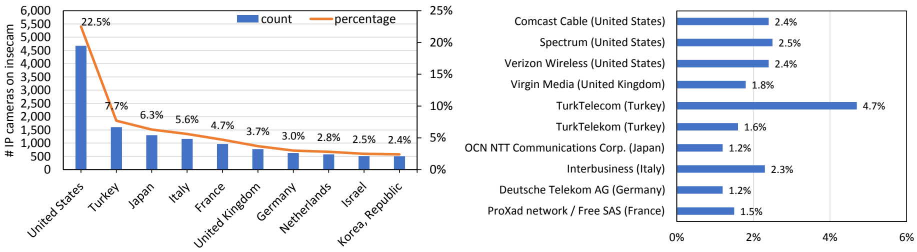

Fig. 4: (a) Top 10 countries contributing the most IP cameras on *insecam*. (b) Top 10 ISP responsible for the IP addresses of *insecam* cameras.

By querying the IP addresses of *insecam* cameras in an online IP geolocation database [5], we obtain the corresponding ISP information. There are 4,094 unique ISPs responsible for the IP addresses of *insecam* cameras. Figure 4(b) provides the top 10 ISPs and their origin countries. Reasonably, the top ISPs belong to the top 10 countries in Figure 4(a). Specifically, three out of the top 10 ISPs are from `United States`, which are `Comcast`, `Spectrum`, and `Verizon`. In addition, up to 296 (7.2%) ISPs could be identified to be universities and colleges, from 26 countries.

5.2 Installation Locations of *Insecam* IP Cameras

insecam assigns a tag describing the subject or installation location of the video feed (e.g., animal, street). We verified the correctness of the installation location information provided on *insecam* by manually viewing tens of camera live feeds. Based on the tag information associated with 7,602 IP cameras, we present the

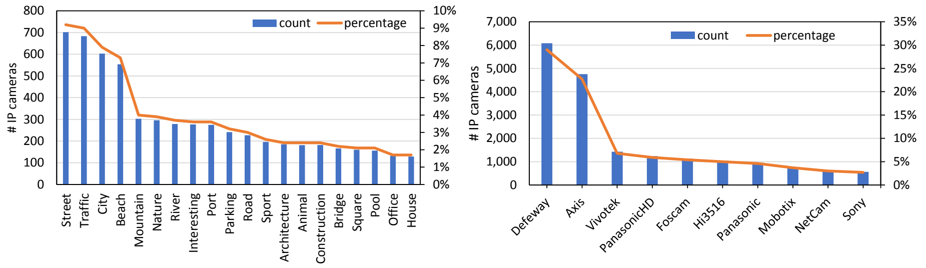

Fig. 5: (a) Top 20 installation places of the *insecam* cameras. (b) Top 10 manufacturers of those *insecam* cameras.

distribution of *insecam* IP cameras by installation location in Figure 5(a). It shows that most IP cameras are being installed in public places such as street, city, beach, mountain, and parking lots, and only a small proportion are deployed in private areas such as pool, office, and house. However, the results do not reflect the whole picture of vulnerable IP cameras in the world, given that *insecam* was almost shut down by authorities in 2014 due to too many private IP cameras being streamed on the site at that time [8,10,11] and that the site administrator claims in the home page that only filtered cameras are available on the site and the site does not stream private or unethical cameras. Nevertheless, the video feeds of a significant proportion of current active *insecam* cameras still contain privacy-sensitive content.

5.3 Manufacturers of *Insecam* Cameras

The complicated manufacturing and distribution chain in the IP camera market has resulted in too many vendors selling IP cameras. We are not sure about how *insecam* gets the manufacturer information of an IP camera or whether such information is correct. But we observe that the access URL to video feeds of an IP camera could be used for fingerprinting the manufacturer information. For instance, `axis-cgi/mjpg/video.cgi`, the substring of such a URL, indicates that a camera is manufactured by `Axis`. We manually inspected several pieces of manufacturer information provided by *insecam* and verified that they appear correct. We provide the distribution of those *insecam* IP cameras by manufactures in Figure 5(b). Among the 20,923 IP cameras with the manufacturer metadata information, the two manufacturers `Defeway` and `Axis` dominate the cameras, occupying 29% and 22.7%, respectively. Most other manufacturers occupy no more than 5% each.

5.4 TCP/UDP Ports Used by *Insecam* Cameras

We also examined on which port an *insecam* IP camera is working. Figure 6(a) provides the top 10 most used ports by *insecam* IP cameras. The top 10 ports are 80-84, 8000, 8080-8082, and 60001. Port 80 (HTTP) is the most used port by IP cameras to communicate to their administrative interface, occupying 32.8%. The uncommon port 60001 comes second, occupying about 15%. Further examination

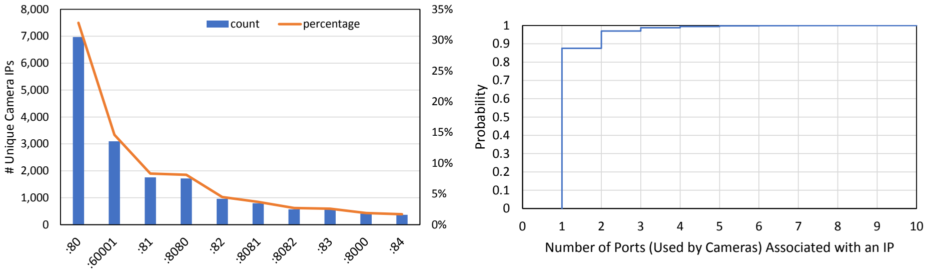

Fig. 6: (a) Top 10 ports used by *insecam* cameras. (b) CDF of the number of ports per IP address of *insecam* cameras.

reveals that 96.5% of *insecam* cameras using port 60001 are `Defeway` cameras, which is interesting since the port seems to have the power of fingerprinting the manufacturer of an IP camera and thus could be exploited by miscreants.

One IP address could be associated with multiple IP cameras, with each one using a different port. Figure 6(b) gives the cumulative distribution function (CDF) of the number of ports used by IP cameras (i.e., the number of *insecam* IP cameras) associate with one IP address. It shows that 87.5% IP addresses are connected with only one IP camera, about 10% IP addresses are associated with two IP cameras, and 3% IP addresses are connected with three or more IP cameras. Note that the results represent a lower bound of the number of IP cameras associated with an IP address, since it is quite probable that an IP address is indeed connected with multiple cameras but only one IP camera is known by *insecam*.

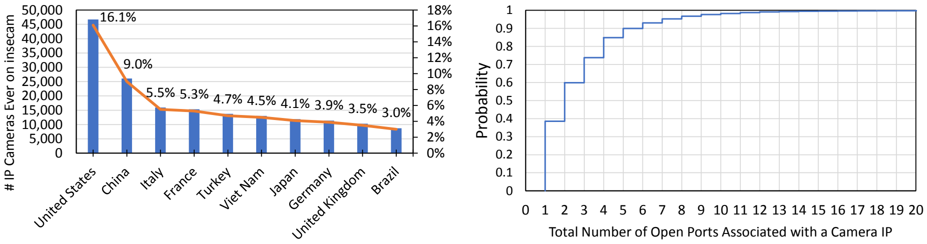

Fig. 7: (a) Top 10 countries ever contributing the most IP cameras on *insecam*. (b) CDF of the number of ports per IP address of *insecam* cameras.

5.5 Exhaust Historical IP Cameras Ever Posted on *Insecam*

In addition to the currently available and active IP cameras on *insecam*, we manage to exhaust or at least very close to collect all the history records of IP cameras ever appearing on *insecam*. We were able to collect the metadata information for 290,344 IP cameras (28,386 active ones included), and present the distribution of those cameras by country in Figure 7(a).

The figure shows the top 10 countries which have the most IP cameras ever disclosed on *insecam* since the creation of *insecam* in September 2014. We can see that 9 out of the 10 countries have had more than 10,000 vulnerable IP cameras posted by *insecam*. `United States` still tops the list, with more than 45,000 IP cameras ever posted. `China` comes second, with more than 25,000 IP cameras ever listed on the site, which is quite strange given our current observation that only 188 *insecam* IP cameras on average at any specific time are from `China`. It is still unknown why there is a huge decrease in the number of IP cameras from `China` on *insecam*. One clue is that the *insecam* administrator points out two ways out for an IP camera, which are either contacting him to remove IP cameras from *insecam* or simply setting the password of the camera. Compared with the current top 10 countries shown in Figure 4(a), `Viet Nam` and `Brazil` also appear in the top 10 countries which contribute the most vulnerable cameras on *insecam* in the past several years.

6 Vulnerability Analysis of Internal Network of IP Cameras

In addition to the vulnerability of no password protection, we would like to explore other possible vulnerabilities of those *insecam* IP cameras from the perspective of a real attacker. To this end, we first utilized an IP scanning tool [1] with an attempt to discover the hidden hosts and services co-residing in the same internal network as the vulnerable IP cameras. Specifically, the tool sends probes to an IP address and returns information including 1) whether the host is up, 2) responding TCP and UDP port numbers, 3) the services and their versions behind open ports, and so on. We may run the tool on an IP address multiple times to make sure that the host is not down so that we can gather the relevant information.

6.1 Open Ports

Number of Open Ports per IP Address. We first examine the open ports associated returned for an IP address. Figure 7(b) depicts the CDF of the number of open ports associated with the IP address of an IP camera. We can see that an IP camera often has several other open ports. Specifically, 38.5% IP addresses seems to be exclusively used for IP cameras; more than 60% IP addresses have at least two open ports; about 40% IP addresses have three or more open ports; about 10% IP addresses have at least 6 open ports. On average, an IP address has 3 open ports. 31 IP addresses have more than 100 open ports, and 14 IP addresses have more than 200 open ports.

Remote Access Ports. In addition, we paid special attention to the services (mainly `SSH` and `TELNET`) which tend to be exploited by attackers for malicious activities such as DDoS attacks. `Mirai`, the `IoT`-based botnet that took the Internet by storm in late 2016, was found to harvest bots by sending probes on TCP ports 22 (`SSH`) and 23 (`TELNET`) [14]. In our test, 22.4% of alive hosts (i.e., responding to pings) have ports 22 and/or 23 open. These remote access ports make those IP cameras vulnerable to the `Mirai`-like attacks.

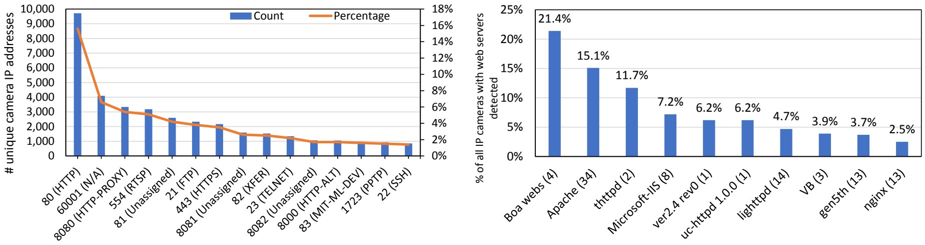

Fig. 8: (a) Top 15 most common open ports on the host of an *insecam* camera. Words in parentheses denote the corresponding protocols or services running on the ports. (b) Top 10 most popular web servers of *insecam* IP cameras. Numbers in parentheses denote the number of web server versions.

Most Common Open Ports. Figure 8(a) shows the top 15 most common open ports on the host of an *insecam* IP camera. Compared to Figure 6(a), there are many more kinds of port numbers (services) commonly accessible on the IP camera host, such as 21 (`FTP`), 22 (`SSH`), 23 (`TELNET`), 443 (`HTTPS`), 554 (`RTSP`), and 1723 (`PPTP`). Some services are directly related to IP cameras, including `HTTPS`, `RTSP`, and `PPTP`, while some services could be easily exploited by attackers as a pivot point to the internal network, such as `FTP`, `SSH`, and `TELNET`, especially when the co-residing IP cameras could be directly accessed due to no password protection.

6.2 Web Servers

With the help of the IP scanning tool, we are able to detect a total of 300 different versions of web servers use by 2,564 IP cameras. The different versions of web servers were then aggregated to the web server software. Figure 8(b) shows the top 10 web server software used by IP cameras. Numbers in parentheses denote the number of web server versions used. Specifically, four different versions of `Boa` web server software are used most, about 21.4%. `Apache HTTP` server is also prevalent, and up to 34 versions were used by 15.1% IP cameras. The `thttpd` web server software comes third, with 11.7% rate.

Furthermore, we studied the release dates of the popular versions of web servers as well as the number of known `CVE` (Common Vulnerabilities and Exposures) vulnerabilities contained in them. We found that nearly all those cameras were running extremely old and vulnerable web server software. For example, the most popular web server software, `Boa`, has been discontinued since 2005 [3]. Most popular web servers have been found to bear a significant number of `CVE` vulnerabilities. Specifically, all 34 versions of `Apache HTTP` server have 3 to 49 vulnerabilities, and 19 vulnerabilities on average [2]. All the two thttpd web server versions contain 2 to 3 vulnerabilities. All 8 Microsoft IIS versions contain 1 to 9 vulnerabilities, and 5 on average. 84.6% (11 out of 13) nginx web server versions used have 1 to 3 known vulnerabilities. Such vulnerabilities could include authentication bypass vulnerability, cross-site scripting (XSS) vulnerability, buffer overflow, directory traversal, and many other vulnerability types. They allow attackers to gain administrator access and execute arbitrarily malicious code on IP cameras and other internal network devices.

7 Related Work

Previous studies on IP cameras are the most related works. Stanislav et al. [19] conducted a case study on baby monitor exposures and vulnerabilities. They found that most vulnerabilities and exposures are trivial to be exploited by a competent attacker and can only be effectively mitigated by disabling the device and applying a firmware update. Albrecht et al. [12] presented a real-world hacking incident that the baby monitor was hacked and then turned on the owners, and provided precautions to reduce the chance of getting hacked. Campbell [16] focused on the vulnerability analysis of the authentication mechanisms of IP cameras, discussed potential attacks, and presented mitigation solutions. Costin [17] reviewed the threats and attacks against video surveillance systems at different levels and provided a set of recommendations to increase the security of those systems. Nearly all the above works aim to provide a good summary of existing attacks and possible mitigation solutions, but none of them conduct a deep, large-scale quantitative analysis of vulnerable IP cameras as we do. Also, our work performed vulnerability analysis of the surrounding environment of IP cameras, including open ports and services in the same internal network and the web server software used, which is not seen in previous work.

Many other works studied security issues in general IoT systems or in other IoT devices. Amokrane [13] reviewed security challenges and attack surface in IoT. The author showcased the accessibility of IoT attack surface with several real-world cases on exploitation and attacking IoT devices. Apthorpe et al. [15] investigated the privacy vulnerability of encrypted IoT traffic and found that the network traffic rate of IoT devices can reveal user activities even when the traffic is encrypted. Rotenberg et al. [18] performed an evaluation of authentication bypass vulnerabilities in SOHO (Small Office/Home Office) routers and found that a significant number of routers could be potentially taken control over by attackers due to misconfiguration issues. Our work focuses on estimating the magnitude of vulnerable IP cameras and characterizing them.

8 Conclusion

IP cameras have come prevalent in our everyday lives. The need for comprehending and solving various security and privacy issues surrounding IP cameras has become pressing. Our work represents one of such efforts. In this paper, we conducted a large-scale comprehensive measurement study of IP cameras without password protection. We collected data from *insecam*, the world biggest directory of live IP cameras without password protection. We first studied the dynamics of the site, then performed a detailed characteristic analysis on those IP cameras, and finally conducted vulnerability analysis of the internal networks where IP cameras reside. Our work produces a series of interesting findings, which are expected to provide valuable knowledge of the current threat landscape that IP cameras are facing.

Acknowledgement. We would like to thank our shepherd `Mark Gondree` and anonymous reviewers for their insightful and detailed comments. This work was partially supported by `Microsoft Research Asia`, `CCF-NSFOCUS Kunpeng Research Fund`, and `Alipay Research Fund`. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agencies. The co-author `F. Xu` is the contact author.

References

1. Angry IP Scanner. `http://angryip.org/`.
2. Apache web server CVE vulnerabilities. `https://goo.gl/FaWh8y`.
3. Boa (web server). `https://goo.gl/6d251V`.
4. Breaking Down Mirai: An IoT DDoS Botnet Analysis. `https://goo.gl/7VcfMh`.
5. DB-IP: IP Geolocation and Network Intelligence. `https://db-ip.com/`.
6. How Many Time Zones Are There? `https://goo.gl/fWwFxQ`.
7. Insecam - World biggest online cameras directory. `http://www.insecam.org/`.
8. Insecam Displays Unsecured Webcams Worldwide. `https://goo.gl/hBqpni`.
9. The Botnet That Broke the Internet Isn't Going Away. `https://goo.gl/VqFi7f`.
10. Webcam 'creepshot' pictures shared on Reddit. `https://goo.gl/ffKtTK`.
11. Website spies on thousands of people. `https://goo.gl/SdbVcc`.
12. K. Albrecht and L. Mcintyre. Privacy nightmare: When baby monitors go bad [opinion]. *IEEE Technology and Society Magazine*, 34(3):14–19, 2015.
13. A. Amokrane. Internet of things: Security issues, challenges and directions. *C&ESAR 2016*, page 70, 2016.
14. M. Antonakakis and others. Understanding the mirai botnet. In *USENIX Security'17*.
15. N. Apthorpe, D. Reisman, and N. Feamster. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805*, 2017.
16. W. Campbell. Security of internet protocol cameras–a case example. 2013.
17. A. Costin. Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. In *TrustED*, pages 45–54. ACM, 2016.
18. N. Rotenberg, H. Shulman, M. Waidner, and B. Zeltser. Authentication-bypass vulnerabilities in soho routers. In *SIGCOMM Posters and Demos*, 2017.
19. M. Stanislav and T. Beardsley. Hacking iot: A case study on baby monitor exposures and vulnerabilities. *Rapid 7*, 2015.