Flow-based detection of RDP brute-force attacks

Martin Vizváry

vizvary@ics.muni.cz

Institute of Computer Science
Masaryk University
Brno, Czech Republic

Jan Vykopal

vykopal@ics.muni.cz

Institute of Computer Science
Masaryk University
Brno, Czech Republic

Abstract

The Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a remote access to a computer over a network connection. Recently, we have seen an increase in attacks on Microsoft Windows remote desktop connection authentication. Current detection methods are based on event log analysis or the Account Lockout Policy used in Windows domain networks. However, the methods are applicable only in environment where the devices are under control of the network administrator.

We propose attacks detection method based on the network-based approach which provides host independency and highly scalability. The network flow data provides sufficient information about communication of two nodes in network, even though the communication is encrypted.

Currently we are able to determine whether a detected IP flow is ordinary remote desktop session or single authentication with a small ratio of false-positive detection. An analysis was based on the network flow data collected in the Masaryk University network and host-based data from logs of a server with opened Remote Desktop Connection. These data helped us to improve the flow detection using the information gathered from the server event log. Despite the fact that RDP is encrypted, flow data gives us a sufficient amount of information to determine whether the connection is an authentication or regular remote desktop session.

We implemented the attacks detection as a plugin for the widely used NfSen collector. The plugin is involved in the active defense of the network of Masaryk University. In two months, the plugin detected nearly two million of authentication attempts and reported 3,430 RDP authentication attacks. Despite the fact that attackers IP address was blocked for two days, many of them continued or repeated the attack after the block had been lifted. An analysis of the frequency with which the attackers returned, suggests the suitable duration of settings of blocking of attackers.

Keywords: Remote Desktop Protocol, RDP, brute-force attack, intrusion detection, NetFlow, NfSen, bidirectional flow, dictionary attack.

1 Introduction

Both brute-force and dictionary attacks are aimed at a wide-spread knowledge-based authentication. In both cases, attackers suppose that users choose their passwords from a small subset of the full password space, e. g., short passwords, dictionary words, proper names, and lowercase strings [1]. The attackers attempt to login to user accounts by trying possible passwords until they find the correct one. If the attackers use a predefined list of common passwords, they conduct dictionary attack, otherwise they systematically search entire space of passwords using brute-force attack. In this paper, we use the term brute-force attack for both types of attacks since we cannot distinguish them at flow level because it does not provide any information about the packet payload.

In our previous work [2], we focused on brute-force attacks on the popular SSH service but currently we have been observing an increase in attacks on the authentication of the Remote Desktop Protocol (RDP). It is a Microsoft proprietary protocol used for remote desktop connection for Windows operating systems. Since Windows XP, the systems provide not only client but also server (denoted as *Remote Desktop Connection* and *Remote Desktop Services)* that is often left unsecured by unskilled users. This causes a growing number of brute-force attacks on remote desktops. For instance, *Morto* [3] represents a recent example of a worm that spreads by remote desktops secured by weak passwords.

Current detection and prevention of brute-force attacks on RDP is done at the host level. The detection is based on an event log analysis: if a number of unsuccessful login attempts exceeds a predefined threshold, the attack is reported and the attacker may be blocked by a host firewall. For attack prevention, Account Lockout Policy is often used in networks of devices under control of the network administrator.

In this paper, we describe a design (Section 2) and evaluation (Section 3) of a network-based detection of brute-force attacks on authentication of Microsoft Windows RDP. Similarly to [2], we analyze both legitimate and malicious RDP traffic. As a result, we derive flow-based signatures of traffic generated by RDP attacks. In contrast to [2], we benefit from the use of bidirectional flows (biflows) that provide a natural view of interactive client-server communication. We evaluate the detection in the 10 gigabit campus network of Masaryk University, Brno, Czech Republic including hundreds of RDP servers.

2 Design of the flow-based signature of RDP authentication

To derive the flow-based signature, we analyze RDP traffic both at host and network level. We use Microsoft Windows Server 2008 with RDP server that is backward compatible with lower versions of clients. To acquire authentication signatures of the most widely used clients for remote connection, we choose three desktop clients for Windows 7, Windows XP, Ubuntu 12.40 and two mobile clients for Android 2.3, iOS. Next, we analyze two tools used for brute-force attack and a worm called *Morto* [3]. These signatures are revisited in further analysis conducted in the entire campus network of Masaryk University. Finally, we thus derived the general flow-based signature of RDP authentication.

2.1 Traffic analysis of RDP clients

We analyze a flow signature of several clients used for connection to the remote desktop. Table 1 shows flow records of the client in Windows 7. The authentication process of the client works with very low bandwidth requirements. The whole authentication fits in several packets and every authentication attempt forms two separate flows. Every authentication attempt does fit in two flows. The actual remote desktop session is started after the successful authentication. The two flows lasting 0.8 seconds represent canceled connection right after the successful authentication. The last two long-lasting flows contain the actual session. There is also a large increase in number of packets and bytes transferred in contrast to the authentication.

Duration [s]	IP address		TCP flags	Number of	
	Source: port	Destination: port		Packets	Bytes
0.126	A: 27631	B: 3389	AP.SF	8	1704
0.126	B: 3389	A: 27631	APRS.	9	1506
0.128	A: 27634	B: 3389	AP.SF.	8	1704
0.127	B: 3389	A: 27634	APRS.	8	1466
0.845	A: 29908	B: 3389	AP.SF	20	3560
0.843	B: 3389	A: 29908	APRS.	19	2783
75.081	A: 27635	B: 3389	AP.SF	684	101941
75.080	B: 3389	A: 27635	APRS.	678	217802

Table 1: Flows acquired during connection from a Windows 7 client
TCP flags: A – ACK; P – PUSH; R – RESET; S – SYN; F – FIN

Table 2 shows flow records of the client running on Windows XP with Service pack 3 installed. In contrast to the client for Windows 7, the authentication process is a part of the remote session, i. e., the credentials are entered in the login prompt on the remote desktop. The first two flows in Table 2 are authentication attempts using incorrect passwords. All authentication attempts are in one network flow. There are more transferred packets in one flow so the authentication have the same flow signature as regular remote desktop connection. The last flow is flow signature of work on the remote desktop. To detect, whether the connection is brute-force attack or a short legitimate session of remote desktop, is not possible. The flow with duration of 3 seconds is canceled connection right after the successful authentication. The *rdesktop* client in Ubuntu and both mobile clients have similar flow signature as the client in Windows XP. The difference in signatures is only in the volume of the traffic. Neither the *rdesktop* client, nor mobile clients have as good traffic optimization as the client in windows.

Duration [s]	IP address		TCP flags	Number of	
	Source: port	Destination: port		Packets	Bytes
15.740	A: 10067	B: 3389	AP.SF	167	12582
17.738	B: 3389	A: 10067	APRS.	190	113750
3.133	A: 10250	B: 3389	AP.S.	51	6999
3.133	B: 3389	A: 10250	APRS.	55	28008
61.756	A: 10140	B: 3389	AP.SF	507	41601
61.754	B: 3389	A: 10140	APRS.	586	343475

Table 2: Flows acquired during connection from a Windows XP SP3 client

2.2 Traffic analysis of tools for brute-force attacks

We also analyzed other tools that can be used for brute-force attacks on RDP. We tested the *xTSCrack* [4] tool for Windows platform and *Ncrack* [5] for Linux systems. The flow signature of the *Ncrack* is shown in Table 3. The signature of the *xTSCrack* is very similar to the signature of the *Ncrack.* The only difference is the volume of traffic due to lower client optimization in Linux system. The first four lines in the table are two unsuccessful authentication attempts. One login and password combination per remote session forms a separate couple of flows. In contrast, the authentication from regular clients is a part of one flow, except the client in Windows 7. The last two flows describe the signature of successful authentication. The differences between successful and unsuccessful authentication are not compelling enough to be able to reliably determine whether the attack is successful or not.

Duration [s]	IP address		TCP flags	Number of	
	Source: port	Destination: port		Packets	Bytes
1.772	A: 17090	B: 3389	AP.SF	87	6138
1.773	B: 3389	A: 17090	APRS.	139	170028
2.491	A: 17121	B: 3389	AP.SF	75	5528
2.491	B: 3389	A: 17121	APRS.	139	177910
1.474	A: 17131	B: 3389	APRSF	99	7273
1.416	B: 3389	A: 17131	APRS.	142	160827

Table 3: Flows acquired during connection from a *Ncrack* tool

Table 4 shows flow records of the worm called *Morto.* We used a test bed with three virtual machines – a victim, a host infected with the worm (i. e., attacker) and a NetFlow probe. There are three login attempts. First two flows are unsuccessful login attempts and the last flow is successful attempt with infection of the remote system. After successful connection the worm copies itself to the new system and continues spreading through the network.

Duration [s]	IP address		TCP flags	Number of	
	Source: port	Destination: port		Packets	Bytes
2.404	A: 1727	B: 3389	AP.SF	76	6768
2.403	B: 3389	A: 1727	APRS.	96	9934
2.404	A: 1728	B: 3389	AP.SF	76	6488
2.405	B: 3389	A: 1728	APRS.	96	9940
7.269	A: 1729	B: 3389	AP.SF	216	153284
7.269	B: 3389	A: 1729	APRS.	262	27454

Table 4: Flows acquired during attack from a worm *Morto*

2.3 Flow-based signature of authentication

The results of the analysis give to us enough information to derive the NetFlow signature of the process of authentication. During the analysis we do not find any evidence that the client in Windows 7 or a tool with similar signature of flow are used for a brute-force attack. The use of other clients will not be very effective because the remote session is closed by server after several unsuccessful authentications. Attacking tools and the worm have very similar behavior. In contrast to proper clients, every authentication attempt is in separate flow therefore we are able to determine the number of attempts. The clients can be divided into two categories. The first category in which belongs only the client in Windows 7 uses optimized authentication and the remote desktop connection is opened only if the previous authentication was successful. The second category covers all other clients and the authentication process takes place on the remote desktop.

From the given flow signatures and the differences in direction of the communication in flow, we decide to use bidirectional flows. The client requests and the server responses are linked in one biflow record. As opposed to using unidirectional flows, biflows enable us to distinguish more accurately between the legitimate and malicious traffic. The final signature is generalized over all clients and all tools that we analyzed.

The flow-based signature of the RDP authentication attempt uses the following six features:

- *in packets* – the number of the incoming packets – <20, 100>,
- *in bytes* – the volume of the incoming traffic in Bytes – <2200, 8001>,
- *out packets* – the number of the outgoing packets – <30, 190>,
- *out bytes* – the volume of the outgoing packets – <3000, 180000>,
- *flags* – TCP flags – ACK, PUSH, RESET, SYN,
- *dst net* – the address of the local network.

Since we deploy attack mitigation based on the detection using this signature in the production network, we use three additional conditions based on measurements presented in [6] to lower false positives:

- attacker used a TCP SYN scan technique[1] of network reconnaissance before the actual brute-force attack,
- time factor of attack, i. e., the time distance of the attack and the network reconnaissance is lower than a predefined value,
- at least three authentication attempts per server and at least three attacked servers at the same time.

If all these conditions hold, the source IP address of the attacker is reported.

3 Evaluation of the flow-based detection signature

To evaluate the accuracy of the derived flow-based signature, we analyzed NetFlow data acquired in the large campus network of Masaryk University from October 1 to November 30, 2012. To automate the detection of the RDP attacks in the campus network, we implemented RdpMonitor [7], a publicly available NfSen plugin that uses the derived NetFlow signature. The plugin monitors the network traffic, collects attack data and reports detected incidents via e-mail.

During the two months the plugin has detected 3,430 attacks originating from 2,057 unique IP addresses and has collected 1,845,740 login attempts. If we take into account the average size of the authentication attempt and the number of login attempts, we get 140 GB of this malicious traffic. Hence, we estimate that approximately 40 % of all RDP related traffic in the campus network is malicious. Next, we analyze user names collected in the event log of the server used as a simple honeypot. The most frequently used user names were: *administrator; admin; user; test; user1 and user2*. We found out that 60 % of attacks captured by the honeypot used the same sequence of user names which is used by the worm *Morto.* We assume that the attacks in the campus network share the same pattern.

[1] TCP SYN scan – attacker starts with TCP handshake and waits for response after which resets the connection

Furthermore, we analyzed the behavior of attackers which were detected and blocked on the edge of the campus network. To mitigate brute-force attacks and to protect the entire network, we block the IP address of the attacker for two days. Due to the restrictions of the technology used for blocking we have not been able to block attackers for a longer time. In the two months, we blocked on average 56 source IP address a day and observed that some of them return back after the block expired. Therefore, we assigned all attackers to three groups: those blocked 2 times, 3 times and more than 3 times. For each group of attackers, we computed the intervals between two blocking of an IP address. Figure 1 depicts clusters of intervals between the time when attackers were unblocked and the time when they attacked our network again (one point corresponds to one interval). The more dense cluster is, the more attackers returned in the specific time interval. The most attackers returned in twenty days and the average time of their return was 10 days. If we had extended the period of blocking to 12 days, we would have prevented 1,100 attacks. Consequently, we would have prevented attackers to conduct malicious activities in the campus network and would have lowered the possibility of successful attack.

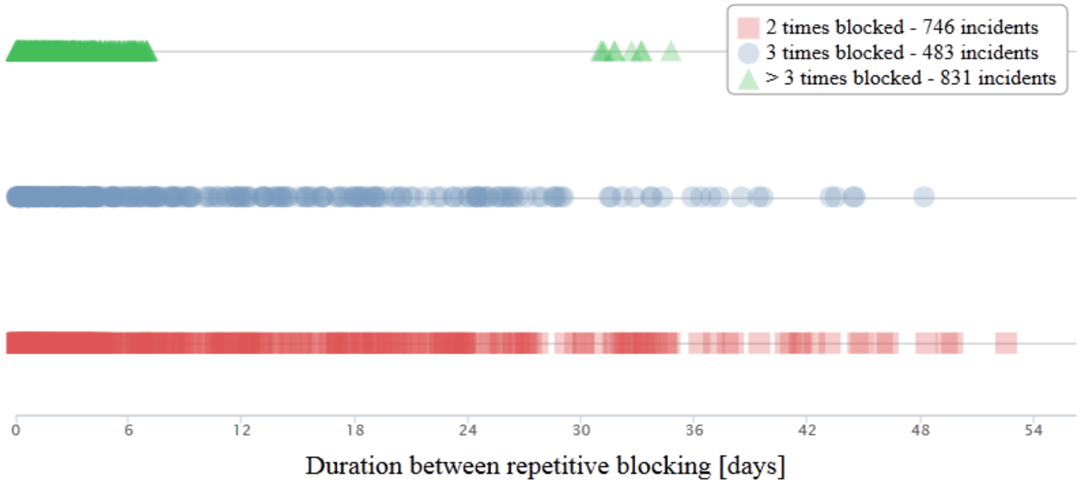

Figure 1: Time between repetitive blocking of attackers on the edge of the campus network

Last but not least, we compared the total number of detected brute-force attacks on RDP and SSH, respectively. In the two months, we detected 111 brute-force attacks on authentication of SSH in contrast to 3,430 attacks on RDP.

4 Conclusions

Currently, detection of online brute-force attacks on RDP authentication is done at host level. In spite of the fact that network-based detection offers advantages such as scalability or better capability of detecting distributed attacks, we were not aware of any network-based or even flow-based method of detection of RDP attacks. We analyzed network flows acquired during RDP authentication of various clients and proposed the general signature for detection of RDP brute force attacks. The proposed signature benefits from bidirectional flows since brute-force attacks consist of interactive communication between two parties. In addition, we are able to detect the authentication attempts even though the protocol is encrypted. The detection based on this signature was evaluated in the 10 gigabit campus network of Masaryk University network connecting about 15,000 hosts.

We dealt not only with the attack detection itself but also with eliminating of false positives since this is crucial for consecutive attack mitigation. Since a decision based on incorrect results of intrusion detection negatively affects benign users, a fundamental requirement for operational use of the detection is zero false positive rate even with the risk of false negatives. We therefore used three additional conditions for lowering false positives based on the study of attackers' behavior. The first condition requires that brute-force attacks are preceded by network reconnaissance probes. The second one assumes that the majority of attacks is non-targeted and thus it hits more than one server. Finally, the third condition takes into account a time factor of the whole attack.

The signature-based detection of brute force attacks on RDP with the additional conditions of lowering false positives had been already deployed in routine operation by CSIRT-MU, Computer Security Incident Response Team of Masaryk University, in 2012. The detection method was successfully implemented as a publicly available plugin for the NfSen collector [6]. Since the time, thousands of attacks with almost zero false positive rate have been mitigated and reported. In addition, this successful prototype was transferred to a university spin-off company and became a part of a successfully sold product.

In future work, we would like to analyze the impact of various values of thresholds of additional conditions to false positive rate and the impact of changes in duration of blocking to attackers' behavior.

References

[1] Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, and R. L. Rivest. Handbook of Applied Cryptography, chapter Identification and Entity Authentication. CRC Press, 1997.

[2] VYKOPAL, Jan, Tomáš PLESNÍK and Pavel MINAŘÍK. Network-based Dictionary Attack Detection. In Proceedings of International Conference on Future Networks (ICFN 2009). Los Alamitos, CA, USA: IEEE Computer Society, 2009. p. 23-27, 5 pp. ISBN 978-0-7695-3567-8.

[3] F-secure. Worm:W32/Morto.A analysis. URL http://www.f-secure.com/v-descs/worm_w32_morto_a.shtml

[4] xTSCrack web site. http://atrixteam.blogspot.cz/2012/09/updated-news.html

[5] Ncrack – High-speed network authentication cracker web site. URL http://nmap.org/ncrack

[6] VYKOPAL, Jan. A Flow-Level Taxonomy and Prevalence of Brute Force Attacks. In Advances in Computing and Communications. Berlin: Springer Berlin Heidelberg, 2011. p. 666-675, 10 pp. ISBN 978-3-642-22714-1. doi:10.1007/978-3-642-22714-1_69.

[7] RdpMonitor web site. http://www.muni.cz/ics/services/csirt/tools/rdpmonitor.