# Security Analysis and Monitoring Assessment of Networked Printers: A Report

Quanbo Pan,[1,2,3] Shengbao Li,[2,3] Na Li,[3] Peiying Zhang,[1,4] and Lizhuang Tan[1]

[1]*Key Laboratory of Computing Power Network and Information Security, Ministry of Education, Shandong Computer Science Center (National Supercomputer Center in Jinan), Qilu University of Technology (Shandong Academy of Sciences), Ji'nan 250014, China*

[2]*School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China*

[3]*Shandong Branch of National Computer Network Emergency Response Technical Team/Coordination Center (CNCERT/SD), Ji'nan 250002, China*

[4]*College of Computer Science and Technology, Qingdao Institute of Software, China University of Petroleum (East China), Qingdao 266580, China*

Email: tanlzh@sdas.org

In this letter, we give a comprehensive and detailed introduction to the current security risks faced by networked printers, explain the security monitoring platform and attack detection method, and analyze the actual monitoring results. In particular, the most comprehensive feature knowledge database for networked printer is organized and published.

*Introduction:* In recent years, network security threats faced by networked printers have become increasingly severe[1]. Different from traditional printers, networked printers often have built-in operating systems, storage devices and IP protocol stacks. They are usually connected to the network environment as independent network nodes. Attackers can launch attacks on printers through remote penetration[2]. At the same time, there are many hidden dangers in networked printer security vulnerabilities, and they are often neglected in management[3]. Networked printers usually carry sensitive data of governments, enterprises, and individuals. Once hacked, it can easily lead to serious consequences of information theft.

This letter reports on the related technologies for networked printers and latest network security risks[4]. Firstly, it summarizes and introduces the mainstream networked printing architecture and technology, and then makes a detailed analysis of various risks and hidden dangers of networked printers. Secondly, the most complete feature knowledge database for networked printer is organized and published. Finally, a security monitoring system and attack detection methods are introduced, and we use the rule/feature-based matching to detect single-step attacks and the subgraph matching to diagnose multi-step attacks.

*Networked Printing:* Networked printers are connected to the LAN or the Internet as independent devices. End users directly access and use the target printer through the network to perform various operations, including checking the printer status, sending printing instructions, and transferring printing files, etc.

Networked printing technology includes networked printing protocols and printer languages, as shown in Fig.1. The former is used to establish a network connection between the user and the printer, and the latter is used to complete specific operations and printing tasks.

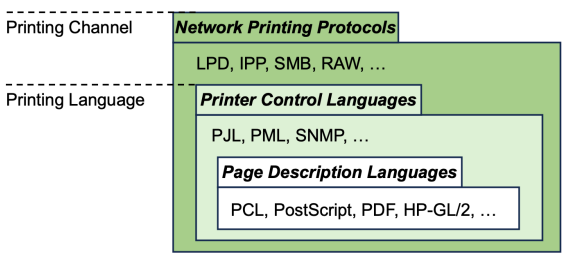


**Fig 1** *The composition of the networked printer protocol.*

The industry has formed a variety of networked printing protocols dominated by different manufacturers and organizations. On the Windows OS, the SMB/CIFS printing protocol introduced by Microsoft is the mainstream, and the more common protocols include LPD, IPP, and Raw. In recent years, some printers have built-in private cloud printing protocols.

Printer languages are divided into two categories, printer control language and page description language. The more popular printer control language standards include Printer Job Language (PJL) from HP, Common Peripheral Controlling Architecture (CPCA) from Canon, EJL from Epson, etc. Page description language is used to define and describe the actual printed document, such as Printer Command Language (PCL) from HP and PostScript from Adobe. The former is streamlined and difficult to attack.

*Security Analysis:* As a device that can operate independently on the Internet, a networked printer has a complete built-in operating system, command interpreter and other applications. While providing printing services, it also exposes multiple specific network ports to the outside world. The printer language allows visitors to obtain high-risk operation permissions. Compared with traditional computer networks, some network protocols and language standards of printers were not designed with security features in mind and have security flaws.

As shown in Fig. 2, the types of cyberattacks and security risks targeting networked printers are:

(1) **Denial of Service**[1]

a) **Port Blocking**: The attacker continuously initiates requests to TCP port 9100, causing normal print requests to fail to respond.

b) **Resource Consumption**: Time-consuming or resource-consuming operations occupy a large amount of printer resources, such as the infinite loop feature of PostScript, uploading font files of PCL, etc.

c) **Physical Damage**: The attacker frequently performs write operations on non-volatile RAM memory using PJL or PostScript until the RAM is physically damaged.

(2) **Over Permission**

a) **Factoryreset**: The attacker remotely sends the printer settings to restore the factory mode, causing all security configurations (e.g., management passwords) to become invalid, thereby gaining full operating permissions.

b) **Backdoor**: Some printers have built-in backdoors that could allow attackers to gain maximum operating privileges. For example, an attacker can obtain and modify the Kyocera 3830 printer system settings by constructing a packet starting with "!R!SIOP0".

(3) **Information Disclosure**

a) **Memory Leak**: The Attacker uses proprietary PJL commands to read and write RAM on some Xerox printers.

b) **File System Access**: The Attacker performs file system operations using PostScript and PJL.

c) **Password Cracking**: The Attacker obtains PJL and PostScript passwords by brute-force attacks.

(4) **Code Execution**

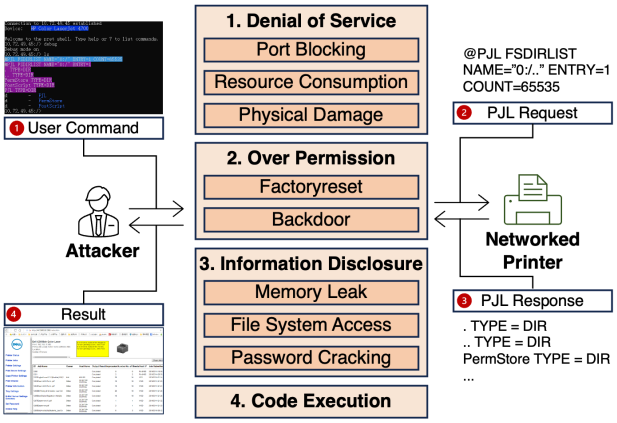


**Fig 2** *Networked printer security threats.*

We simulate normal printer communication or intrusion attacks, and

*Table 1. Feature Knowledge Database for Networked Printer*

| Type | Brand | *Model*/Function | Protocol | Feature rule |
|---|---|---|---|---|
| Fingerprint | HP | *P1102w* | HTTP | SSI/index.htm P1102w |
| | HP | *P377dw MFP* | HTTP | Server:HP HTTP Server; HP PageWide 377dw MFP - J9V80B |
| | Lexmark | *E352dn* | HTTP | /cgi-bin/dynamic/config/config.html |
| | Lexmark | *MX310dn* | HTTP | cgi-bin/dynamic/topbar.html MX310dn |
| | Canon | *All* | HTTP | Server:CANON HTTP Server |
| | RICOH | *MP4001* | HTTP | server:Web-Server/3.0 title:Web Image Monitor |
| | RICOH | *MP7503* | HTTP | webArch/mainFrame.cgi MP 7503 |
| | Brother | *MFC-L6900DW* | HTTP | general/status.html MFC-L6900DW |
| | Brother | *DCP-L2540DW* | HTTP | general/status.html DCP-L2540DW |
| | Dell | *C2665dnf Color MFP* | HTTP | inurl:framelogo.htm C2665dnf |
| | Dell | *C2330dn Laser Printer* | HTTP | inurl:framelogo.htm 2330dn |
| | Samsung | *SCX-483x* | HTTP | sws/app/information/home/home.json SCX-483x |
| | Samsung | *SCX-4x24 Series* | HTTP | sws/app/information/home/home.json SCX-4x24 |
| | FUJI XEROX | *C3350* | HTTP | default.htm C3350 |
| | FUJI XEROX | *M225* | HTTP | default.htm M225 |
| | Konica | *C284* | HTTP | wcd/system_device.xml C284 |
| | Konica | *C458* | HTTP | wcd/system_device.xml C458 |
| Attack | HP | Remote scanning | HTTP | /#hId-pgWebScan |
| | All | DDoS attack 1 | TCP | SERVICEMODE=HPBOISEID |
| | All | DDoS attack 2 | TCP | JOBMEDIA=OFF |
| | All | Restart 1 | TCP | 1.3.6.1.2.1.43.5.1.1.3.1 |
| | All | Restart 2 | TCP | 040006020501010301040106 |
| | All | Erase NVRAM | TCP | @PJL DEFAULT COPIES |
| | All | Change Password | TCP | DEFAULT PASSWORD |
| | All | Upload files | TCP | @PJL FSDOWNLOAD FORMAT:BINARY SIZE |
| | All | Tampering with page numbers | TCP | @PJL SET PAGES |
| | All | Print interception | TCP | @PJL SET HOLD=ON |
| | All | Buffer overflow | TCP | @PJL INQUIRE 00000000000000000000000000000000 |
| | All | Get status information | TCP | @PJL INFO STATUS |
| | All | Get model | TCP | @PJL INFO ID |
| | All | Setup information | TCP | @PJL INFO CONFIG |
| | All | Get variables | TCP | @PJL INFO VARIABLES |
| | All | Modify wifi | HTTP | tab=Networking&menu=DirectWifi |
| | All | Format memory | TCP | @PJL FSINIT VOLUME="0" |
| | All | Create a file | TCP | FSAPPEND FORMAT |
| | Lexmark | Tampering with configuration | TCP | /cgi-bin/dynamic/config/config.html |
| | Lexmark | Change Web password | TCP | admin/password.html |
| Vulnerability | All | File system access | TCP | \x1B%–12345X@PJL FSDIRLIST |
| | All | Print transfer | TCP | \x1B%–12345X@ && POSTSCRIPT |
| | All | State information leakage | TCP | @PJL INFO CONFIG |
| | All | Number of printed pages leaked | TCP | @PJL INFO PAGECOUNT |
| | All | Printed documents leaked | TCP | \x1B%–12345X@ && POSTSCRIPT |
| | All | File create | TCP | FSAPPEND FORMAT |
| | HP | Printer setting | HTTP | printer/config/gen/general.html |
| | Brother | Printer setting | HTTP | general/panel.html |
| | Konica | Printer setting | HTTP | wcd/system_device.xml |
| | RICOH | Printer setting | HTTP | websys/webArch/mainFrame.cgi |
| | Konica | Printer setting | HTTP | wcd/copy.xml |
| | All | Memory access | TCP | PJL RNVRAM ADDRESS = |
| | All | Memory write | TCP | @PJL WNVRAM ADDRESS |
| | Brother | Fax access | HTTP | fax/fax/fax.html |
| | HP | Fax access | HTTP | set_config_faxRecv.html?tab=Fax&menu=FaxRecv |
| | Lexmark | Scan access | HTTP | dynamic/printer/netscan/scanpc.html |
| | HP | Scan access | HTTP | scantoConfiguration.html |
| | HP | Email access | HTTP | info_scantoEmailSetup.html |
| | HP | Network access | HTTP | tab=Networking&menu=NetConfig |
| | HP | Cloud printing access | HTTP | tab=Networking&menu=ProxyConfig |

extract networked printer fingerprints (71), attack threats (20), and vulnerabilities (20) signature database, involving a total of 9 brands and 50 models, as shown in Tab. 1.

*Networked Printer Security Monitoring Platform:* We develop a prototype of a networked printer security monitoring platform based on the Django framework, as shown in Fig. 3. The Data Layer and Service Layer serve data collection and processing. The Visualization Layer supports the display of information such as the global distribution map of networked printers, the distribution ranking of networked printers in China, the distribution of security vulnerability types of networked printers, the time trend of the number of network security logs, the statistics of the number of networked printers, the ranking of high-risk network ports, and the real-time monitoring logs of networked printers. The

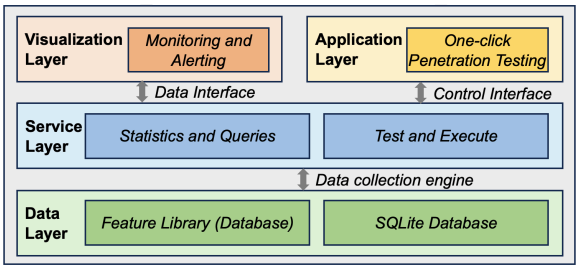


**Fig 3** *The architecture of networked printer security monitoring platform.*

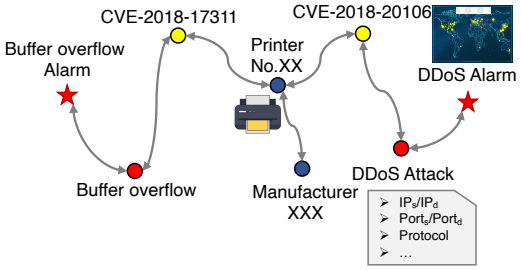


**Fig 4** *The MDATA diagram of attack detection.*

Application Layer supports penetration tests such as target network survivability test, denial of service attack test, printer internal status information acquisition test, file system arbitrary access test, LAN printer scan test, printer unauthorized restart test, etc.

*Attack Detection Model:* Consider $G = (V, E)$, where each node $v_i \in V$ represents an entity, including primary entities such as printer, brand, country, network operator, owner, and secondary entities such as model and version. The edge $(v_i, v_j)$ represents the connection between two nodes $v_i$ and $v_j$. For two connected nodes, if one node is attacked, the attacker can try to attack the other node. For each device node, according to Tab. 1, the feature set of node $v_i$ is $F(v_i) = \{f_1(v_i), f_2(v_i), ..., f_k(v_i)\}$, as shown in Fig. 4.

The types of network attacks against networked printers can be divided into single-step attacks and multi-step attacks, which are uniformly expressed as $S(i) = \{s(1), s(2), ..., s(l)\}$, Among them, each attack step can be expressed as a tuple $s_i = (IP_s, Port_s, Attack_j, IP_d, Port_d, Protocol, Time, ...)$. The set of various security alarm events $A = \{a(1), a(2), ..., a(t)\}$. Therefore, the attack detection problem can be expressed as finding all attacks $S(i)$ and the corresponding attack steps according to the alert $a(i)$.

We use the rule/feature-based matching method to detect single-step attacks and the subgraph matching algorithm[5] to find multi-step attacks that can match the detection subgraph in the real-time attack graph that satisfies spatiotemporal constraints, as shown in Algo. 1.

**Algorithm 1:** Attack Detection Algorithm

**Input:** $G = (V, E)$, Alarm Set: $A$, Detection Subgraph: $SG$.
**Output:** Attack Set: $S$.

```
Initialize list m = ∅ and MDATA node set M;
for i = 1 : length(A) do
    covert a(i) to the MDATA node M(t_i);
    if M(t_i) is the first step of SG then
        add M(t_i) to the start node of m;
    else if M(t_i) is a follow-up step of m and satisfies space
      and time constraints then
        add M(t_i) to end node of m;
    end
    if m consists SG then
        Output m as an multi-step attack;
    end
end
```

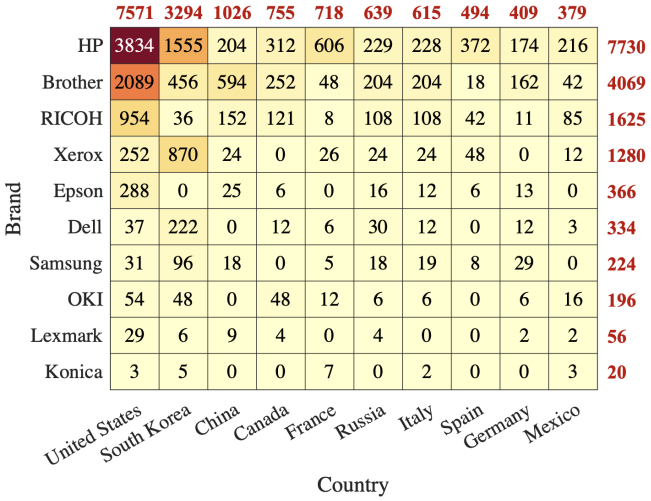


**Fig 5** *Top 10 countries and brands of printers exposed to the Internet.*

*Result Evaluation:* We assess the global security posture and Chinese attacks on networked printers. Between March 1 and March 20, 2023, we found that a total of 29,170 printers worldwide were directly exposed to the Internet. The United States and South Korea had the largest number of networked printers, with 7,571 and 3,294 printers respectively, as shown in Fig. 5. At the same time, we conducted attack detection on 1,225 focused networked printers in China, and found a total of 2,992 attacks. The main attack methods include malicious code (1,762), abnormal permission acquisition (332), password theft (148), etc.

*Author contributions:* Quanbo Pan: Conceptualization, Formal analysis, Methodology, Writing original draft. Shengbao Li: Writing-Review and Editing. Na Li: Data Curation. Peiying Zhang: Methodology. Lizhuang Tan: Investigation, Funding Acquisition, Paper review.

*Conflict of interest statement:* The authors declare no conflict of interest.

*Data availability statement:* The data that support the findings of this study are openly available in www.tanlizhuang.cn/data.html.

*Acknowledgments:* This work was supported in part by the Shandong Provincial Natural Science Foundation under Grant No. ZR2023QF025, No. ZR2022LZH015 and No. ZR2023LZH017, and the Innovation Project of Qilu University of Technology (Shandong Academy of Sciences) under Grant No.2023PX057 and No.2023RCKY141.


*Received:* 17 October 2023

## References

1. Müller, J., et al.: Sok: Exploiting Network Printers. In: Proceedings of IEEE Symposium on Security and Privacy, pp. 213–230. IEEE (2017)
2. McCormack, M., et al.: Security Analysis of Networked 3D Printers. In: Proceedings of IEEE Symposium on Security and Privacy, pp. 118–125. IEEE (2020)
3. Gao, Y., et al.: Watching and Safeguarding Your 3D printer: Online Process Monitoring Against Cyber-physical Attacks. In: Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, pp. 1–27. ACM (2018)
4. Bella, G., Biondi, P., Bognanni, S.: Multi-service threats: Attacking and protecting network printers and voip phones alike. Internet of Things 18, 100507 (2022)
5. Jia, Y., et al.: Artificial intelligence enabled cyber security defense for smart cities: A novel attack detection framework based on the mdata model. Knowledge-Based Systems 276, 110781 (2023)