Nubeprint
EU + 34 911 610 328
US +1 734 794 4790
info@nubeprint.com
www.nubeprint.com

Nubeprint
Cloud Printing Suite

v17.06

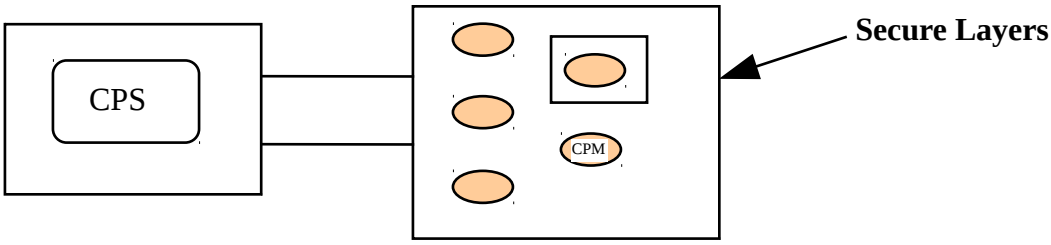
Security Concepts

June 2017

Nubeprint
EU + 34 911 610 328
US +1 734 794 4790
info@nubeprint.com
www.nubeprint.com

1. Introduction

The Cloud Printing Suite® is composed by the Cloud Printing Monitor (CPM) -aka DCA- and the Cloud Printing Server (CPS) that handles the network of agents and transforms the received data into information and services.



NubePrint's development process and policy follow secure software development best practices, which include formal design reviews and audits. Internal tools for code analysis are executed in an automatic manner as part of the standard building process and daily over the dedicated testing Git software repository.

This document is focused on the security aspects of both elements, Cloud Printing Monitor and Cloud Printing Server. For further related information, please contact at production@nubeprint.com.

2. CPM security aspects

The CPM is a piece of software that is installed on the network's customer and therefore, besides its high default security accomplishment, it is adaptable to any demand in terms of internal security policies or particularities of the networks on which it works.

The observance of the security requirements can be established on different complementary categories.

2.1. Security by design

Due to the SDD (Security Driven Development), the CPM accomplishes the most strict security policies (Banking, Health Services, Agencies).

•100% auditable, open source: the CPM is delivered with its sources (PAR toolkit) in order to easily be examined by the security crew.

•Core admitted and public released on CPAN.

•Interpreted language: with a direct access to the code that is executed.

•Implementation with strict adherence to standards and rules: RFCs for communications and network security, IETF, HIAPP, etc.

•Security compliance by design rules: experience has shown that the security through obscurity does not work.

2.2. Security in data transmissions

At all level, the CPM permits that the collected data treatment can be defined by the security crew in order to accomplish their own security policies (HIAPP, etc).

• Data collected: strictly collection of counters of pages, levels of consumables and operation alerts (i.e. drum damaged).

• Collection frequency: it's defined by the IT crew using the standard operating system scheduler instead of an internal or *adhoc* application timer.

• HTTP channel: ability to transmit through HTTP with strong SSL layer (256 bits), with support for authenticated or anonymous proxies.

• SMTP channel: ability to connect through customer's SMTP server with SSL layer (256 bits) with the possibility of copies from the origin (without the use of Forwarding rules) of each message for auditing purposes.

Nubeprint
EU + 34 911 610 328
US +1 734 794 4790
info@nubeprint.com
www.nubeprint.com

2.3. Security on the network

The CPM is fully adaptable to the Network Security Policies and Procedures due to its flexible deployment architectures and to its extensible configuration.

• Unlimited CPMs by network, multiple networks from a single CPM and/or multiple ranges per network: the IT crew decides the number and logical location of the CPMs in order to fit their needs.

• Compatibility with firewalls, segmented networks and dynamic routes: it admits port blocking and routes also during the discovering process using escalations.

• Reading list of IP addresses: with its functioning in “list mode”, the CPM targets to the specific group of IPs.

• Latency and Timeout: admits the internal definition of the timeout and latency being its default gentle values in order to fit the non-invasive gold rule.

2.4. Security by isolation

The CPM works as a transparent layer that doesn't disrupt any customer's network element. It is a fully portable software that can be connected without any system modification.

• No installation needed: allows the IT and Security crew to define their particular usage policies.

• No network changes needed: the routes and specific network architecture are handled by the CPM extensible configuration. Multiple networks, subnets, Vlans, etc.

• No printer/copiers changes needed: the usage of a fully SNMP stack (v1, v2c and v3) is used on strictly read-only mode in every case.

3. CPS Security aspects

CPS security is composed by three elements: Hosting, Operating System and Application. These elements work together in order to provide the Security Level demanded.

3.1. Hosting

Cloud Printing Server is prepared to work on security top level hosting/housing providers including our own datacenter.

We are aligned to the Auditing Standards Nº 70 / SAS70 Type II audit procedures that involve the basic control objectives:

– *Secure Organization*: controls provide reasonable assurance that there is a clear information security policy that is communicated throughout the organization to users.

– *Employee Lifecycle*: controls provide reasonable assurance that procedures have been established so that the crew accounts are added, modified and deleted in a timely manner and reviewed on a periodic basis to reduce the risk of unauthorized / inappropriate access.

– *Logical Security*: controls provide reasonable assurance that unauthorized internal and external access to data is appropriately restricted and access to customer data is appropriately segregated from other customers.

– *Secure Data Handling*: controls provide reasonable assurance that data handling between the customer's point of initiation to a CPS storage location is secured and mapped accurately.

– *Physical Security*: controls provide reasonable assurance that physical access to hosting's operations building and the data centers is restricted to authorized personnel.

– *Environmental Safeguards*: controls provide reasonable assurance that procedures exist to minimize the effect of a malfunction or physical disaster to the computer and data center facilities.

– *Change Management*: controls provide reasonable assurance that changes (including emergency / non-routine and configuration) to existing IT resources are logged, authorized, tested, approved and documented.

– *Data Integrity, Availability and Redundancy*: controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing.

– *Incident Handling*: controls provide reasonable assurance that system incidents are recorded, analyzed, and resolved in a timely manner.

3.2. Operating System

The default Cloud Printing Server is installed on Debian based GNU/Linux distributions as Debian itself or Ubuntu Server (Long Term Support).

Security Features:

1.No open ports controlled by policy
2.Password hashing: sha512 or md5
3.SYN cookies controlled by kernel and syctl
4.Firewall based on iptables/ufw
5.PR_SET_SECCOMP controlled by kernel
6.AppArmor enabled
7.SELinux available
8.SMACK controlled by kernel
9.Encrypted LVM available
10.eCryptfs available
11.Stack protection controlled by gcc patch
12.Heap protection controlled by glibc
13.Pointer Protector controlled by gilbc
14.Stack ASLR controlled by kernel
15.Libx/mmap ASLR controlled by kernel
16.Exec ASLR controlled by kernel
17.brk ASLR controlled by kernel
18.VDSO ASLR controlled by kernel
19.Built as PIE availability
20.Built with Fortify Source by gcc patch
21.Built with RELRO by gcc patch
22.Built with BIND_NOW availability
23.Non-Executable Memory by PAE
24.maps protection controlled by kernel
25.0-address protection controlled by kernel
26./dev/mem protection controlled by kernel
27./dev/kmem disabled controlled by kernel

Nubeprint
EU + 34 911 610 328
US +1 734 794 4790
info@nubeprint.com
www.nubeprint.com

28.Blcok module loading controlled by systcl
29.CONFIG_DEBUG_RODATE controlled by kernel
30.CONFIG_CC_STACKPROTECTOR controlled by kernel

Security updates is daily or on demand:

Debian and Ubuntu distributions take security very seriously, handling all security issues with the highest attention and ensuring that they are corrected within a reasonable time-frame. Many advisories are coordinated with other software vendors and are published the same day a vulnerability is made public.

Unlike other business solutions, the CPS servers are configured by default to be updated on daily basis.

3. Applications

By company policy, the Cloud Printing Server only works with the secured versions of the applications involved:

– Web Server: Apache2 with SSL layer and security tips/flags enabled
– Database: Mysql with Security Best Practices applied
– Nubeprint's Engine on strict mode
– Perl and PHP interpreters and the Java compiler: daily updated to its latest production release or security patches
– SSH: daily updated to latest release in production or security patches.
– Firewall: iptables/ufw enabled
– Apparmor: custom configuration over the CPS utilities
– VPN: on demand, the system is prepared to create a secure connection (VPN or SSH tunneling) to the CPS 's operator