PrintFleet Enterprise Printer DCA Security

This document discusses security-related issues related to the Printer DCA. These include the measures PrintFleet takes to protect the data and code, as well as identifying network requests that may be made by the Printer DCA in the course of diagnosing communication problems.

Protection Measures

PrintFleet recognizes the importance of protecting vendor MIB data. In order to safeguard this information, PrintFleet has implemented various types of security.

Protecting the Printer DCA Data

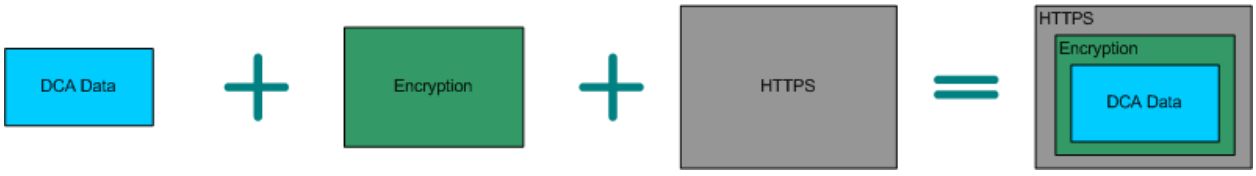
To protect the Printer DCA data, PrintFleet uses encryption from end to end (both for DCA files and Semaphore commands). The data is never stored in plain text; the only time it is "in the clear" is when it has been processed and stored in the PrintFleet Enterprise database (security from there is up to MS SQL Server).

There are two purposes of encryption:

- To protect the data from interception and viewing/use without using PrintFleet Enterprise.
- To authenticate the Printer DCA and ensure integrity of the data (i.e. that it hasn't been tampered with).

Each Printer DCA has its own encryption key, which must match the encryption key on the PrintFleet Enterprise server to verify the data is actually coming from that Printer DCA. It makes it difficult to tamper with the data, because an attacker would need to know the encryption keys, algorithms used, and be able to re-create the checksums. Even so, if a key is ever compromised, it only affects that specific Printer DCA, and re-activating the Printer DCA will create a new key.

HTTPS adds an additional layer of encryption, but is not required. When using HTTP (not encrypted) to transmit Printer DCA data, the only difference is the message container is in plain text; the actual Printer DCA data itself is still encrypted.



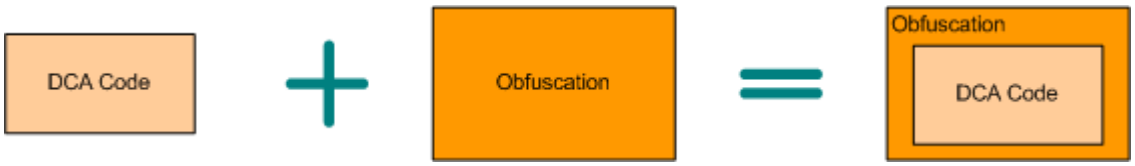
275 Ontario St., Suite 301
Kingston, Ontario
K7K 2X5
www.printfleet.com

Issued: June 25, 2012

Protecting the Printer DCA Code

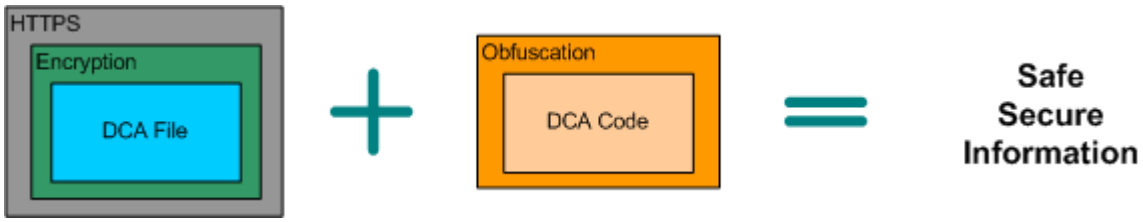
In addition to protecting the Printer DCA data, PrintFleet uses obfuscation to protect the Printer DCA code (see http://en.wikipedia.org/wiki/Obfuscation for information about obfuscation). By applying several obfuscation techniques it is close to impossible to reverse engineer the Printer DCA code to figure out how we collect data from devices. This achieves two important security objectives:

- Protect our IP (Printer DCA code) to make it difficult to build a Printer DCA clone, or modify the Printer DCA to report somewhere else.
- Protect our OEM partners' IP (the locations they store things in their private MIBs) – which is sometimes public knowledge, and sometimes protected under NDA or other contracts.



Summary

We recognize the importance of protecting our clients' valuable MIB data, and have taken all reasonable steps to safeguard that information. It is in our own best interest to ensure that our clients feel confident that their information is safe and secure.



Network Requests

Printer DCA may make a network request when you:

- Activate (or reactivate) the Printer DCA, and the Printer DCA fails to detect the web service
- Manually initiate a communications test following a change to the communication method or port, and one or more of the files fails to be successfully transmitted.

In these cases the Printer DCA will use the following URL to try to diagnose the nature of the failure:

http://networktest.printfleet.com/