May 24, 2019

TRUSTED CERTIFICATE INSTALLATION SERVICE FOR PRINTERS WITH EMBEDDED WEB SERVER

HP INC

Trusted certificate installation service for Printers with Embedded Web Server.

Herein a web-based service is proposed which provides printer users with a straightforward and simple way to secure their connection to printers supporting Embedded Web Server [EWS] functionality.

The current implementation of the Printer's EWS forces https:// connections to the user PC for printer configuration and administrative pages in order to establish an encrypted communication channel to avoid communication "Sniffing" attacks that may reveal to the attacker the printer administrative password to gain access to sensitive configuration pages or job content. The printer's EWS uses a self-signed certificate to establish this secure connection through Secure Socket Layer protocol.

Even though all the communications between the EWS and the user PC over https:// are encrypted, the self-signed certificate used by the printer triggers a security warning on the user's browser. In consequence, the user has no way to distinguish the genuine printer's EWS interface from a spoofed EWS as in both cases the user's browser will show the same warning message which makes unprotected printers vulnerable to a Spoofing or Mand in the Middle attacks as shown in the Figure 1.

Some printers offer to their users the capability of installing in the printer certificates provided by the user itself. These certificates my fall into two categories:

1. Signed by a Globally Trusted Certification Authority [CA] (Pre-Installed in standard browsers).
2. Signed by a CA Trusted by the user (Added by the user to the browser).

These two choices require either an investment from the user to pay a CA for the Signing Service or having an understanding and tool set that most of the users don't have to create their own Certificate and CA pair and install the CA in the browser. Either way there is also a cost in time involved.

The proposed Sign and CA installation Service comprises a Sign Server to which the printer connects to upon user request.

Once the printer is registered by the service the printer downloads a signed certificate from the Certificate Sign Server and the user receives a download link for an application that installs the Certificate Authority [CA] in the user PC key store.

The high-level steps involved in the process are shown in Figure 2 and comprise the following:

1. EWS redirection with printer data to the Sign Server.
2. Printer certificate generation and signing by the Certificate Sign Server.
3. Direct Printer Certificate download to the printer.
4. Download link provided to the user through redirection from the EWS to the Sign Service portal.
5. The user PC now recognizes the printer EWS as a secure and protects the user against Spoofing Attacks.

The proposed Service makes it easily accessible for the user the protection of its connection to the printer's EWS and enables scalability for securing printer communications over Enterprise environments in three steps:

1. The user accesses the printer's EWS and clicks on the "Request Sign Protection" link.
2. The user is redirected to the Sign Server and confirms the printer data form.
3. The user downloads the CA installation executable from the Server and double clicks it.

This way it is simple to secure the communications with the printer reducing the attack surface to be exploited by cybercriminals and helping to extend the telemetry services for printing solutions as the benefit for extended protection offered by the certification revocation process control will also rely on such system.

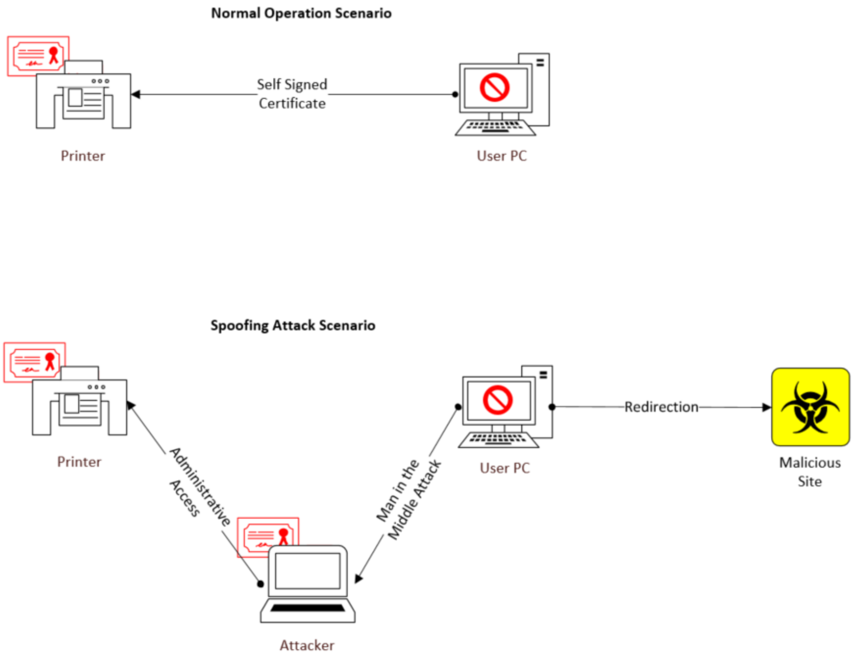

Figure 1. Spoofing or Man in the Middle Attack using a self-signed certificate.

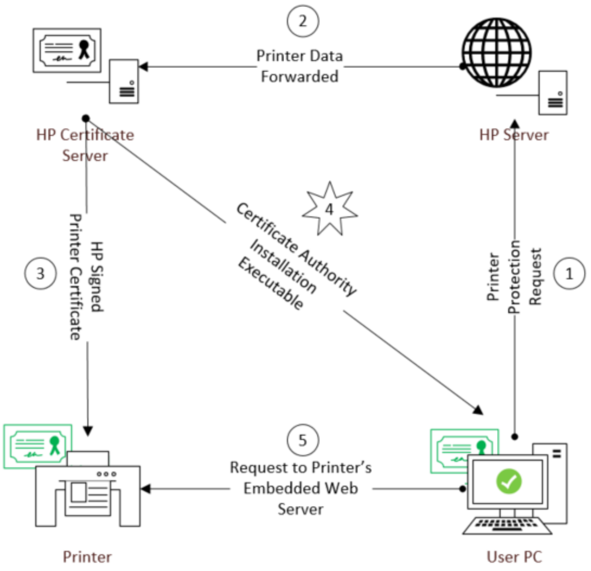
2
Printer Data Forwarded
HP Certificate Server
HP Server
4
Certificate Authority Installation Executable
3
HP Signed Printer Certificate
Printer Protection Request
1
5
Request to Printer's Embedded Web Server
Printer
User PC

Figure 2. Trusted certificate installation service steps.

Disclosed by Bladimir de la Hoz Matveeva, Naroa Gonzalez Sanchez and Nebojsa Cosic, HP Inc.