KEYPOINT INTELLIGENCE | InfoTrends

PREPARED FOR:

WHITE PAPER

HP OFFICE CARTRIDGE SECURITY

PRINTING SECURITY FROM START TO FINISH

AUGUST 2020

contents

Document

Figures

Introduction

The pressing need for robust IT-infrastructure security safeguards is well understood, as the legion of reports about network hacks, data breaches, ransomware attacks, and phishing scams grows monthly. While network and cloud infrastructures (and the endpoints attached to them) garner most of the attention, however, an easily overlooked potential vulnerability lurks inside every office-class printer and MFP: the consumables cartridge. These cartridges come equipped with embedded integrated circuit (IC) microcontroller chips that contain code that enables them to communicate with the printer and perform essential functions. Without tight control over the origin of the chip and its coding, as well as safeguards against tampering with the cartridge at every step of its lifecycle, dealers could be putting their customers' devices and networks at risk.

For this whitepaper, Keypoint Intelligence was contracted by HP Inc. to report on the security protections provided by its Original HP consumables strategy and the potential threat posed by non-HP consumables in office-class printing devices. Our analysts learned that HP incorporates security into every step of the design, supply chain, and production process of its consumable cartridges for office-class devices—including unalterable firmware resident on the cartridges' control chips. This, combined with HP's class-leading device security, makes it essentially impossible for a factory-sealed Original HP consumables cartridge to be used as a "Trojan Horse" to compromise the functionality of a customer's office printing device, or potential data on it. This is not necessarily the case with third-party aftermarket consumables.

Background: Toner and Ink Cartridges

Laser and inkjet printers each need black and often color materials to deposit an image onto a piece of paper. Laser printers use a solid powder called toner while inkjet printers use a liquid ink. In each case, these materials are housed in a cartridge for easy replacement and maintenance.

With laser printers, there are other mechanical components within the all-in-one cartridges that participate in the laser printing process. These parts frequently include the photosensitive drum, cleaning station, and drum charging roller. These components would typically wear out over time and eventually require replacement. As such, those components are also housed within the cartridge so that laser printers do not need the periodic technical service that A3/MFP copiers typically require. For laser printers, the all-in-one toner cartridge reduces the need for periodic machine service by a technician. Based on Original HP color and monochrome All-In-One cartridges and the EP process steps required to print a page, HP says that up to 70% of the printing technology of the device is inside the Original HP toner cartridge system.

Figure 1: Examples of Office-class Cartridges

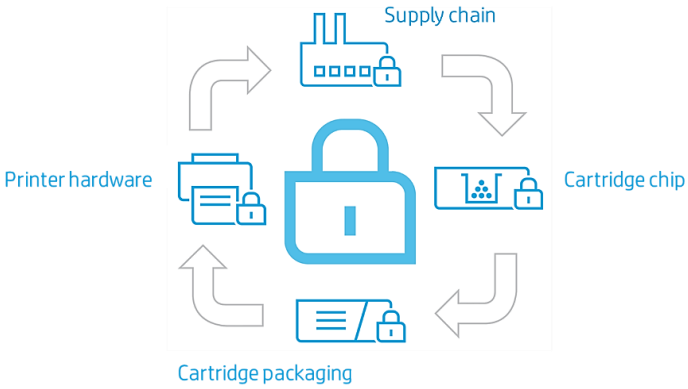
51%

Of IT decision makers identified data and document security as their top priority over the coming three years.

HP Office Cartridges Manufactured & Designed for Security

Original HP Office Class cartridges are manufactured and designed to provide a broad range of security protections for users of HP Office-Class printers[1]. HP Office Class cartridges are manufactured using secure supply chains and secure facilities. Only Original HP components are used in the manufacturing process. A secure, unalterable chip is installed on the cartridge. Cartridge packaging is tamper-resistant to ensure that an Original HP cartridge is inside the box. In some cases, there is even available Customer validation of security label package at point of purchase[2]. Finally, the communication and authentication between the cartridge and the printer is designed and manufactured to be secure.

Figure 2: Original HP Cartridges Designed for Security



[1] For HP Office-class printing systems that includes enterprise-class devices with FutureSmart firmware 4.5 or above, Pro-class devices and their respective Original HP toner, PageWide, and ink cartridges; it does not include HP integrated printhead ink cartridges.
[2] Digital supply-chain tracking, hardware, and packaging security features vary locally by SKU. See hp.com/go/anticounterfeit.

Functions of Original HP Cartridge Chips

Toner and ink cartridges have an IC chip on them to communicate with the printer. Cartridges need to be able to communicate with the printers to provide beneficial functions, including:

- **Supplies levels management** of ink or toner, which can be viewed like a gas gauge. This provides enough time to reorder supplies or (if an automatic supply fulfillment plan is used) for automatic supplies reordering. With some inkjet printers, if one continues to try to print when the ink is completely out, the printheads may be damaged—requiring replacement. The HP chip on the ink cartridge monitors and helps protect the printhead.

- **Notice/Cartridge Compatibility/Electronic Keying** (for color cartridges) to check for and inform of proper installation and cartridge compatibility to make sure that the correct cartridge is installed properly.

- **Authentication** informs the user that an Original HP cartridge has been installed as opposed to a third-party cartridge that is potentially masquerading as an Original HP one or was mistakenly ordered.

- **Consistent print quality**:

    - For laser toner printing, other cartridge components wear out over the life of the cartridge. The HP chip is used to make various adjustments to voltages applied to the various components—assuring that the cartridge will provide optimum print quality even as components inside the cartridges start to wear. Without such adjustments, print quality would deteriorate with use.

    - For inkjet printing, the HP chip includes technology packages with resources and recipes that make color maps to transform colors from the source to the different colors in the target image. This allows the cartridge to deliver optimal print quality over its life on different papers.

        - When improved ink formulas become available, these packages on the cartridge chip may be revised to optimize print quality. Original HP chips on HP Integrated Print Head (IPH) cartridges deliver consistent print quality with enhanced detail by communicating the ink drop weight/volume and estimated ink levels.

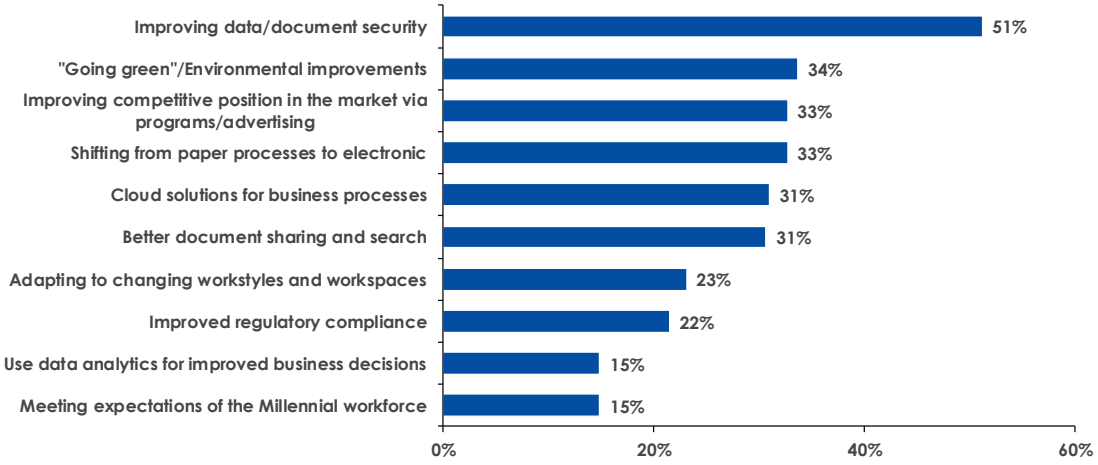
        - This produces sharp black text and vivid graphics, with reduced image grain and increased color gamut for photos and graphics with smooth gradations and accurate colors.

- **No personally identifiable information** is stored on the HP cartridge chip, so it can be confidently returned for recycling.

The Importance of Security

Our recent survey of US IT decision makers and influencers revealed that "improving document security" is the number-one business objective for respondents from companies of all sizes. This finding has shown up consistently in several of Keypoint Intelligence's studies.

Figure 3: IT Decision Makers' Top Priority Over the Next Three Years



Source: *US IT Decision Makers Survey in SMB & Enterprise Markets* (Keypoint Intelligence, December 2019)

It has become increasingly clear that all network endpoints—printers and MFPs included—need to be hardened against potential attacks. In the early days of printers, the programming and various software modules that enabled the printer to function—collectively referred to as firmware—used to reside in read-only memory (ROM) that was "set in stone" when the device was manufactured.

Today's more sophisticated output devices, however, have full operating systems that allow advanced capabilities, such as complex (and customizable) user interfaces and downloadable "apps" that add extra features. In addition, manufacturers quickly saw the benefit of being able to update firmware of devices already in the field to correct issues or improve functionality. Therefore, firmware now typically resides in addressable memory spaces that can be overwritten. Such an overwrite can come from a trusted source (such as the manufacturer) or from a hacker or other bad actor looking to place malware on a device for destructive or other nefarious purposes.

Moreover, office-class printing devices support bi-directional network and Internet communications—putting them at the intersection of the private corporate network and the wide-open web. Hence, the security integrity of MFP hardware is crucial not only to protect the information that may reside on the device (such as the e-mail address book and documents stored in a user box on the machine's hard drive), but also because the

device can be exploited as a conduit to the wider corporate network or as a "bot" in a planned DNS attack.

Unfortunately, these attack vectors are not just theoretical; there is a growing list of real-world incidents that were made possible by holes in MFP security. For example, in April 2019, security researchers in the Microsoft Security Response Center discovered malware of known Russian hackers compromising an unsecured office printer that allowed the attacker to gain access to any network segment—even though VLAN security and firewalls were implemented on the network. In effect, the printer was the perfect "unlocked back door" to the network.

HP has taken such threats seriously and has designed its devices to be among the most secure in the industry. In fact, HP is the only print-device maker to have successfully completed all three phases of the Keypoint Intelligence's Security Validation program. This vendor-agnostic security testing program standardizes the benchmark requirements for output device and office "Internet of Things" (IOT) security and addresses security from various vectors to determine if devices are safeguarded against vulnerabilities.

To protect the bootup (aka BIOS) and operational firmware modules, HP Enterprise-class printers are equipped with HP FutureSmart Firmware (version 4.x and later), which delivers a host of proprietary security features. With HP Sure Start—a concept ported over from HP's vast experience engineering secure PCs and servers—a secure boot mechanism will detect any potential attack on the BIOS and (in the event that the BIOS is compromised) restart the device using the factory-correct "golden copy" of the BIOS and resume bootup in a safe state. Enterprise-class devices also support run-time intrusion detection, which detects any malware intrusion attempts during complex firmware and system memory operations; it validates that the memory space is not modified to prevent memory corruption. HP devices also support whitelisting, so non-approved code (i.e., code not digitally signed off on by HP) will not execute on the device. In addition, with the HP Connection Inspector, network traffic is continuously analyzed for anomalous activity indicative of a DNS attack originating from the device.

HP Pro-class printers also include firmware integrity validation to protect against compromised firmware that could open the device and network to attack. The machines' secure-boot capability validates the integrity of the boot code and can trigger a recovery mode should an anomaly be detected. These models also offer run-time code protection that prevents intruders from adding malicious code when the printer is running; all run-time code memory is write-protected and all data memory is non-executable.

Nevertheless, it is not just the device firmware that is at risk. Since the cartridge firmware needs to interface with the device firmware, HP has recognized cartridge security is another possible attack vector. Rather than relying on all the other device protections in

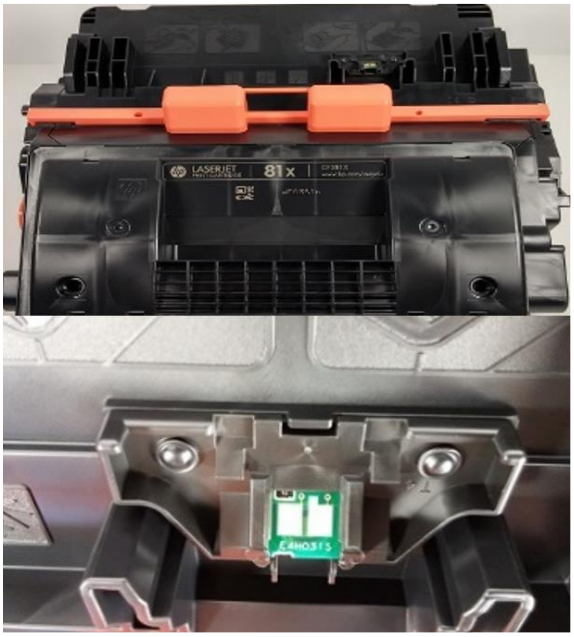
place, HP has left nothing to chance and opted to remedy that potential vulnerability as well. Just as with non-ROM device firmware before it, reprogrammable chips used by third-party cartridge vendors are inherently unsecure. The chips are vulnerable to being "flashed" (overwritten) with other code after leaving the factory—and that code could be malicious. Indeed, chip reset devices for reprograming aftermarket chips are publicly available to anyone[3].

Benefits to the Customer

HP Office Cartridge Security Chips

To protect the office customer, HP uses custom designed, purpose-built chips on its original cartridges. Original HP office cartridges use modern secure "smart card" technology chips—the same chip technology used in credit and debit cards—that authenticate and then allow information to be transferred back and forth between the printer and the chip securely. Non-HP chips may use general-purpose microcontrollers, which can be vulnerable to reprogramming or insertion of malware code[4].

Figure 4: Example of Original HP Cartridge with Chip



Note: Sample HP cartridge chip photo provided by HP; location and chip style vary

[3] Apex Chip resetter and Chip resetter/programmer from Zhono sold on Alibaba

[4] CRN Article by Shivaun Albright, Chief Technologist for Print Security at HP

While the instances are rare, the altering of cartridge chips has happened. In one instance, chips fitted to third-party remanufactured cartridges were able to alter the printer-resident firmware without the knowledge or approval of the customer nor the hardware OEM. The malware was used to instruct the printer to no longer recognize otherwise-compatible cartridges from other manufactures—including original OEM cartridges. Users of these devices had to download new firmware provided by OEM vendor to remediate the changes made to the printer. The incident illustrates that firmware changes can indeed be delivered by an unsecure cartridge chip and that device functionality can be impacted in a way never intended by the device manufacturer. With a vulnerable cartridge such as this, unscrupulous actors could deliver a payload that is more malicious than the one in this example[5].

Tamper Resistant Packaging

HP Office Class cartridges are packaged in tamper-resistant boxes that vary locally by SKU. This includes a box that cannot be re-sealed once opened and security labels on the box[6]. If the cartridge box has been tampered with, the box may very well contain a non-original cartridge, a counterfeit cartridge, chip of unknown origin containing malware or worse.

Figure 5: Original HP Cartridge Packaging Security

1. Tamper-resistant packaging

2. Security label on box

[5] Aftermarket printer cartridge company Aster discuses destructive chips from another unnamed aftermarket chip company causing damage so that the Aster products were no longer recognized by printers. They say their chips are anti-destructive and resolve the incompatibility program and permit their brand of aftermarket printer cartridge to function.
[6] Tamper-resistant packaging that protects the chip and cartridge from replacement or alteration, including options like security label, sealed inner package (zip-strip or foil) and tamper-evident label (packaging security features varies locally by SKU).

The Security of Knowing What You Put in Your Printer

Original HP cartridge secure chips and tamper-resistant packaging makes sure that you get and can verify what you have purchased. The market for toner and ink cartridges for use in HP Office Class devices include original HP cartridges as well as non-original third-party cartridges from aftermarket providers. Non-original cartridges may be remanufactured or refilled from what was an empty original HP cartridge, or may be a newly manufactured imitation cartridge with no original HP parts.

When a company remanufactured/refills a cartridge it may or may not reuse the original HP chip. If an original HP chip is reused, when a remanufactured/refilled cartridge is placed into the HP printer, the chip recognizes that the cartridge was refilled and communicates to the printer and the user that the cartridge is no longer an original HP cartridge. This is important because not all remanufactured/refilled cartridges are clearly marked and packaged to indicate that they are no longer original HP cartridges. Further, particularly when purchasing cartridges off the Internet, some websites do not make it entirely clear whether a cartridge is an original HP or not. When the unalterable HP chip communicates to the user that the office cartridge is no longer original HP, this helps the user to be assured that what they got is what they intended to purchase.

Some remanufactured/refilled cartridges and all newly built imitation cartridges use non-HP chips with programs that have not been written by HP. They are not secure HP Chips.

New Working Styles Increase Vulnerability

With many office employees working at home due to potential health risks associated with going into the office, the security of personal and company information needs heightened attention as employees may need to work in inherently insecure locations. In fact, early research by Keypoint intelligence indicates that about 45% of people who moved to work at home in the first half of 2020 also acquired new printers to support their working from home[7]. Looking forward, it may be years before offices can operate at full occupancy or that workers will even choose to return to the office at all.

The expectation is that the landscape for remote working may be permanently changed with far more employees working at home than prior to the pandemic. With data thieves and scam artists multiplying, insecure cartridges and printers could become a target in the future. Original HP cartridges coupled with secure office printers closes a potential risk.

[7] Keypoint Intelligence *US and Western European The Future Office Survey 2020*

opinion

Opinion

Unlike third-party remanufactured cartridges, HP maintains a "closed loop" in the manufacturing and distribution of its original HP cartridges. In addition, given that there is a data interface from the chip to the printer, an attacker with the right skills and resources may be able to uncover and exploit a vulnerability—taking advantage of this interface to add malicious code. Time will tell how office printer cartridge customers and channel partners respond to this innovative approach by HP to differentiate original HP office printer cartridges.

As Justine Bone, CEO of medical cyber-security provider MedSec noted, "Original HP office-class print cartridges are part of HP's comprehensive security in depth strategy, which takes security into account throughout the design, supply chain, production process and packaging to help keep printers protected from unintended consequences of non-HP cartridges of unknown origin. These efforts give you peace of mind that when you choose HP Printers using original HP office cartridges, you are helping protect the integrity of your office systems."

appendix

Appendix

The following links were helpful in the creation of this white paper:

- **Original HP Office Cartridge Security:**
  - http://www.hp.com/go/suppliesthatprotect
  - http://www.hp.com/go/suppliessecurityclaims
  - https://h20195.www2.hp.com/V2/getpdf.aspx/4AA7-6186ENW.pdf
- **Shivaun Albright Article**
- **Original HP Printer Supplies Collateral:**
  - Ink
  - Toner

authors

Jamie Bsales
Director
+ 1 973.797.2156

Jamie Bsales is an award-winning technology journalist who has been covering the high-tech industry for more than 20 years, nine of those at Buyers Lab. In his role as Director, Office Workflow Solutions Analysis, Jamie is responsible for BLI's coverage of document imaging software and related services.

John Shane
Director
+ 1 781-616-2140

John Shane is a leading industry expert on marking materials such as toner, inkjet ink, and cartridges. As a Director for the Communication Supplies Consulting Service, Mr. Shane is responsible for all forecasts, research reports, consulting, and client care concerning those topics.

Comments or Questions?