OFFICE PRINTER SECURITY, STARTING WITH THE CARTRIDGE

HP's cutting-edge security features go beyond the printer to encompass the cartridge itself.

By **Shivaun Albright**, Chief Technologist, Print Security, HP Inc.

In our increasingly connected world, any network device can become an avenue of attack for hackers. And if we're going to enjoy the many benefits and conveniences of the Internet of Things, we must commit to securing every "thing" we connect. Servers and client PCs top the list, but network printers may also be vulnerable to attack. Why? Because they're less likely to be thought of as needing protection.

Over the past few years, we have seen a rise in attacks of embedded system technologies, which are often shared across connected devices. The risk includes PC firmware/BIOS as well as printer firmware. Cyberattacks are rapidly increasing in sophistication. Because of this, HP is hyper-focused on printer security, especially in the office environment, and on improving our security strategies to protect resellers and customers.

Of course, wherever there are printers, there are printer cartridges. As with all other components of your office infrastructure, you want to know and trust what cartridges go into your printer. Counterfeit or imitation cartridges come with many risks. Counterfeiters make and market fake printing supplies intended to deceive customers. These illegal counterfeit cartridges masquerading as HP cost the industry billions of dollars each year, undermine trust in the market and may fund other kinds of criminal activity. Non-HP imitation cartridges may yield poor printing results[1] and cause printer damage.[1] Imitation toner may exceed ecolabel emission limits[2], and non-HP imitation cartridges may attach untrusted and unknown electrical hardware to your network infrastructure. The threat landscape is constantly changing, and what was secure today might not be secure tomorrow.

To minimize that risk, HP's office printing security features go beyond the print hardware and extend to the cartridge itself. We've made significant investments in ink and toner cartridge research and development to help protect customers. Indeed, our office-class Original HP printer cartridges take security into account throughout the design, supply chain and production process to help keep the printers running efficiently.[3] Original HP are secure office printer cartridges you can trust. By using only Original HP cartridges in your HP device, you can help protect the integrity of your data.

Security from Every Angle

We truly believe office printing system security must be built in — not bolted on. It can't be something you do after the fact. That's a recipe for failure.

While the industry has become sophisticated at spotting and blocking software-based intrusions, the same can't be said for hardware. In fact, it is well understood in the IT industry that counterfeit hardware can become the source of hardware-based exploitation.[4]

HP Supply Chain Security

HP is vigilant about recognizing and mitigating security risks in the supply chain to help reduce the risk of malicious code entering the office cartridge chip. Measures are taken to help protect the chip from being replaced or altered while in the supply chain. HP and our partners have world-class manufacturing – carefully managing internal supply chains, working

with partners who follow industry best practices on security and partnering with security experts. HP office printer cartridge chips are manufactured in secure facilities. HP's chips are certified as EAL5+ and manufactured in facilities where products have achieved EAL5+ certification.[3]

HP Office Cartridge Chip Security

HP office printer cartridge chips are designed for security. Only Original HP cartridges contain a chip with HP proprietary firmware that is designed from the hardware to be secure and resistant to tampering. Non-HP supplies include chips of unknown origin that could employ untrusted firmware. 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.[3]

HP office cartridge chips help protect your printer with secure smart card technology that is commonly found on chip-based credit and debit cards. Original HP office printer cartridges, introduced since 2015, use smart card technology for maximum data integrity with resistance to tampering and hacking. Non-HP chips may use general purpose microprocessors, which may introduce risks.[3]

HP Enterprise Printer Hardware Security

HP recognized the potential threat vector for enterprise printer hardware and cartridges years ago and now offers Runtime Intrusion Detection solutions that flag anomalies in system memory. HP's enterprise-class printers also offer Sure Start technology, which automatically detects, stops and recovers from a BIOS attack or corruption without IT intervention, thus self-healing from the attack.[5]

HP Packaging Security & Tracking

HP was one of the first tech companies to include holographic security labels — complete with verifiable QR codes — on office printer cartridges, a technology that's helped to crack down on fakes. Made with advanced printing techniques, the labels function much like the security marks found on currency.[3]

Digital tracking through the supply chain for many office printer cartridges provides end-to-end supply chain validation for resellers and end users. These Original HP office cartridges can be tracked from the factory to printer and checked throughout that journey.[3]

Resellers and Security Strategies

While end-users certainly benefit from this kind of multi-layered printer cartridge security, HP's partners and resellers need the protection as well. No savvy reseller wants to deal in non-HP cartridges that may contain a chip of unknown origin which may have untrusted firmware containing malicious code, potentially making the customer's network infrastructure a target of attack.

HP is working to educate its partners and resellers about all of our office printer and cartridge security features, including tamper-resistant packaging, security labels, zip-strip sealed inner packaging, tamper-evident labels and trackable ID codes. Resellers (and end users) can report a suspected counterfeit online or, for larger volumes of inventory, request an on-site anti-counterfeit Customer Delivery Inspection.

As we all navigate an increasingly complex world of cyberthreats together, it's paramount that we utilize every possible resource to deliver trusted, resilient security for office printers. Technology companies must design security into everything they build, hardware, firmware and software. The channel must remain ever vigilant to the differences between vendors who are well-versed and serious about security and those who are not.

Hackers are always looking for the weakest links on customer networks as an entry point to start their attacks. Collectively, we must do everything possible to frustrate those aspirations. For office printing, using only Original HP ink and toner cartridges should be a key step of an in-depth defense strategy.[3]

Learn more at hp.com/go/suppliesthatprotect and https://www8.hp.com/us/en/cartridge/anti-counterfeit.html.

[1] Non-HP printer cartridges may cause poor printing results, printer damage: Counterfeit cartridges may North America results based on a SpencerLab 2018 study commissioned by HP for the on-average performance of 12 brands of remanufactured cartridges, refilled cartridges from leading refill service providers, and refill kits compared to Original HP ink cartridges (61XL, 62XL, 63XL, 564XL, 950XL, 951XL, 970XL & 971XL) sold in North America. See http://www.spencerlab.com/reports/HPInkReliability-NA-2018.pdf.

2018 SpencerLab Color and 2019 SpencerLab Monochrome Reliability studies for North America, both commissioned by HP. Color study compared Original HP color cartridges with six brands of non-HP cartridges for the HP LaserJet Pro 400 M451dn; CE410A/X, CE411A/12A/13A cartridges. See https://www.spencerlab.com/reports/HP-CLR-Reliability-NA-2018.pdf. Monochrome study compared Original HP cartridges with seven brands of non-HP cartridges for the HP Pro M402 and Pro M521 printers; HP 26A and 55A cartridges. See https://www.spencerlab.com/reports/HPReliability-NA-2019.pdf.

Non-HP printer cartridges may cause printer damage: North America results. 2019 NA Market Strategies International study commissioned by HP. Results based on 222 surveys from HP ServiceOne Partners who have at least 6 months of experience servicing HP monochrome and Color LaserJet printers with HP and non-HP toner cartridges installed and have done so within the previous 12 months of the study. See marketstrategies.com/hp/NA-Technician2019.pdf

[2] Imitation toner may exceed ecolabel emission limits: Nov 2019 WKI Blue Angel Indoor Air Quality study, commissioned by HP, in compliance with DE-UZ 205: 21 imitation and five remanufactured toner cartridge brands compatible with HP Color LaserJet Pro MFP M477fdw (sku# CF410A, 411A, 412A, 413A) purchased in EMEA, LA and NA regions. See HP.com/go/IAQnonhpWKI2019

[3] HP Office Printer Cartridge Security: HP Office-class printing systems include Enterprise-class devices with FutureSmart firmware 4.5 or above, Pro-class devices, and their respective Original HP toner, PageWide, and ink cartridges. Does not include HP integrated printhead ink cartridges. See: https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA6-8438ENW and www.hp.com/go/SuppliesSecurityClaims. Digital supply-chain tracking and packaging security features vary locally by SKU.

[4] Counterfeit hardware and counterfeit hardware-based exploitation: "A survey of emerging threats in cybersecurity" published in Journal of Computer and System Sciences, Volume 80, Issue 5, August 2014, Pages 973-993. CSIRO ICT Centre, Australia. https://doi.org/10.1016/j.jcss.2014.02.005

[5] HP enterprise-class security features: HP's most advanced embedded security features are available on HP Enterprise and HP Managed devices with HP FutureSmart firmware 4.5 or above. Claim based on HP review of 2019 published features of competitive in-class printers. Only HP offers a combination of security features to automatically detect, stop, and recover from attacks with a self-healing reboot, in alignment with NIST SP 800-193 guidelines for device cyber resiliency. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/PrinterSecurityClaims.