Reinventing PC & Printer Security
Kurt Lysy, HP Security Product Consultant
HP STUDIOS | intel

PRESENTS:

Exclusive Premiere  
TRUE ALPHA

Room 802 – October 3rd

Showtimes:
12:30 pm - 1:00 pm  
1:30 pm - 2:00 pm  
2:30 pm - 3:00 pm  
3:30 pm - 4:00 pm

- Popcorn!
- Sodas!
- Alcohol!
- T-Shirts!
EVERY PC & PRINTER DECISION IS A SECURITY DECISION.
THREATS TARGET EVERY LEVEL OF THE SYSTEM
HARDWARE IS THE LEAST VULNERABLE TO ATTACK

**ABOVE THE OS**
Manageability Infrastructure, Visual Hackers

**OPEN DOORS**
Security tools are useless unless policies enforced. Manageability is required to make security effective.

**IN THE OS**
Operating System, Software, Downloads

**COMMON TARGET**
Unpatched software vulnerabilities are easy to exploit. Malicious websites, infected downloads.

**BELOW THE OS**
Firmware (BIOS, etc.)

**IDEAL TARGET**
Complex target. Successful attacks mean persistence, stealth, and access to almost anything they want.

**HARDWARE**
Extremely difficult to penetrate

**MOST SECURE**
Extremely difficult to penetrate
THE BOTTOM LINE

It’s not a matter of **if** you’re PCs and printers will be attacked, but **when** and **whether** an attack is successful, and (most importantly) whether you’re able to **recover**.
WHAT ABOUT VIRTUAL DESKTOPS?

• Virtual Desktop Infrastructure (VDI) deployments have been gaining increasing interest in many verticals

• In most VDI environments, customers use thin clients to connect to data centers which host the Virtual Machines.

• Any endpoint can be breached, whether it be a printer, desktop PC or notebook, or even a thin client.

• Simply deploying virtual desktops to PCs does not by itself eliminate security threats.
SECURITY THAT’S “BUILT-IN, NOT BOLTED ON”
DESIGNED FOR CYBER-RESILIENCE

Increase protection at all levels of compute platform

Protect

Recover

Detect

Continuous business productivity, lower Total Cost of Ownership (TCO), and seamless recovery

When protections fail (and they will), proactive detection is essential
A SECURE SYSTEM REQUIRES A HARDENED ROOT OF TRUST

To protect against the malware of the future PCs and printers must have security rooted in HARDWARE

- Out of reach of malware attacks
- Independent of the BIOS and OS
- Can’t be tampered with
DEVICE SECURITY STARTS WITH THE BIOS

What is the BIOS?
• First million lines of micro code that validates device safe power up

Who cares?
• YOU SHOULD! Once corrupted, the hacker “owns” your PC or printer
• All other protection is useless if the BIOS is infected below the OS

No antivirus or OS firewall can detect an infected BIOS!
WHAT’S NEEDED?

• A multi-layered, defense-in-depth strategy with features and tools to protect, detect, and recover from malware attacks

• Proven technologies below, within, and above the OS

• Built-in (NOT bolted-on) hardware-enforced protections

• Protection across device, identity, and data
RECOMMENDED PROTECTIONS

• Secure and protect the BIOS

• Protect critical processes within the OS (such as antivirus, anti-spyware, OS firewall, Windows Defender, etc.) and ensure they’re automatically restarted whenever disabled or shut down

• Ensure that you’re able to immediately and quickly recover bricked PCs from a baseline or custom image

• Protect against malware attacks thru corrupt web links and from infected document downloads (PDFs, Word, Excel, & Powerpoint)
• Use multi-factor authentication (biometric, smart card, etc.)

• Protect against visual hacking

• Lock down USB and other ports

• Protect against malware attacks thru corrupt web links and from infected document downloads (PDFs, Word, Excel, & Powerpoint)
For printers, deploy security and manageability features that:

- Keep the BIOS safe
- Keep the firmware safe (“whitelisting”)
- Keep the memory safe via runtime intrusion detection of the SMM (System Memory Module)
- Monitor connections made to printers and blocks those deemed suspicious
- Provide automatic updates of security policy settings to entire fleet from a centralized console
2018 HP SECURITY FRAMEWORK

MANAGEABILITY

For use with customers under current Confidential Disclosure Agreement only.
© Copyright 2018 HP Development Company, L.P. The information contained herein is subject to change without notice.
Enables Hardware Enforced, Self-Healing, Manageable Solutions Independent of BIOS & Tamper Resistant

HP’s ENDPOINT SECURITY CONTROLLER PROVIDES A HARDENED “ROOT OF TRUST”

Foundation of HP PC Security since 2014

Enables Hardware Enforced, Self-Healing, Manageable Solutions Independent of BIOS & Tamper Resistant

Hardened, Cyber-Resilient Protection Against Unexpected Attacks Including Malware of the Future

BELOW THE OS
Firmware (BIOS, etc.)

TRUSTED BIOS
HP Sure Start Gen4

Hardware

HP Endpoint Security Controller
DEFEND AGAINST DEVASTATING FIRMWARE ATTACKS
PROTECT YOUR BIOS WITH HP SURE START GEN4

HP Sure Start is the industry’s first and still the only self-healing BIOS.

The BIOS is the first million lines of code that run. It is the key to your PC’s foundation.

Why should customers care?
Once the BIOS is corrupted, the hackers “own” your PC: all other protection is useless.

Antivirus, anti-malware, and OS firewalls will not detect an infected BIOS!
HP SURE RUN
SECURES KEY PROCESSES THAT SECURE YOUR PC

- Extends self-healing protection of HP’s Endpoint Security Controller into the OS
- Monitors key processes including anti-virus software and firewall
- Immediately alerts of any changes
- Automatically restarts PC if malware detected

*Available on HP Elite products equipped with Intel 8th Generation or AMD Ryzen Pro processors

HP Endpoint Security Controller enables hardware-enforced application persistence
HP SURE RECOVER
SECURE, SELF-SERVICE NETWORK IMAGE RECOVERY

Leverages HP’s Endpoint Security Controller

Executed thru BIOS; protects OS from malware

Provides fast, secure, \textit{automatic} image restoration\(^1\)

Minimizes user downtime and IT effort

Easily manageable with HP Client Security Manager or HP MIK Gen2 plug-in for SCCM

\(^1\) Only available on new HP EliteBook x360 1030 G3 with Intel 8th Generation processors.

\(^2\) Available on new HP EliteBook 800/700 G5 series and requires an open, wired network connection.

Because HP Sure Recover\(^4\) is based in hardware, you can reimage a PC, \textit{even from a blank or wiped hard drive}
CLICK WITH CONFIDENCE
Open attachments and work online with HP Sure Click

SECURE BROWSING
Stay protected from bad websites - just close the tab, and the malware is gone

FILE PROTECTION
Protects against malware lurking in common files. In addition to .pdf files, HP Sure Click now protect users viewing Word, Excel, and PowerPoint files

COMPLEMENTS MICROSOFT EDGE
While Microsoft continues to enhance the security of its Edge browser, HP Sure Click covers Internet Explorer users

---

1 Available on select HP platforms and supports Microsoft® Internet Explorer, Google Chrome, and Chromium™. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files in read only mode.
2 Check platforms as they become available.

---

HP Confidential. For use with HP customers under HP CDA only.
HP SURE CLICK Gen2
HARDWARE-ENFORCED PROTECTION FOR SAFE BROWSING

Isolates malware in it’s own CPU-isolated virtual machine where it cannot infect your PC

Protects against infected PDF and Microsoft Office files

Just close the browser tab... and the malware is gone!

Compatible with Internet Explorer, Google Chrome and Chromium browsers
HP Elite PCs with HP Sure Click\(^8\) offer secure, hardware-enforced protection for browsing the internet.

- **HP Sure Click\(^8\)** isolates malware attacks.
- **HP Sure Run\(^3\)** ensures HP Sure Click\(^8\) isn’t disabled.
- **HP Sure Start\(^2\)** protects the SMM, and enforces HP Sure Run\(^3\).
WORK FREELY IN PUBLIC SPACES
HP SURE VIEW GEN2: THE WORLD’S ONLY INTEGRATED PC PRIVACY SCREEN

HP Sure View Gen2 protects against visual hacking with the press of a button

Privacy at the push of a button

Provides better visual experience in light or dark environments – from plane to the café

What’s New

• Option across EliteBook 1000 & 800 series
• Ultra-bright IPS LCD technology
• Thinner panel; ideal for ultra-thin designs
• 120Hz refresh rate for smoother motion
HP MULTI-FACTOR AUTHENTICATE GEN2
HARDENED SECURITY EASILY MANAGEABLE

NOW SUPPORTS:

FACIAL RECOGNITION
Login with a look using the optional IR camera

MULTI-FACTOR VPN CREDENTIALS
Secure the company when mobile workers connect outside the workplace.

UP TO 3 FACTORS
1 million times more secure when with 3 factors. Ideal for users who have access to the most sensitive info.

Harden authentication policies with an HP exclusive integrated and manageable implementation of Intel® Authenticate (v3)
SECURING PCs – BEST PRACTICES
Enable Multi-Factor Authentication (MFA)

• Multi-factor authentication (MFA) requires you to use two or more independent credentials to prove your identity, substantially increasing your level of security.

• Credentials can be something the user knows (passwords or PINs), something the user has (Bluetooth® phones or smartcards), or something the user is (facial or fingerprint recognition).

• If one factor is compromised or broken, the attacker still must face a second and different type of barrier.

• HP MFA and Intel® Authenticate both allow for multiple authentication factors to be required at every login attempt.
• If your device or service doesn’t support MFA, the next best option is making that one password work as hard as it can.
  • Most people do not have strong passwords because they simply don’t understand how to create them, assuming it would probably be an arbitrary combination of letters, numbers, and symbols.
  • There are stronger and simpler ways to dramatically increase your level of password protection by deploying strong passwords.

• Use a password manager.
  • Password managers work by generating and storing long, complicated passwords for each of your online accounts — freeing you from remembering them.
  • Generally, you’ll only need to remember one password: the master password to your “vault”. Password manager setup is simple, and the process is usually the same.
  • Most password managers will require you to manually update your old passwords: log in to your account, go to your account settings, and let your password manager generate a new, more secure password.
SECURING PCs – BEST PRACTICES
Use Anti-Malware Software

- The bombardment of viruses on your endpoint is constant, so a tool that protects it must be strong, deeply rooted, and regularly updated.

- Anti-malware software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses (and other malicious software such as worms, trojans, adware, and more).

- A typical anti-malware program will scan your system on a regular schedule and automatically remove malware it finds, as well as alert you about dangerous downloads and software updates.

- HP Sure Run should be deployed to ensure that your anti-malware software always remains up and running.
SECURING PCs – BEST PRACTICES

Keep Your Software Up To Date

• If your software is not up to date, it might be missing important security patches to newly-discovered vulnerabilities.

• Older or discontinued software may no longer receive security updates. As time goes by, cyber-criminals could find vulnerabilities in published software and take advantage of these findings.

• Patching older software isn’t the same as updating to the latest version – the older your software, the less secure it is.
SECURING PCs – BEST PRACTICES
Secure Your Browser

• Not all browsers are created equal! Internet Explorer, Edge, and Chrome all offer strong security features.

• Enable automatic browser updates through Settings.
  • Ensures that all security updates are applied to your browser, making it much safer and increasing the chance that malware attacks will fail.

• Heed warnings from your browser!
  • Many browsers have a basic threshold for detecting malicious websites and will display a warning if they believe there to be a reasonable threat.
  • Some also offer URL “autocorrect” features, to prevent navigating to a commonly misspelled domain (where malicious software and sites are often hosted).
  • Restrict content by disabling JavaScript and Flash, as these can increase your vulnerability on the internet.
Because routers transmit ALL the data that flows into and out of your business, including credit card information, routers have long been a favorite target for hackers.

Routers have been cited as the most frequently exploited type of endpoint attacks.

What to do to secure your network:

- Always secure your routers with non-default, strong administrator passwords.
- Configure encryption – Most wireless routers support four wireless encryption standards: WEP (weakest), WPA (strong), WPA2 (stronger), and WPA3 (strongest). Go with the highest encryption standard supported by your routers.
- Keep the router firmware up to date, as a router with the latest updates is much less likely to be infected by malware.
- Most router vendors apply firmware updates automatically without requiring customers to perform this operation.
SECURING PCs – BEST PRACTICES
Stop Visual Hackers

• As the modern workplace continues to move outside traditional offices to remote and public spaces, the possibility of being “visually hacked” is more real than ever.
  • Visual hacking may be the most underrated, low-tech threat businesses face today (simple, effective, and often goes unnoticed until it is too late)

• Limit your exposure to visual hacking via privacy screens.

• Many HP PCs offer HP Sure View, an integrated privacy screen designed to deter visual hacking.
SECURING PCs – BEST PRACTICES

Encrypt Your Data

• When an endpoint is lost or stolen, the hard drive is the first point of attack. Only a few screws hold it in place, and once removed, it can be mined on another device.

• Hardware encryption is the preferred recommendation, but software solutions can also be considered.

• Never store your data unencrypted under any circumstances!

• Some options to consider –
  • Use self-encrypting drives.
  • If available on your endpoints, turn on Trusted Platform Manager (TPM), which activates a security chip within your device to encrypt your new passwords and data on the drive; the TPM prevents access to encrypted data if it detects the system has been tampered with while turned off.
  • BitLocker (Windows 10) provides software encryption that is unlocked with a hardware key.
SECURING PCs – BEST PRACTICES
Secure Your Devices Below The OS

• If a hacker gains access to your BIOS, they essentially own every aspect of your device.

• OS tools such as anti-malware and OS firewalls will not be able to detect or prevent an attack of the BIOS.

• To protect the BIOS settings from being changed by unauthorized users, set a strong BIOS admin password.

• To ensure that your BIOS is never hacked, use HP Sure Start!
EVERY PC & PRINTER DECISION IS A SECURITY DECISION.
Exclusive Premiere
TRUE ALPHA

Room 802 – October 3rd

Showtimes:
12:30 pm - 1:00 pm
1:30 pm - 2:00 pm
2:30 pm - 3:00 pm
3:30 pm - 4:00 pm

- Popcorn!
- Sodas!
- Alcohol!
- T-Shirts!
THANK YOU!