The Printer Working Group

IPP Workgroup Session

May 7, 2024

Before We Begin...

- PWG Antitrust Policy:
  - https://www.pwg.org/chair/membership_docs/pwg-antitrust- policy.pdf
  - The IEEE-ISTO Printer Working Group ("PWG") will not become involved in the business decisions of its Members. The PWG strictly complies with applicable antitrust laws. Every PWG meeting attendee shall comply with this policy. The PWG Officers and PWG Workgroup Officers are responsible to ensure that this policy is adhered to in all PWG activities.
- PWG Intellectual Property Policy:
  - https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf
  - TL;DR: Anything you say in a PWG meeting or email to a PWG address can be used in a PWG Document
  - (but please do read the IP policy above if you haven't done so)
- **This meeting is being recorded to assist in preparation of minutes but will not be published**

Agenda (1/2)

May 7, 2024 (US Eastern Standard Time)

When	What
10:00 - 12:00	OpenPrinting
12:00 - 12:45	Lunch Break
12:45 - 13:45	PWG Plenary
13:45 - 14:15	IPP WG: Status / Prototype-Ready Specifications
14:15 - 14:45	Break
14:45 - 15:30	IPP WG: 3D Printing
15:30 - 17:00	IPP WG: IPP Shared Infrastructure Extensions v1.1

Agenda (2/2)

May 8, 2024 (US Eastern Standard Time)

When	What
10:00 - 12:00	IDS WG
12:00 - 12:45	Lunch Break
12:45 - 13:15	IPP WG: Strong Device Identity BoF
13:15 - 14:45	IPP WG: IPP System Service v1.1, IPP Everywhere v2.0
14:45 - 15:00	IPP WG: Next Steps

Charter

- Current charter:
  - https://ftp.pwg.org/pub/pwg/ipp/charter/ch-ipp-charter-20210409.pdf
- Stable draft charter for 2024-2025:
  - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ipp-charter-20240309.pdf
  - **PWG Call for Objections ends May 10, 2024 (this Friday)**
- The Internet Printing Protocol (IPP) workgroup is chartered with the maintenance of IPP and the IETF IPP registry, and support for new clients, network architectures (Cloud, SDN), MFD/Imaging service bindings, and emerging technologies such as 3D Printing
- In addition, we maintain the IETF Finisher MIB, Job MIB, and Printer MIB registries, the PWG MIBs, the PWG Semantic Model schema, and handle synchronization with changes in IPP

Errata

- Pending:
  - PWG 5100.6-2003 (IPP Page Overrides v1.0): 2 issues
  - PWG 5100.8-2003 (IPP "-actuals" v1.0): 1 issue
  - PWG 5100.9-2009 (IPP Printer State Extensions v1.0): 2 issues
  - PWG 5100.15-2014 (IPP FaxOut v1.0): 2 issues
  - PWG 5100.19-2015 (IPP Implementor's Guide v2.0): 9 issues
  - PWG 5107.3-2019 (MFD Alerts v1.1): 1 issue
- In-Progress:
  - PWG 5100.5-2019 (IPP Document Object v1.1): 4 issues
  - PWG 5100.11-2010 (IPP JPS2/Enterprise Printing Extensions v1.0): 7 issues
  - PWG 5100.12-2015 (IPP 2.0, 2.1, and 2.2): 2 issues
  - PWG 5100.14-2020 (IPP Everywhere v1.1): 4 issues
  - PWG 5100.18-2015 (IPP Shared Infrastructure Extensions v1.0): 8 issues
  - PWG 5100.20-2020 (IPP Everywhere v1.1 Self-Cert): 1 issue
  - PWG 5100.22-2019 (IPP System Service v1.0): 3 issues

IPP OAuth Extensions v1.0 (OAUTH)

- Prototype draft:
  - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippoauth10-20230814-rev.pdf
- Goals:
  - Define/reference best practices for using OAuth/OpenID with IPP
  - Prototype/deploy OAuth/OpenID support for printing
- Prototyping Status:
  - OAuth (JWT) and X.509 support code is available in libcups v3 and CUPS 2.5
  - https://github.com/OpenPrinting/cups/tree/master
  - https://github.com/OpenPrinting/libcups/tree/master
  - https://github.com/OpenPrinting/cups-local/tree/master
  - https://github.com/OpenPrinting/cups-sharing/tree/master
- Proposed Schedule:
  - Stable draft Q3 2024

IPP Encrypted Jobs and Documents v1.0 (TRUSTNOONE)

- Prototype draft:
  - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ipptrustnoone10-20210519.pdf
- Goals:
  - Provide end-to-end privacy and integrity of IPP Job/Document attributes and Document data, even through intermediaries
- Prototyping status:
  - Initial support code started in libcups project (not complete, needs refactoring)
  - https://github.com/OpenPrinting/libcups/tree/smime
- Proposed schedule:
  - Stable draft Q4 2024

Other Working Drafts

- IPP Document Object v1.2 (DOCOBJECT):
  - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippdocobject12-20240301.pdf
  - Stable draft
  - **PWG Call for Objections ends May 17, 2024**
- IPP Wi-Fi Configuration Extensions v1.0 (WIFI):
  - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippwifi10-20240102.pdf
  - Prototype draft
- Internet Printing Protocol/2.x Fourth Edition (BASE):
  - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippbase23-20240504.pdf
  - Stable draft
- ACME-Based Provisioning of IoT Devices:
  - https://datatracker.ietf.org/doc/draft-sweet-iot-acme/
  - Currently awaiting decision from IETF Area Directors

The Printer Working Group

Break

May 7, 2024

IPP workgroup resuming at 14:45pm ET

3D Printing and Scanning Discussions

- Current documents:
  - PWG 5100.21-2019: IPP 3D Printing Extensions v1.1
  - PWG 5199.5-2017: PWG 3D Print Job Ticket and Associated Capabilities v1.0 (PJT3D)
  - PWG 5199.7-2019: PWG Safe G-Code Subset for 3D Printing v1.0
- Discussion:
  - PWG Safe G-Code for sharing test files
  - Common Criteria certification of 3D printers
  - Secure job submission/monitoring via IPP

PWG Safe G-Code for Sharing

- Opportunities for Promoting the Benefits of Using PWG Safe G-Code with 3D Concrete Printing at Conferences
  - The ASTM International Conference on Additive Manufacturing (ICAM 2024 – Oct 28-Nov 1, 2024 – Atlanta, GA)
    - https://amcoe.org/event/icam2024/
  - 4th RILEM International Conference on Concrete and Digital Fabrication (Digital Concrete 2024) – September 4-6th, 2024 in Munich, Germany
  - Transportation Research Board Conference on Advancing Additive Manufacturing and Construction in Transportation – November 7-8, 2024 in Irvine, CA
- Use cases:
  - ???

IPP Shared Infrastructure Extensions v1.1 (INFRA)

- Interim draft:
  - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippinfra11-20240226-rev.pdf
- Errata update of PWG 5100.18-2015:
  - Fixed typos
  - Updated references
  - Reference OAUTH and SYSTEM specifications
  - Sync up with EPX - Release Printing and Proof Printing
- Discussion:
  - Release Printing
  - Resource URIs and Authentication
- Proposed schedule:
  - Prototype draft Q2 2024

INFRA: Release Printing

- Q: How to support Release Printing via INFRA?
  - https://www.pwg.org/archives/ipp/2024/021557.html
- Option 1 - Mode Configuration Attribute (what is in the current draft):
  - Define new "printer-mode-configured (type2 keyword)" and "printer-mode-supported (1setOf type2 keyword)" Printer Description attributes. The value 'immediate' means the Printer is configured to schedule and print jobs immediately while 'release-printing' means that the Printer is configured to hold jobs until they are released at the printer console.
  - The Proxy looks for the value of the "printer-mode-configured" attribute and either accepts all queued jobs immediately ('immediate') or waits to accept jobs until the end user releases them from the printer console.
  - *This is a simple mode switch and doesn't give the end user an opportunity to choose a different mode.*
- Option 2 - Rely on 'pending-held' Job State and Defaults:
  - Document that the "job-release-action-default" and "job-release-action-supported" Printer Description attributes control whether jobs are printed immediately or held for release. The "job-password" and "job-password-encryption" operation attributes can also be used for PIN/password printing.
  - The Proxy accepts any job in the 'pending' state immediately but waits until the end user releases any 'pending-held' jobs from the printer console before printing those.
  - *This is more flexible, allowing both immediate and release printing with the same printer. But if the xxx-default/supported values are not configured correctly an end user could bypass the mode wanted by the administrator.*

INFRA: Resource URIs and Authentication

- Q: How to support resource URIs with authentication?
  - Also, do these URIs need to use the same host/domain name as the Printer/System?
  - https://www.pwg.org/archives/ipp/2024/021572.html
- INFRA requires that all resources be accessible Public Internet Accessible URIs, which can be accessed via the public Internet without additional credentials or authentication.
- Intent was to allow authentication as long as the *same* credentials can be used.
- Should we require using the same host/domain name (W3C "Same Origin" policy)?
  - What about resources that do not require special handling/protection (ICC profiles, printer icons, strings files, etc.)?

The Printer Working Group

IPP Workgroup Session

May 8, 2024

Before We Begin...

- PWG Antitrust Policy:
  - https://www.pwg.org/chair/membership_docs/pwg-antitrust- policy.pdf
  - The IEEE-ISTO Printer Working Group ("PWG") will not become involved in the business decisions of its Members. The PWG strictly complies with applicable antitrust laws. Every PWG meeting attendee shall comply with this policy. The PWG Officers and PWG Workgroup Officers are responsible to ensure that this policy is adhered to in all PWG activities.
- PWG Intellectual Property Policy:
  - https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf
  - TL;DR: Anything you say in a PWG meeting or email to a PWG address can be used in a PWG Document
  - (but please do read the IP policy above if you haven't done so)
- **This meeting is being recorded to assist in preparation of minutes but will not be published**

Agenda

May 8, 2024 (US Eastern Standard Time)

When	What
10:00 - 12:00	IDS WG
12:00 - 12:45	Lunch Break
12:45 - 13:15	IPP WG: Strong Device Identity BoF
13:15 - 14:45	IPP WG: IPP System Service v1.1, IPP Everywhere v2.0
14:45 - 15:00	IPP WG: Next Steps

Strong Device Identity BoF

- Now tracking on the "ippsample" wiki:
  - https://github.com/istopwg/ippsample/wiki/Strong-Device-Identity
- Primary use cases:
  - Robustly validate the provenance of a device (printer, etc.) discovered on a LAN
  - Establish trust with printer discovered on LAN
  - Correlate / validate identity of a printer discovered on the LAN with printer found via some other listing service (e.g., LDAP, cloud print server, Wi-Fi Direct, etc.)
  - Validate that the software running on a device has not been tampered with by a third party malicious actor, using a Client connected to the device via a LAN

Strong Device Identity – Who needs it?

- Increasing need for robust trust establishment now includes the home and small business environments
  - Zero Trust Networks
  - Hybrid work environments driving this into the home, but still using enterprise (awkward) workflows
  - Growth of IoT is creating a second more trustworthy "realm" within a home network
- Legacy trust establishment (self-signed certificates / TOFU / certificate pinning) nearing threshold of unacceptability
  - Trust on First Use has no system for initial validation
- Printers are either basically untrusted or have trust established using "enterprise" credential provisioning, which is awkward and unwieldy for home / SMB market segment

Trust on First Use

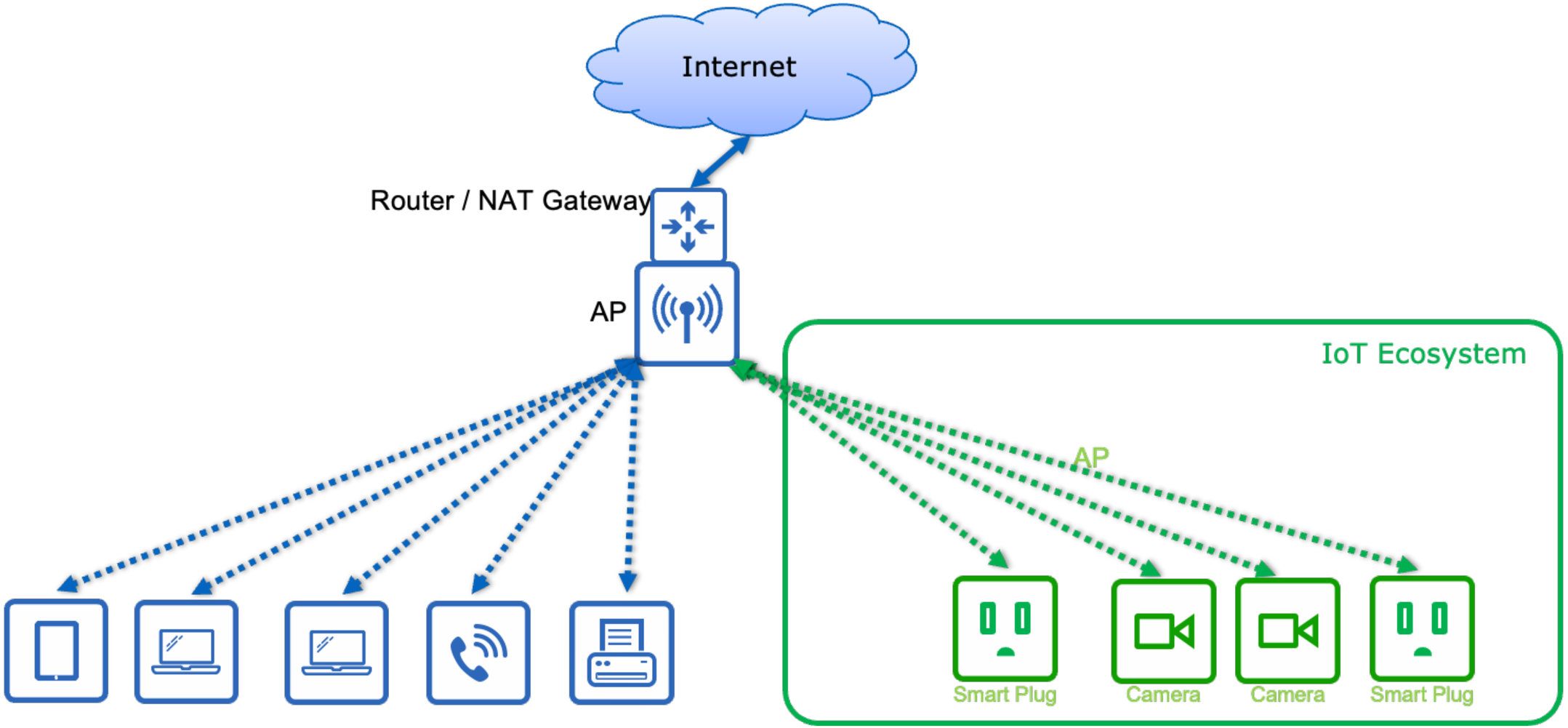
- Device joins network
- Client connects to Device via TLS
  - If the device is unrecognized (no entry in cache for whatever identifying keys are used), cache TLS server cert for that device and trust it***
  - If the device is recognized and the cert hasn't changed, continue to trust it
  - If the device is recognized but the certificate has changed, suspend trust and request user intervention

***** Validation in a web browser is awkward; most print systems trust with no validation**

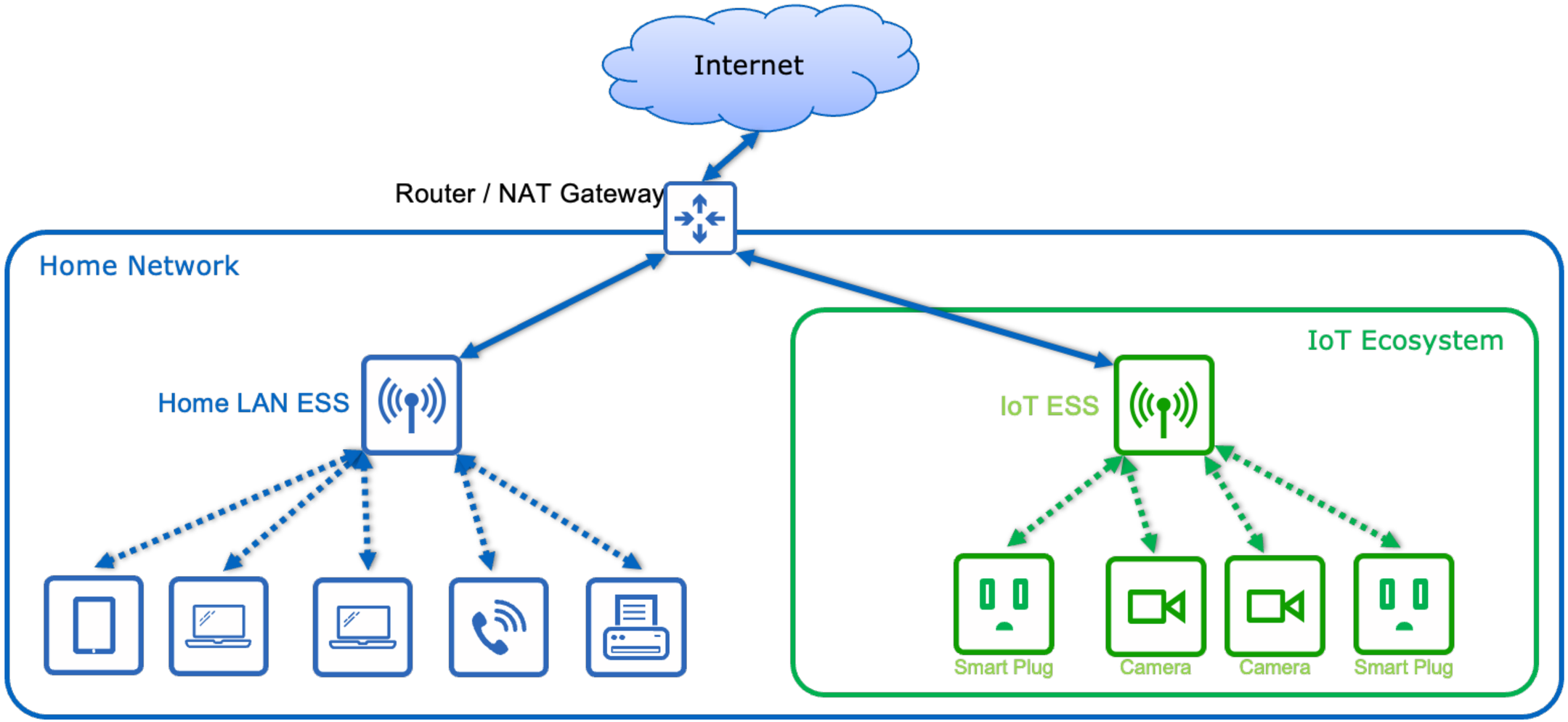
Strong Device Identity vs. Device Attestation

- What is the difference?
  - Device Identity: Verifiable individual identity and manufacturer identity
  - Device Attestation: Device Identity + verifiable device health assertions (software / firmware is unaltered)
- Do we need Device Attestation, or is Device Identity good enough?

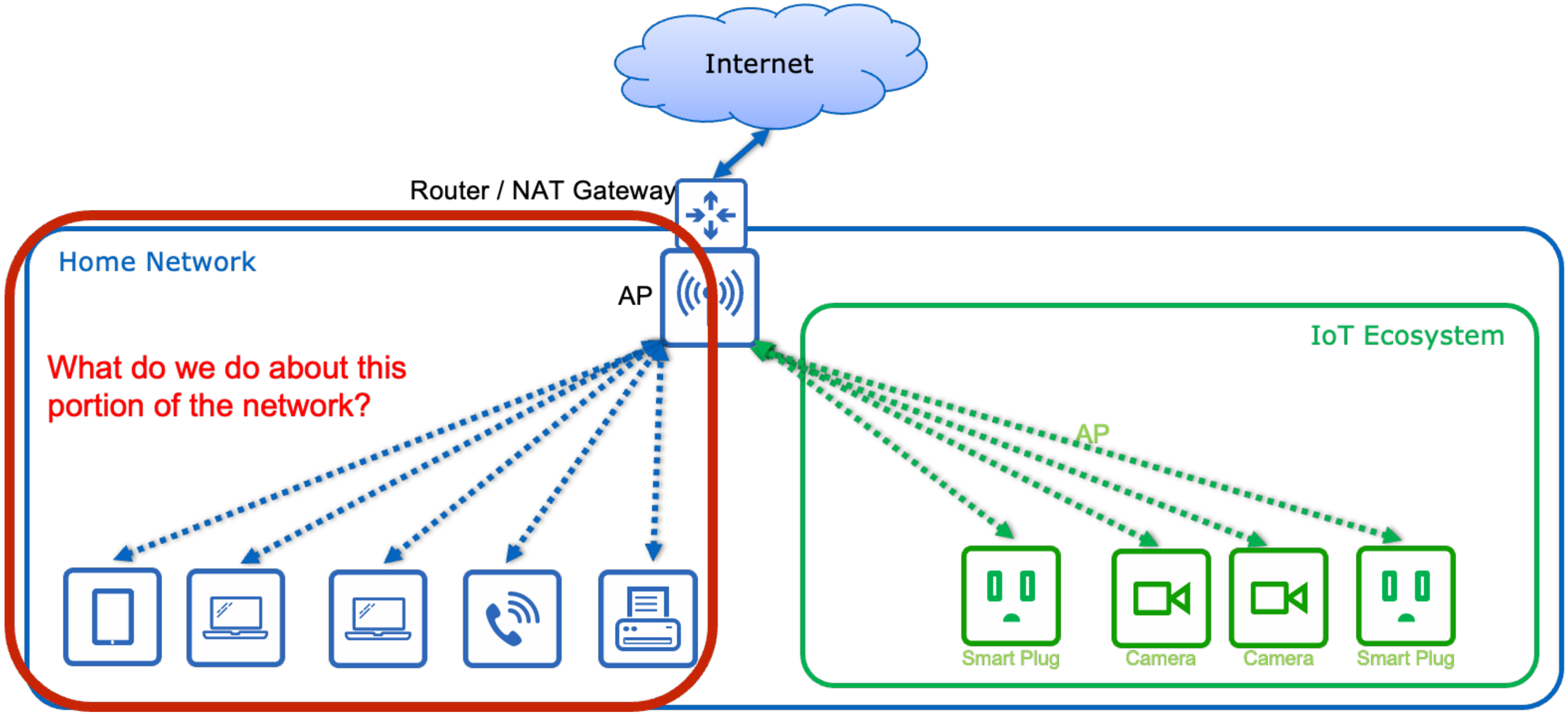
Home Network



Home Network



Home Network



Strong Device Identity

- Bring IoT trustworthiness to all ~~home~~ networks

Use Case 0: Adding a Trusted Device to a Home Network

User is a home owner who buys a printer and attaches it to their network via an Ethernet cable.

A Network Manager daemon running on the User's home router notifies the agent app on the User's phone that a new device has been added to the network, indicating that it will be isolated until the Printer's identity and assertions of health have been validated, and requests approval to perform the validation. The User approves the offer.

The Network Manager performs the validation, which succeeds. The User points their laptop's browser at the Printer to configure some settings, and the browser trusts the Printer because it is now holding a TLS certificate issued by a CA associated with that network.

USE CASE 1 (Positive): Validate the Provenance of a Printer Discovered on a LAN

Vicky goes to work, sits down at an available hot desk, and connects her laptop to the office LAN Wi-Fi network. She switches windows to a presentation she's working on, clicks "File" >>> "Print", and looks at the available printers.

Her laptop's print system discovers an IPP print service, validates that it is hosted on a physical printer with a known provenance and is in a healthy state, and offers that printer as a selection with a badge indicating that it is verified to be a printer and is safe to use.

USE CASE 1 (Negative): Validate the Provenance of a Printer Discovered on a LAN

Rafa goes to work, sits down at an available hot desk, and connects his laptop to the office LAN Wi-Fi network. He switches windows to a presentation he's working on, clicks "File" >>> "Print", and looks at the available printers.

His laptop's print system discovers an IPP print service, but the laptop is unable to validate that it is hosted on a physical printer with a known provenance and is in a healthy state. The laptop offers that printer as a selection with a warning badge indicating that it is not verifiable to be a printer that is safe to use.

USE CASE 2 (Positive): Establish trust with printer discovered on LAN

Vicky chooses the printer from USE CASE 1 and clicks "Print". Since the laptop has validated that the printer is a printer and is healthy, it can categorize this printer as a more trustworthy printer than other printers.

USE CASE 2 (Negative): Establish trust with printer discovered on LAN

Rafa chooses the printer from USE CASE 1 (Negative) and clicks "Print".

Since the printer has been provisioned with a self-signed certificate, it will be accepted only via the weaker TOFU trust model.

USE CASE 3 (Positive): Correlate identity of LAN discovered printer with one found via other methods

The printer Vicky is using is also discoverable over Wi-Fi Direct. An identifying value provided by the printer over the LAN is also available via Wi-Fi Direct, so the laptop is able to robustly identify that a discovery listing for LAN and a discovery listing for Wi-Fi Direct are in fact the same device.

The laptop lists the printer only once.

USE CASE 3 (Negative): Correlate identity of LAN discovered printer with one found via other methods

A malicious third-party device advertises itself as a printer via Wi-Fi Direct. It identifies itself using the "printer-uuid" value queried via IPP on the LAN.

The laptop uses "printer-uuid" to search for a match on Wi-Fi Direct, and believes it has found a match, not recognizing that if the job is sent over Wi-Fi Direct, it will pass through the malicious third-party device.

Technologies to Consider

- Matter IoT Device Attestation
- IEEE 802.1AR / TPM

Matter IoT Device Attestation

- Taken from the new Matter Handbook:
  - https://handbook.buildwithmatter.com/howitworks/attestation/

- During the commissioning process, a device cryptographically proves (attests) to the commissioner that:
  - it is a genuine product
  - it is a product that passed Matter compliance tests and has been thus certified by CSA.

- In order to accomplish those goals, the device carries:
  - A Device Attestation Certificate (DAC) that conveys device's manufacturer ID (VID) and product ID (PID). The DAC chains up to a set of trusted roots, approved by CSA members.
  - A securely-stored, private key associated with the public key stored in the DAC that proves the device owns this unique certificate.
  - Certificate declaration is a statement cryptographically signed by CSA that states that a tuple (VID,PID) has passed Matter compliance tests.

IEEE 802.1AR / TPM

- IEEE 802.1AR-2018
  - "C.2 DevID uses in consumer devices
  - End users are not expected to directly use the IEEE 802.1AR device identity. Instead the DevID is expected to be used by a home networking access point or router. These devices provide network connectivity to all devices on the home network and also provide security mechanisms such as passwords or Web-based authentication.
  - Often routers and access points also include a mechanism for limiting which devices can join the network through configuration of a list of allowed MAC addresses or other device identifying information. The IEEE 802.1AR device identity can be used as a secure form of identity for these purposes. Vendors that include human readable identity information within the DevID subject field, or use a machine readable serialNumber attribute, or the subjectAltName hardwareModuleName, can provide integrated solutions with interfaces that are both more user-friendly and more secure than current MAC address-based solutions.

IPP System Service v1.1 (SYSTEM)

- Prototype draft:
  - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippsystem11-20240504-rev.pdf
- Errata update of PWG 5100.22-2019:
  - Fixed typos
  - Updated references
  - Merged System Service Discovery registration content
  - Added Register-Output-Device extensions for X.509 authentication
- Proposed schedule:
  - Stable draft Q3 2024

IPP Everywhere v2.0

- Prototype draft:
  - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippeve20-20240426-rev.pdf
- Major update of PWG 5100.14-2020: IPP Everywhere v1.1
  - Most RECOMMENDED items become REQUIRED
  - New CONDITIONALLY REQUIRED items
  - REQUIRE "printer-firmware-xxx" Printer Status attributes
  - REQUIRE Get-Printers from PWG 5100.22 for print servers
  - RECOMMEND IPP-USB support
- Prototyping Status:
  - Mostly in shipping printers; dependent specifications are prototyped separately
- Proposed Schedule:
  - Stable draft Q3 2024

IPP Everywhere Printer Self-Certification Manual v2.0

- Initial Draft:
  - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippeveselfcert20-20220510.pdf
- Major update to PWG 5100.20-2020
  - Synchronize with changes in IPP Everywhere v2.0
  - Add IPP-USB support (particularly for USB-only printers)
  - Add feature tests for duplex, finishings, roll, tray
  - Add Get-Printers test for servers
- Prototyping Status:
  - Mike is working on updates to the ippeveselfcert repository
    - https://github.com/istopwg/ippeveselfcert
  - Flutter-based "ippevetool" application taking shape, can be run from Visual Studio Code
    - Short demo
- Proposed Schedule:
  - Prototype draft and beta tools Q3 2024

The Printer Working Group

Next Steps

Next Steps (1/2)

- Internet Printing Protocol/2.x Fourth Edition (Mike)
  - PWG Last Call in Q3 2024
- IPP Document Object v1.2 (Mike)
  - **PWG Call for Objections ends May 17, 2024**
- IPP Encrypted Jobs and Documents v1.0 (Mike/Smith)
  - Stable draft in Q4 2024
- IPP Everywhere v2.0 (Mike)
  - Stable draft in Q3 2024
- IPP Everywhere Printer Self-Certification Manual v2.0 (Mike)
  - Prototype draft in Q3 2024
- IPP OAuth Extensions v1.0 (Mike/Piotr)
  - Stable draft in Q3 2024

Next Steps (2/2)

- IPP Shared Infrastructure Extensions v1.1 (Mike)
  - Prototype draft in Q2 2024
- IPP System Service v1.1 (Mike)
  - Stable draft in Q3 2024
- IPP Wi-Fi Configuration Extensions v1.0 (Mike)
  - Stable draft in Q3 2024

More Information

- We welcome participation from all interested parties
- IPP Working Group web page
  - https://www.pwg.org/ipp/index.html
- Subscribe to the IPP mailing list
  - https://www.pwg.org/mailman/listinfo/ipp
- IPP WG holds bi-weekly phone conferences announced on the IPP mailing list
  - Next conference calls scheduled for Thursday, May 23 and June 6, 2024 at 3pm ET