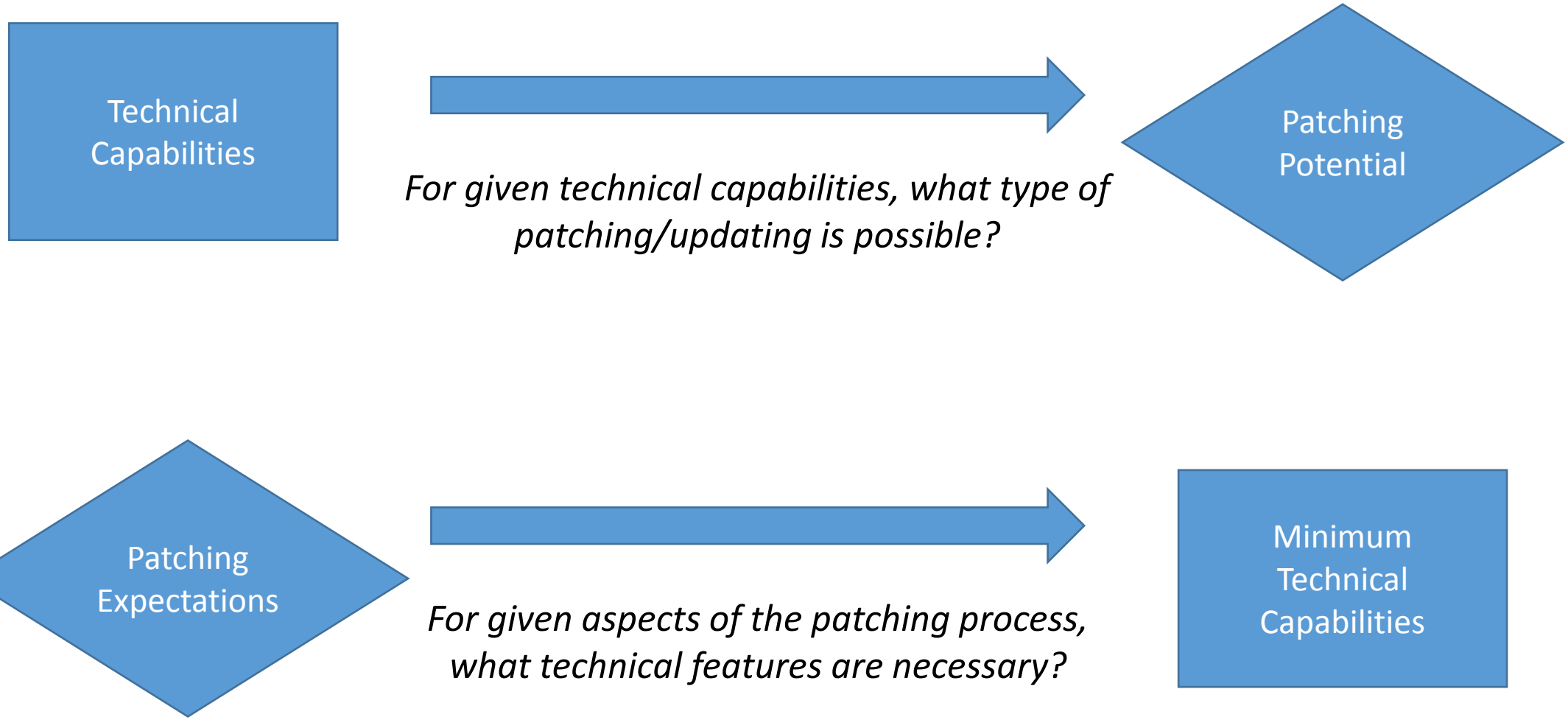
WG2: Capabilities and Expectations

NTIA Multistakeholder Process on IoT Upgradability and Patching

Jan 31 Virtual Meeting

Two initial approaches



Steps in patching – An idealized model

- Transmit the updated code
  - Secure transmission: validate the source
  - Transport layer security to encrypt the patch
  - Mutual authentication is necessary
    - The small device has to have a pre-programmed public key
  - Possibly a physical update (USB, etc)
- Decrypt file, verify signature.
  - Credentials may need to be stored securely.
- Securely store file
- Awareness of presence of update
- File manipulation: unpacking, etc
- Verify that the new file is appropriate
- Selection of time to apply the update
- Apply update step
  - …
  - [Want to stay general purpose]
- Detect the failure of the update, and have a ‘fail safe”
  - Potential fall back to last good state, or even factory default.
  - Assumes further storage and state capabilities
- Rebooting / reset / restart
  - Generic: activate new code or components
  - Potentially a secure boot.
- Post-processing: help the system know how to handle the new data / features

What is missing from this model?

IoT Device Categorization

		Device Categories (another path/idea: usage categories such as consumer, manufacturing medical, critical infrastructure, etc.)							
		Micro	Small	Medium	Large	Huge	Controller	Gateway	Composite
Device Capabilities	Network	ZigBee or BLE or serial link (no network)	Cellular and/or WiFi and/or Ethernet and/or Satellite	Cellular and/or WiFi and/or Ethernet and/or Satellite	Cellular and/or WiFi and/or Ethernet and /or Satellite	Cellular and/or WiFi and/or Ethernet and/or Satellite	Cellular and/or WiFi and/or Ethernet and/or Satellite	Cellular and/or WiFi and/or Ethernet and/or Satellite	<built from composite items>
	Compute	8 /16 bit MCU ARM	32 bit MCU ARM & X-86	32 bit MCU ARM & X-86	32 bit MCU ARM & X-86	32 bit MCU ARM & X-86	32 bit MCU ARM & X-86	32 bit MCU ARM & X-86	As above
	Storage	RAM << 16KB, FLASH << 128KB	RAM ~16KB , FLASH ~128KB	RAM~64KB, FLASH~256KB	RAM~1MB, FLASH~10MB	RAM~1GB, FLASH~16GB	RAM~1GB, FLASH~16GB	RAM~1GB, FLASH~16GB	As above
	OS like primitives	Tiny OS, Contiki, Mantis, Nano-RK, Lite OS, Free RTOS, etc..	RTOS like or as above- No Linux	RTOS like or as above- No Linux	Linux, RTOS-Like	Android, Linux, iOS, Windows 10/IoT	Android, Linux, iOS, Windows 10/IoT	Android, Linux, iOS, Windows 10/IoT	As above
	Application	none	none	several	many	many	none	several	As above
	Power Usage	3-5V, battery, solar	3-5V, battery, rechargeable	3-5V, battery, rechargeable	110-220V, 50-60Hz	3-5V, battery, rechargeable (mDevices), 110V-220V, 50-60Hz			As above
	Human Interaction	none	none	none		human-attended	human-attended	human-attended	As above
	Update Controls	Use intermediate device	Use intermediate device	Use intermediate device					As above
	Expected Lifespan	Long	Long	Long					As above
	Expected Inventory Size	O(Billions)	O(Millions)	O(Millions)	O(Millions)	O(Millions)	O(Millions)	O(Millions)	O(Billions)

Initial findings and tentative assertions

- There is no one-size-fits-all solution for updating.
- Network connectivity is the first constraint.
  - If no TCP/IP stack, then a direct networked update is impossible.
    - Remote update requires specific infrastructure and/or physical contact.
    - Alterantively, gateway/proxy system can buffer and forward update.
  - The ability to have a socket connection is probably sufficient for mutual authentication
    - In some cases, capability for lightweight exchange of keys possible without Trusted Platform Module or similar capabilities.
    - In others, will need strong encryption, secure storage, etc.
- Storage may not be a binding constraint.
  - Many (most?) modern devices have sufficient memory and storage to hold either complete images or partial updates.

Other potential outputs

- Examples of how different types of devices might be upgraded, based on their capabilities.
- Glossary
  - Technical terms for a broader audience
  - Particular steps of the upgrade process

Open questions

- Variable security requirements: consumer needs vs. high security
  - Consumer-grade devices or components may be used in critical infrastructure environments.
  - Should this be explicitly addressed? Or rely on transparency to support sector-specific guidance?
- Network loads of update traffic
  - If there are high numbers of devices, update traffic could have a big impact on network performance.
  - Possible solutions include: random back-off management server-side.
- Significance of operational security
  - Ongoing management by consumer and enterprise
  - Operational monitoring of device status.