THREAT IMMUNE INFOGRAPHIC LABEL OF A DEVICE

HP INC

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation
INC, HP, "THREAT IMMUNE INFOGRAPHIC LABEL OF A DEVICE", Technical Disclosure Commons, (August 06, 2020)
https://www.tdcommons.org/dpubs_series/3502

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.
Threat immune infographic label of a device

Abstract:

A connecting device in a public environment looks for a trusted target device that maintains high security posture. Other devices on the network may learn intent/purpose and might further generate interest of an adversary already performing enticement to lure connecting devices. A visual labels of threat immune in an infographic map provides a subtle information of the trusted target device where a roaming/mobile user need to engage while on the go.

Problem Solved:

In a public domain, a connecting device needs an assurance to choose a trusted target device before engagement. It's tedious task for a roaming/mobile user and brings legal implications as well to probe a target device on security posture without owner's approval. It may further add a complication when connecting device becomes victim of enticement by an adversary who lures others. A roaming/mobile user would need a list of surrounding trusted devices on a infographic or digital map while navigating.

Construction and operation:

There is multiple approach to implement this idea. One of the potential approaches to construct this solution has been described here. And, below diagram shows devices on the Google map those have acquired threat immunity label.

![Diagram of threat immune devices in geolocation map]

Enrollment of threat immune devices in geolocation map

- The confirmation of whether this device is keeping threat immunity or not, there needs to be a flag set on the device. That means “Threat Immunity = True”. The acquisition of threat immunity flag and setting up in the device are owned by device manufacturer. And, a device manufacturer may choose to engage with a custom or proprietary or any other methods to assess threats and certify devices for the threat immunity.
• Pre-condition: device with “Threat Immunity = True” must be set in the device during a manufacturing process or firmware update. The following shows potential steps need to be considered whether device accompanied GPS sensor or not for geolocation tagging/labelling.

Step-1: Devices without GPS (Global Positioning System) navigation sensors & software
• Consider a case of Printer as an IoT – doesn’t ship with a sensor.
• Use mobile App over BLE (Bluetooth Low Energy) or other local wireless connection (802.11 b/g/n) to connect a printer. Upon connection, printer does perform following steps:
  • Collect Mobile’s location (use mobile’s GPS location - latitudes and longitudes)
  • Initiate reverse path/route map to identify the distance between printer and the mobile
  • Calculate Printer’s geo location based on location and distance of Mobile
• Use programming code to automate specification of Geolocation API Navigation
  • Store and publish device location information to a cloud-based service
  • register device in the geo location map using cloud-based service

Step-2: Devices with GPS navigation sensors & software
• Consider a case of Printer (or other IoT) with GPS navigator needed to offer service in public (public print scheme in printer’s case)
• Fetch device location from the device
• Use programming code to automate specification of Geolocation API Navigation to register device in the map
  • Store and publish device location information to a cloud-based service
  • register device in the geo location map using cloud-based service

Benefits: even without GPS sensor, location of device can be determined. Effective to reduce the cost further of IoTs

2

Open mobile app & search for threat immune devices
• Use search field to locate “threat immune” device
• The search field collects request details and passes that to the map program. The scope of discovering devices in an infographic map may vary whether solution has been developed in consideration with vendor neutral or centric approach. Vendor neutral approach needs a wider scope or a discovery platform to determine all sort of IoT devices. However, vendor centric solution needs a narrow scope to determine a device preferably hosted or managed by manufacturer. Any of following approach or a combination can be performed to make necessary changes so to implement narrow or wider discovery mechanism that helps to determine a device in the infographic map.
  • Multicast DNS: Bonjour
    • Can be explored for generic or vendor neutral IoT devices for wider scope by proper modification to this method through forming a required/custom payload
  • Device or network discovery protocols using SNMP
    • Necessary SNMP OIDs & cloud combination-based development could help to implement solution for both vendor neutral and centric device discovery
  • Message broker protocols{software}: RabbitMQ, Kafka, Active MQ etc.
    • Message broker seems suitable for a custom discovery approach by expanding or modifying necessary capabilities in it – an approach manufacturer may want to leverage for device centric discovery. For instance, Printer (as an IoT) manufacturer could use a cloud based RabbitMQ solutions to register and display devices with threat immunity.
• Once discovery method learns about threat immune device list, along with device details it collects device locations and other necessary details acquired in stage
• Program of Mobile calculates nearest device location and shows up in the map, based on its current location and one acquired in above step (of device)

Show up and maintain device label/tag of threat immunity in the infographic map

• Follow Stage 1 to keep information UpToDate in the map when physical position/location or threat immunity of device changes
• This method can be expanded to support service providers in sending notification if the Threat Immune certificate of device is due for renewal etc.

UML sequence diagram of the implementation:

Prior solutions

The most popular google maps, GPS etc. lists devices those are tagged with feature labels or manufacturer specific codes. However, it is found that there is no infographic or digital map exists that shows the list of the devices (printer/IoT) with a threat immunity. And, that too doesn't provide a visual way of trusted public platform to choose

Advantage:

• Visual representation of threat immune labels in a map: great user experience when a map highlights the surrounding devices those are safe to choose
• One need to make multiple filters to know about the surrounding devices – most importantly doesn’t know which one to engage due to lack of trust. Threat Immune labels in a map reduces time & effort to find a trusted device
• One can’t probe a device security posture without prior approval of the owner. Threat Immune labels in a map reduces legal implications - when probing a device security without approval, so no probe required on choosing a safe device.
Disclosed by Verma Manjul, HP Inc.