IoT Location Impact on Network Behavior and MUD

Anat Bremler-Barr ,Bar Meyuhas ,Ran Shister
Reichman University

Supported in part by a Cisco research grant

Research Goal: How the IoT device's location impacts its networking behavior ?

The same IoT device (=same firmware!) acts differently across the globe!

<u>Applications:</u>

- Protect IoT devices by observation abnormal behavior (e.g., as in security MUD Framework, IETF RFC)
- Identify IoT devices based on their network behavior

Learn normal device behavior and then extract rules and features

Device	Israel	China
Domain Names	sg.ots.io.mi.com	Fixed IP
Port	HTTPS (443)	HTTP (80)
IP Resolution	DNS	HTTP Request
Encryption	Standard TLS	Self-signature

Example: Xiaomi Camera

Measurement Setup:

Traffic logs (PCAPs) of 31 IoT devices (plugs, bulbs, cameras, streamers..) deployed in up to 14 countries:

- ***Virtually*** connected to different locations (VPN)
- ***Physically*** connected to different locations [IMC2019]

Create MUD files from PCAP using MUDGEE tool.

- MUD File is network behavior formalization: used by FW to reduce attack surface
- MUD is an Access Control List (ACL), a set of Access Control Entries(ACEs)

ACE = (domain-name/IP/MAC, protocol, source port, destination port, direction)

Observations:

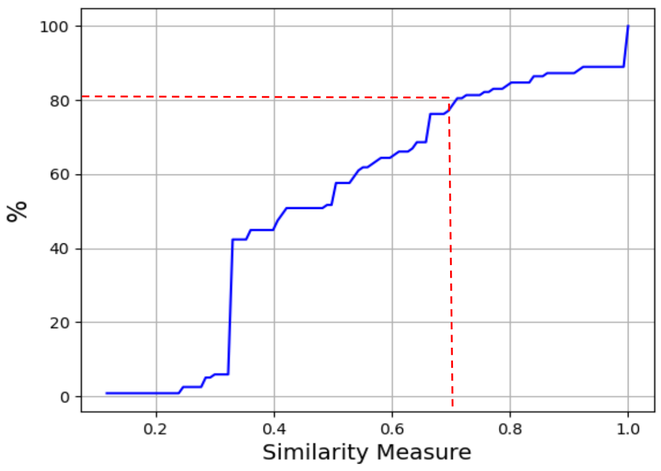
#1: Location impact is very common

- Similarity measure of two MUDs for the same device d, at location i and j is defined:

$$Similarity_d(MUD_i^d, MUD_j^d) = \frac{|MUD_i^d \cap MUD_j^d|}{|MUD_i^d \cup MUD_j^d|}$$

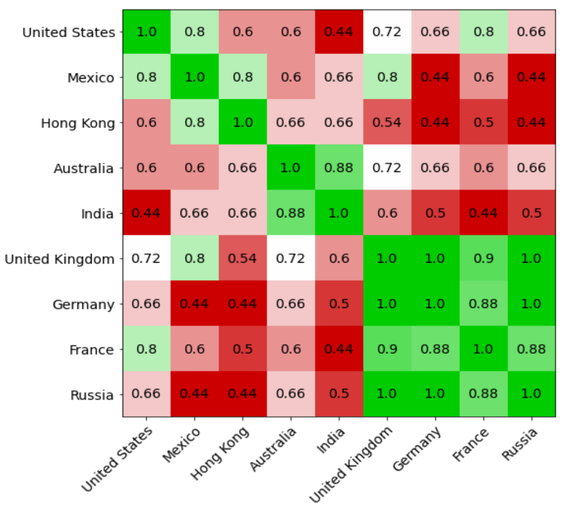
- 80% of the MUD comparisons show similarity measure lowers than~0.7

CDF of MUD similarity measure values

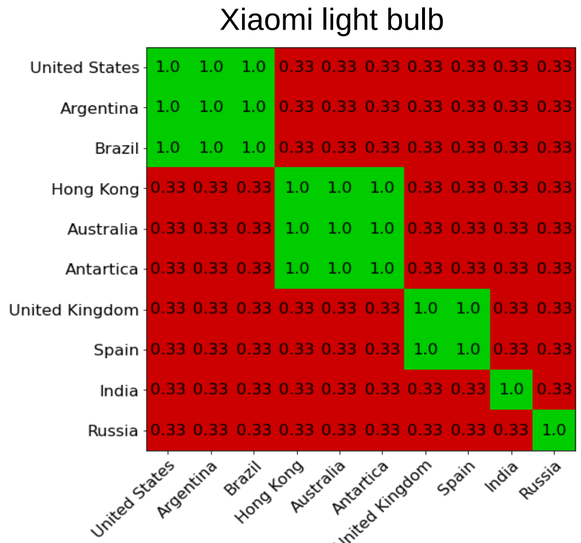


#2: MUD similarity correlates to clouds regions

Yi camera



Xiaomi light bulb



Countries are ordered in the similarity measure's heat-maps according to geographical regions

#3: Different reasons for location impact: cloud regions, CDN-like solution, country encryption policies, privacy regulations (GPDR,FTC) mentioned also in [IMC2019]

#4: Differences mostly in domains:

ru.ot.io.mi.com in Russia vs *de.ot.io.mi.com* in UK → Generalization: **.ot.io.mi.com*

Ongoing work: design a tool to easily compare MUD files and generalize them if possible

BIB: [IMC2019] J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun, and H. Haddadi, "Information exposure from consumer IoT devices: A multidimensional, network-informed measurement approach," in IMC 2019

For more INFO