Project summary

Neuromesh provides a ‘vaccine for IoT’: the lightweight software that is installed on IoT devices (such as web cameras, smart meters, temperature sensors, smart watches, cars) and that prevents bonet attack by creating the mesh network between these devices and storing the access list in the distributed ledger. Each device can identify its peer as potential threat using deep learning technique and vote to exclude it from the distributed whitelist.

Problem

While IoT market is growing at the fast pace (today’s 6.4bn of connected devices is expected to become 20bn by 2020), they are barely protected from cyberattacks. It is expected that ⅔ of all enterprises will experience at least one IoT security breach by 2018. Currently it takes hackers 3 minutes to infect the average IoT device and remediation can take weeks. The main reason behind that is that most of IoT devices use simplified stripped-down version of Linux with key security components frequently omitted. Another reason is the physical memory / processing power limitations that make usage of conventional antiviruses on these devices impossible.

Solution description

Each newly manufactured device will have our software installed and a unique device id assigned. Once connected to the internet, the device would be able to identify other devices with the software installed and request the addition to the p2p network of IoT nodes. The whitelist that governs who the nodes can communicate with is stored in the blockchain. There are following scenarios that can appear in the network:

1.1 Adding device to the whitelist:

Once botnet is installed, it sends device id (key) to command the center, which verifies the device and adds its device id (key) number to the current block with a ‘whitelisted’ marker

- Verification done by Command Center: device is not in whitelist already, device is not in chain marked as removed from whitelist
- Approval of chain addition: authorized nodes (part of command centre) + nodes that communicated with the new device (through multisig)

Once block is approved, it is added to the immutable blockchain and copied to each device in the botnet network

1.2 Removing device from the whitelist:

Each device can submit the removal request for other device to the command center based on suspicious behavior (which is determined by a pattern recognition technology). Command Center verifies the suspicious device and adds device id (key) number to the current block with a ‘removed from the whitelist’ marker

- Verification done by Command Center: device should be in whitelist already
- Approval of chain addition: authorized nodes (part of command centre) + nodes that communicated with the new device (through multisig)

Once block is approved, it is added to the immutable blockchain and copied to each device in the botnet network

1.3 Forming the whitelist:

Each device at any given moment can go through the chain and form the list of the devices that are whitelisted. Based on the device ids (keys) in the whitelist each device with choose to communicate/not communicate with other devices.

Chain architecture

We plan to use one single Ethereum-based blockchain to store all the device ids from various manufacturers. This will prevent the cases when malicious nodes create a branch of the chain that can potentially outgrow the correct ledger. However, such architecture poses a challenge from the computational power side. As mentioned before IoT devices have limited computing power and physical memory. Therefore it costly for these devices to process the blocks for the whole chain and to store the copy of the whole chain locally. That's why we plan to use the sharded blockchain, when each part (shard) of the chain will be processed by a separate group of nodes (the simplest example is that devices with even id numbers will monitor and vote for devices with even id numbers, and devices with odd id numbers will monitor and vote for devices with odd id numbers only). There is an active EIP already on introducing shards technology in Ethereum.

Benefits of the approach

Benefits of such approach are following:

- No centralized storage of whitelist info - no risks of hacking
- Anonymity: only device keys are stored, no other data is visible
- Distributed voting - each new device is added to the whitelist only after txn is signed by their neighbors

Target customers:

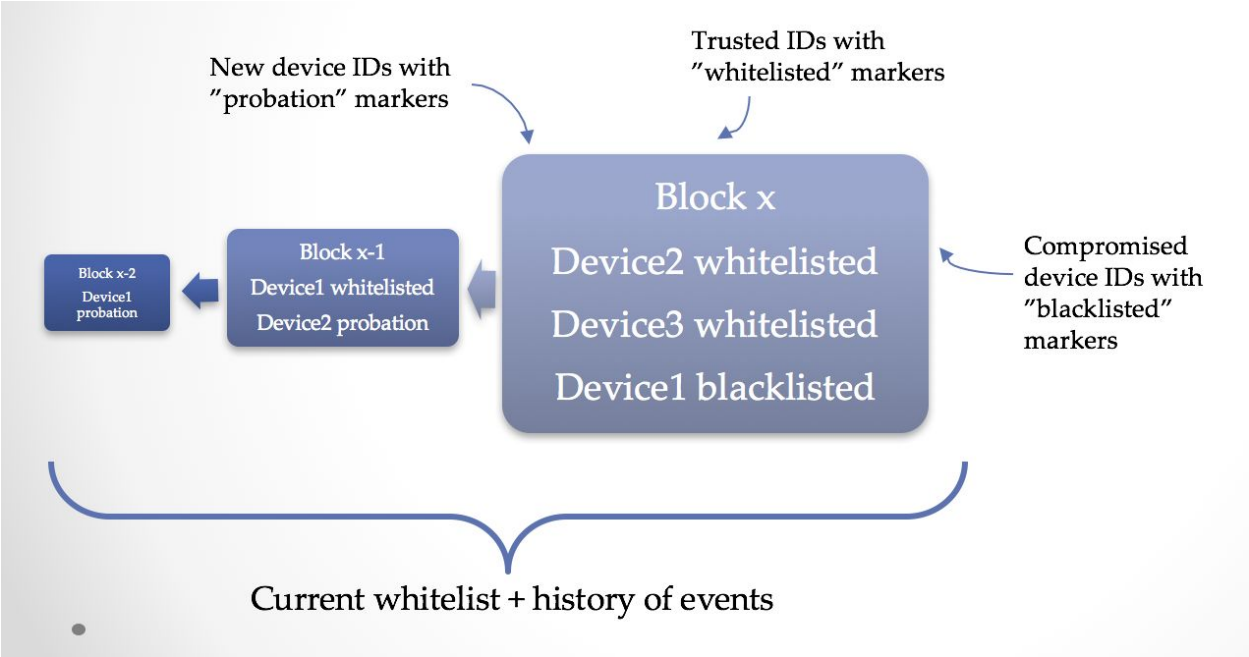
Manufacturers of the "no-frills" IoT devices who care about their PR and litigation risks because of their devices being compromised.
Large users of IoT infrastructure (e.g. power grids using smart meters).

Business model:
We consider several options for our Business Model:

- Regular fee - Neuromesh acts as a managed security service charging device manufacturer and/or user a monthly/annual fee
- Pay per attack attempt - device manufacturer or user would pay a fee for each hackers' attack deflected by Neuromesh

Exhibits:

Ex.1 Blockchain structure



Ex.2 Chain sharding