



IoT Security Function Distribution via DLT

Le Su, Dinil Mon Divakaran, Sze Ling Yeo, Jiqiang Lu, Vrizlynn Thing

Work was done at

Institute for Infocomm Research (I²R), A*STAR, Singapore



Motivation

- IoT devices → while increasingly deployed at enterprise as well consumer networks, also adversely affecting the threat landscape
- Enterprises have multiple levels of security solutions deployed
- Not so for homes/consumers
- Given security-by-design is not a complete solution, what is needed is, easy availability and penetration of IoT solutions in the market

Problem: How to distribute IoT *security functions* efficiently to smart homes?



Outline

- Problem definition
- Overview of the proposed system
- Design
 - Entities and Roles
 - Transactions
 - Smart Contracts
- Discussion on implementation
- Security analysis of the system



Problem

- *Security functions (SFs):* IDS, IPS, DPI, firewall, patches, etc.
- Assuming every smart home premise has an “intelligent” gateway

How can we design a system / network to distribute security functions, in a fast and efficient way?

- Challenges: how to prevent fraudulent entities, and more importantly, their actions that may adversely affect the users of the system

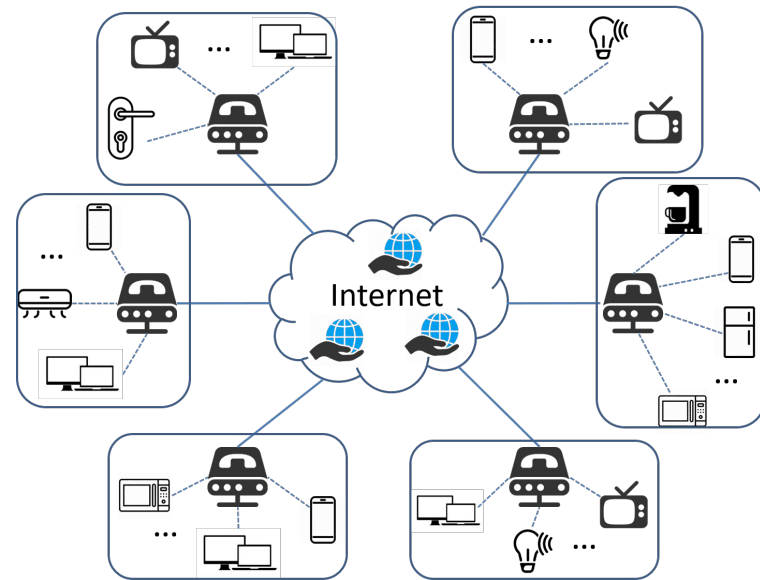


Assumptions

- Every home premise has a gateway
- With sufficient compute and storage resources
- Connected to Internet with, say, 1Gbp link
- Gateway has an IP address and its own public-private key pair
- Each device trusts its gateway

System overview

- A network of nodes, all connected to the Internet
- Node: gateway or SSP (security solution provider)
- SSPs develop SFs for various device types
- SSPs and gateways form a P2P network
 - A distributed ledger network
- Network controlled and managed by:
 - An alliances of ISPs [1]
- Briefly: SSPs distribute SFs over network, gateways evaluate them for devices, records reviews on the network, and may purchase the SFs subsequently.
 - Build a reputation system using the evaluations



[1] "Global cyber security alliance formed by Etisalat, Singtel, Softbank and Telefónica welcomes AT&T,"
<https://www.singtel.com/about-Us/news-releases/global-cyber-security-alliance-formed-by-etisalat-singtel-softbank-and-telefni>



System Design



Entities

- Gateways
 - Last line of defense, with sufficient resources
 - controller/manager for devices at home
 - Capability: test SFs, apply SFs, manipulate device traffic, etc.
- SSPs
 - Any device vendor, or,
 - A third-party security solution provider



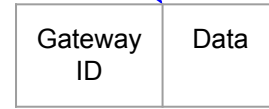
Roles

- Transaction participant
 - Gateways and SSPs (former outnumbers the latter)
 - Both initiate transactions → execution of smart contracts
- Verifier
 - Depends on the implementation
 - Blockchain → only gateways
 - Corda → as per the DLT

Transaction Format

Txn Type	Gateway Info	SSP Info	Smart Contract Info	Amount	PreTxnLink	Digital Signature
----------	--------------	----------	---------------------	--------	------------	-------------------

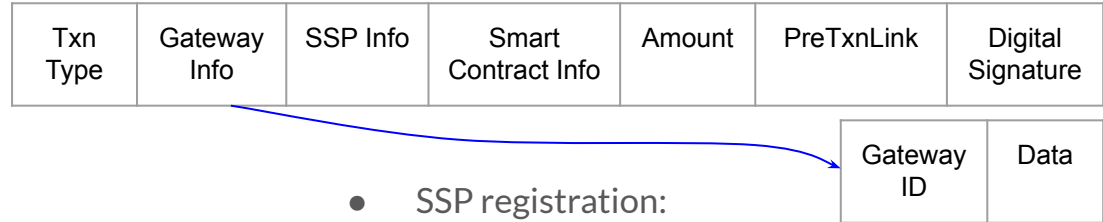
- Each transaction contains the following
 - Transaction type (Txn Type): *register, release, interest, review, purchase*
 - Gateway Info: contains “gateway ID” and “data”
 - SSP Info: contains “SSP ID” and “data”
 - Smart Contract Info: pointer to corresponding smart contract to be triggered
 - Amount: monetary value if the transaction involves monetary transfer (such as purchase)
 - PreTxnLink: link to the previous transaction related to current one
 - Digital Signature: standard field, for authenticity and integrity check





System Transactions & Smart Contracts

register



- Gateway registration
 - Gateway needs to register itself before availing to the services
 - Gateway's public key / IP address forms the ID
 - "Certificate of ownership" is embedded in the "Data" field
 - Amount is monetary pledge
 - "SSP Info" and "PreTxnHash" are left empty
- Smart Contract:
 - Check if the gateway/SSP has registered before
 - Check "legal certificate"
 - Check and store deposit
 - Validate signature
- SSP registration:
 - Similar to gateway's, except fields filled differently
 - Data field to contain proof of company's legal registration info
 - Also, pledges relatively larger collateral



release

Txn Type	Gateway Info	SSP Info	Smart Contract Info	Amount	PreTxnLink	Digital Signature
----------	--------------	----------	---------------------	--------	------------	-------------------

- Only executed by SSPs
 - When releasing a specific SF into the market
 - “Data” from “SSP Info” contains a pointer to the released SF, e.g., a repository
 - “Amount” indicates the deposit the SSP has to pledge for releasing the solution
 - De-incentivize an SSP from offering low quality solution
- Smart Contract:
 - Check SSP has registered earlier
 - Check and store deposit
 - Validate signature



SSP ID	Data
--------	------



interest

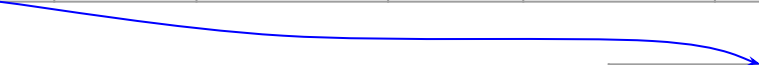
Txn Type	Gateway Info	SSP Info	Smart Contract Info	Amount	PreTxnLink	Digital Signature
----------	--------------	----------	---------------------	--------	------------	-------------------

- Only executed by the gateways
 - To express the interest of testing the trial version of a security function
 - “Amount” indicates the deposit the gateway has to pledge, to incentivize subsequent review of the SF
 - Refunded if review is performed
 - Else might be split between the gateway, SSP and the system owner (ISP alliance)
 - Review deadline: the gateway to provide feedback before the deadline, otherwise deposit will be forfeited
- Smart Contract:
 - Check if the gateway has submitted a review for same security function previously
 - Check if SSP has sufficient deposit balance
 - Else, likely the SF is of low quality
 - Check if the gateway has performed a review upon the review deadline
 - Refund if review submitted; else forfeit the deposit amount



review

Txn Type	Gateway Info	SSP Info	Smart Contract Info	Amount	PreTxnLink	Digital Signature
----------	--------------	----------	---------------------	--------	------------	-------------------



Gateway ID	Data
------------	------

- Only executed by the gateways
 - To provide its feedback for the tested SF
 - Either “success” or “failure”: included in the “Data” subfield of the “Gateway Info”
 - Based on the review, the reputation score of the tested SF will be updated
 - If the report indicates “failure” of SF, gateway can no longer purchase the SF
 - Therefore wrongly giving a failed report has implications
 - SSPs may collude with gateways to provide fake review outcomes, however this would be costly for a large network
- Smart Contract:
 - Check if the gateway has initiated an “interest” or “purchase” transaction earlier
 - Check if there is a “review” transaction for this function from this same gateway
 - Based on the review outcome, re-compute the reputation score
 - Refund / forfeit deposit accordingly



purchase

Txn Type	Gateway Info	SSP Info	Smart Contract Info	Amount	PreTxnLink	Digital Signature
----------	--------------	----------	---------------------	--------	------------	-------------------

- Only executed by the gateways
 - To purchase the solution if it is satisfied with the trial, and needs the full version
 - “Amount” field is filled with the purchase value
- Smart Contract:
 - Checks:
 - If exist a “review” and outcome is “success”. If outcome is “failure”, discard the transaction
 - If no “review” transaction for the security function, searches device registration transaction
 - Re-compute the reputation score
 - Check amount and transfer to SSP



System Implementation




Implementation - Naive Approach

- We envision our system to be a *permissioned* blockchain network
- Naively, could be similar as traditional Bitcoin blockchain
 - Instead of storing monetary value, the system stores different actions on to the blockchain
 - Each block to contain transactions related to the same security function
 - Each block further embedded with a reputation score of that security function, and frequently updated
- Verifiers: only gateways
- Consensus protocol: could use Byzantine Fault Tolerance (BFT) or its efficient variant



Implementation - Corda

- Corda, designed to be a permissioned DLT, might be a better suit for our system
- Properties of interest:
 - The identity of each participating node (gateway/SSP) is mapped to a real-world identity
 - Privacy: Communication is between specific nodes and encrypted
 - Only involved entities and notary validate a transaction (gateway, SSP and ISP alliance)
 - Transaction can involve confidential identity (useful for not revealing identities behind reviews), exposed only to notaries
 - Notion of states, that can represent “certificate of ownership”, a shared fact due to execution of certain transaction (contract), e.g, “gateway has obtained the trial version of SF X”, etc.



Implementation - Corda (cont'd)

- Mapping with Corda design:
 - Gateways in the proposed system are assigned with IP addresses and public/private key pairs
 - Legal binding for gateways with the governing ISPs (i.e., with authenticated certificates)
 - Similarly, have legal binding for the SSPs as well
 - States related to transaction's input and output, checked by smart contracts
 - Some are regular states (e.g., output of `interest`), whereas others are reference states (e.g., output of `register`)
- Consensus
 - Corda doesn't specify a particular consensus protocol, but allows plug-in practical BFT
 - Executed via a group of notaries (instead of all entities in the system): could be the alliance of ISPs



Security Analysis



Sybil Attack

- Malicious SSPs register multiple gateways
 - To influence the reputation system
 - To gain additional advantages in the network
- Counter measures
 - Gateways need to present valid certificate of *ownership*
 - multiple gateways with same ownership is easily detected
 - Malicious SSP registers different certificates for gateways:
 - illegal; dealt using the same technique as today.



Colluding

- SSP may collude with legitimate gateways
 - Not unique to our system, but common in similar systems
 - E.g., mobile app rating, e-commerce rating, etc.

- Counter measures
 - Similar to existing countermeasures (e.g. [2])
 - In general, such an SSP will have to influence large number of gateways → high cost

[2] M. Allahbakhsh and A. Ignjatovic, "An Iterative Method for Calculating Robust Rating Scores," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 2, pp. 340-350, Feb. 2015



Disguising as legitimate SSP

- A malicious entity may disguise as a legitimate SSP
 - Register into the network legitimately
 - Distribute malicious security functions, such as malware, software with trapdoors
- Counter measures
 - SSP has to deposit a large collateral → increases the cost of such attack
 - Malicious entity needs to build-up good reputation based on good security functions
 - Malware could also be detected by alliance of ISPs by carrying out regular testing and sanity checks



Reputation System



Reputation System

- Could be implemented as a modular approach
- High-level idea
 - “positive” review from trial increases reputation score, and “negative” decreases it
 - Successful purchase further increases the score
 - More sophisticated score computing mechanism could be adopted



Summary

- A system design for distributing *security functions* in a rapidly evolving market
 - So as to quickly detect, respond and mitigate, threats and attacks on IoT devices
- Design considered:
 - Potential attacks on the system
 - Computation of reputation scores for security functions
- Next step:
 - Implement on a small testbed with a few gateways



Thank You!