Research section

Introduction

The problem that we are currently facing is that a location cannot be guaranteed to be accurate or correct when it is sent from the producer device. This information can be spoofed or faked, which makes the location information ineffective. There is a need for this location to be secure because location is a very important aspect of logistics and tracking. A consumer would want to know where their product is coming from, and be able to trust that this information is correct.

The main aim of this research paper is to investigate the available methods of tracking and verifying a location. The objective is to identify what sort of available techniques there are that have been used to proof a location. For this project, the particular area of interest includes the use of a mobile app for location verification, specifically for an Android OS where possible.

Proof of location

A number of articles were examined in that were available in the current body of knowledge. These all included the use of mobile device. The idea was to get a better idea of what sort of implementations have been done, and also to help as a pointer to the right general direction as far as location proofs go. By reviewing what is currently out there and what has been done, it will enable the team to have a better understanding of how to approach the problem and come up with possible solutions.

Past research

- Brambilla, Amoretti & Zanichelli 2016

This paper was a starting reference that was mentioned by the client to help the project gain direction for the location aspect of the project. The paper presents a decentralised option for proof-of-location based on the blockchain technology. The idea is there is no actual server that is required to be set up so the server is decentralised. The paper used mobile devices in a surrounding area as witnesses, while the mobile that wants to prove the location is referred to as the prover. This scheme requires multiple devices in an area so it is useful in places that are busy and have a lot of traffic. The authors of the paper states that their scheme guarantees both location trustworthiness and user privacy preservation.

- Lin & He, 2014

Location is verified by mapping the area to its WiFi coverage. Verifier ‘app’ can be installed in an existing device at the location, or could be a server. The way it works/workflow is described in section 2.1, all communication is encrypted using keys and the user checks with the verifier, using time it takes to communicate (communication delay) as a factor for verification. This approach protects from proxy attacks, as well as replay attacks. Their results indicate very low false positive rates which means a legitimate user at the location are almost never denied. This verification system can only be applied to venues with WiFi coverage so areas without it will have to use another implementation.

- Saroiu & Wolman, 2009

This paper talks about getting ‘location proofs’ which allows mobile devices by getting ‘proof’ from a wireless infrastructure such as a cell tower or a Wi-Fi access point. The paper mainly focuses on Wi-Fi technology, implementing location proofs over Wi-Fi. A location proof has an issuer, a recipient, a timestamp, a geographical location, and a digital signature. To verify the proof, an app first checks the client’s signature, followed by the AP’s signature inside the proof itself, followed by identity of the client (section 3.3). Proofs are private, unforgeable, and non-transferable. This implementation also requires the use of wireless APs.

- Sastry, Shankar & Wagner, 2003

The authors proposed the ‘Echo protocol’, a method for secure location verification. The protocol uses radiofrequency and ultrasound, and doesn’t require time synchronisation or any prior agreement between prover and verifier. Verification of location is whether something is in a set region rather than at a specific point. Uses the term prover and verifier for client and server. The protocol uses the time it takes for a packet to travel as its verification method. Ultrasonic methods are applied to decide the distance. Mainly suitable for low-cost devices such as those in sensor networks.

- Gabber & Wool, 1998

Even though the paper is a from a couple years back, it looks at the tracking movement of devices using existing communication infrastructure. Since it is a bit old, the technology was probably new back then. They discussed using GPS for location detection but are also aware its limitations. They also proposed a more secure scheme using wireless cell phone networks, as well as detecting location based on satellite ranging which measures the distance between receiver and satellite using the time it takes for a signal to arrive at the location.

- Zheng, Li, Lou & Hou, 2017

The paper proposes a scheme which protects privacy of the user’s private location and which is less vulnerable to an attacker reporting a false location. The user can establish communication with strangers in the surrounding area without any pre-shared secret key, and also does not reveal the actual location of the user to the server or other users. The authors suggest using a spatial-temporal location tag as a form of location representation. This tag is constructed from signals captured around the device, such as Wi-Fi and LTE signals. It is hard to forge the location tag as there is a variety in the environmental signals at different times.

- Khan, Zawoad, Haque & Hasan, 2014

They propose an architecture to obtain secure location proofs by using a location authority, which provides location proofs for a particular site, and a witness which is any mobile user who can confirm the presence of another user at the same surrounding location. So this method uses distributed environment for location proofs of mobile devices, using witnesses to ensure trust from all parties. The authors claim that their protocol is resistant to collusions and analysed a number of possible security attacks and how their method protects against them such as false presence, relay attack, privacy violation.

- Picciani, 2014

Picciani makes an introduction to the Bluetooth Low Energy(BLE) technology created by Nokia, and made popular by Apple under the name iBeacon. He goes into more detail on why the innovation was made and the benefits over Near Field Communication (NFC). He then goes forward to explaining what are the initials steps to start testing and using BLE, providing a couple of examples of code, as well as libraries and applications that will make it easier to start.

- Borowicz, 2015

This article goes into more detail on how Bluetooth Technology works. It explains the type of signal used and how it behaves in different environments and scenarios. Afterwards, Borowicz goes into even more details and how using math the programs along with the bluetooth signals can be used to calculate location. The article also provides libraries and SDKs for users to be able to try and test some of the solutions mentioned.

- McElrath, 2016

The article by McElrath, proposes an interesting but also more complicated solution to location proving using blockchain. He mentions the calculations that a combination of satellites need to do to be able to provide us with a location, but also mentions that, the information after some time can be replicated. To be able to secure the information and have a more reliable solution, he proposes that the user sends data to the satellite first and have the satellites create a ping response with that hash information sent to them. The combined reply of the hash sent plus the information added by the satellites should provide trustworthy information to know the subjects location at a certain time with almost no possibility of fooling the system. This solution was very interesting but due to time and resources, our team decided it was not the better option for our project.

Consolidating information from the papers

There were several different methods in the papers reviewed that were used to identify a location. These included use of GPS coordinates, using WiFi signals for location data, cell phone tower for triangulation purposes. We also identified bluetooth as another way of wireless communication and could potentially be used for a proof of location concept.

Each paper had their own unique implementation to secure the location information through the use of various technologies. The similarity between the ones that used a centralised approach was that they had a device or server within the vicinity or area of interest. It acts as an authoritative location provider or verifier which basically means that information coming from that source is trusted. For the purpose of this paper, physical security is assumed. The device is not accessible to the public to be tampered with. Although the solutions used in the papers were looked at, some were impractical and unrealistic within the current scope of the project, as well as time and resource constraints.

The were a couple of reasons why the ideas or implementations were not used. These included factors such as:

- Feasibility

        - Requires multiple clients/users to be in the area
    - Constraints
        - Only have a few weeks
        - Limited resources/expertise/manpower with location
    - Resources and familiarity
        - Multiple technologies (sensor, laser)
        - Additional unfamiliar territory (wireless technologies) on top of blockchain

There were also factors that have to be considered from an attacker's point of view. These included ways which an attacker could fake or spoof a location, resulting in inaccurate keeping of records.

- Identifying possible ways of spoofing
    - Attack
        - Malicious device installed on server
        - External device intercept signal send from producer app
        - Android device connect to external device via bluetooth
        - Android device download malicious app (SPH Razor 2013)
        - Malicious devices picks up data before sending it to server
    - Mitigation
        - Prevent device from downloading application
        - Pair devices only can send data (bluetooth)
        - Set bluetooth undiscoverable

Selected solution:

- Bluetooth beacon
    - Reason
        - Range is limited therefore producer app users have to be within the compound to do the authentication
        - Certain devices can only be used
        - Authentication is used
    - How to implement
        - Install beacons in area where producer app is going to be used.
        - Use beacons to confirm location of the phone using the producer app.
        - When location is confirmed, upload data to blockchain.
            - Data is a hash of the producer signature, producer public key, and timestamp before it was signed
    - Sample bluetooth code to send string
      https://stackoverflow.com/questions/22899475/android-sample-bluetooth-code-to-send-a-simple-string-via-bluetooth

Why it meets what the client is expecting

The client wanted a way for location information to be secured, preventing a location from being faked or spoofed. By using the idea of a 'bluetooth beacon', this conforms with the set requirement. The beacons are placed in locations that the client knows the producer app will be functioning. Since these places are not meant to change in the near future, the location only has to be confirmed rather and obtained. The location is given from a trusted source and cannot be faked. The use of public key infrastructure means that only location information from the ‘bluetooth beacon’ can be accepted and trusted. Other devices cannot send location information even if it is the same because it cannot encrypt the data with the unique private key that only the specific ‘bluetooth beacon’ has. So considering all the information above, the bluetooth beacon can be used to confirm that a device is being used on a known location, before uploading the data to the blockchain.

Limitations

Every solution has its limitations and this applies to our project as well. A shortcoming of using something like a bluetooth beacon or bluetooth-enabled device is its battery life. The beacon would need to be changed every half a year or so (Leddy, 2016) depending on the range. Any device (e.g. Android phone or similar) would need to be plugged in or charged everytime it gets low.

In terms of attacks, a malicious user may theoretically be able to perform a proxy or replay attack where the location information sent from the bluetooth device is captured by an attacker, and then reused to claim to be from that specific location elsewhere.

Future implementation

There is certainly room for improvement and growth for the current project. Some of the areas that could be expanded on include:

- Smart contract
  Smart contracts are contracts that are self-executable and are able to keep all parties involved accountable (Hertig 2017). The contracts are able to automate payment on when one party has completed a task which will then remove the need for payment chase.
- Using location to pinpoint where a record was created

Conclusion

This main goal of this research paper is to find possible ways that location can be verified, or how to prove a location. Location information has to be accurate because it is important for tracking the whereabouts of products and how the have moved along the supply chain. There were various different solutions explored in the literature. However, none of them were suitable and did not fit within the constraints of the project. The main concept was to have a location server within the surrounding area, thus the idea of a ‘bluetooth beacon’ was developed.

It provides an easy way to confirm the location of a subject at a specific time with minimal errors, using an existing technology that can be used in any phone with a bluetooth connection. Additionally the beacons are relatively cheap and since the energy consumption is minimal, they can be placed virtually anywhere without the need to be connected to a power source.

References

- Borowicz, W. (2015). How do beacons work? The physics of beacon tech. [online] Reality matters. Available at: http://blog.estimote.com/post/106913675010/how-do-beacons-work-the-physics-of-beacon-tech [Accessed 2 Oct. 2017].
- Brambilla, G, Amoretti, M & Zanichelli, F 2017, "Using Blockchain for Peer-to-Peer
- Gabber, E. and Wool, A., 1998, November. How to prove where you are: Tracking the location of customer equipment. In *Proceedings of the 5th ACM Conference on Computer and Communications Security* (pp. 142-149). ACM.
- Hertig, A 2017, "How Do Ethereum Smart Contracts Work? - CoinDesk", CoinDesk, viewed 5 October, 2017, <https://www.coindesk.com/information/ethereum-smart-contracts-work/>.
- Khan, R., Zawoad, S., Haque, M.M. and Hasan, R., 2014, July. 'Who, When, and Where?'Location Proof Assertion for Mobile Devices. In *IFIP Annual Conference on Data and Applications Security and Privacy* (pp. 146-162). Springer, Berlin, Heidelberg.
- Leddy, P 2017, "10 Things About Bluetooth Beacons You Need to Know", *Academy.pulsatehq.com*, viewed 20 October, 2017, <http://academy.pulsatehq.com/bluetooth-beacons>.
- Lin, X & He, W 2014, "WiLoVe: A WiFi-coverage based Location Verification System in LBS", *Procedia Computer Science*, vol. 34, pp. 484-491.
- Proof-of-Location", *Distributed, Parallel, and Cluster Computing (cs.DC)*, pp. 1-11.
- SPH Razor 2013, *Hacking a mobile phone*, viewed 23 September, 2017, <https://www.youtube.com/watch?v=KnQHgpja7OU>.
- McElrath, B. (2016). *Blockchain Proof of Location – SolidX Blog*. [online] SolidX Blog. Available at: https://blog.sldx.com/blockchain-proof-of-location-7af5eb8073c1 [Accessed 6 Oct. 2017].
- Saroiu, S & Wolman, A 2009, "Enabling new mobile applications with location proofs", *Proceedings of the 10th workshop on Mobile Computing Systems and Applications - HotMobile '09*.
- Sastry, N, Shankar, U & Wagner, D 2003, "Secure verification of location claims", *Proceedings of the 2003 ACM workshop on Wireless security - WiSe '03*.
- SPH Razor 2013, *Hacking a mobile phone*, viewed 23 September, 2017, <https://www.youtube.com/watch?v=KnQHgpja7OU>.
- Zheng, Y., Li, M., Lou, W. and Hou, Y.T., 2017. Location based handshake and private proximity test with location tags. *IEEE Transactions on Dependable and Secure Computing*, *14*(4), pp.406-419.
- Picciani, A. (2014). *Building iBeacon applications on Android • airfy Inc.*. [online] airfy Inc. Available at: https://airfy.svbtle.com/building-ibeacon-applications-on-android [Accessed 10 Oct. 2017].
- Young, D. (2017). AltBeacon/android-beacon-library. [online] GitHub. Available at: https://github.com/AltBeacon/android-beacon-library [Accessed 6 Oct. 2017].