XYO Network: Security Risks and Mitigants

Arie Trouw [*], Andrew Rangel, Jack Cable

February 2018 - Draft

1 Introduction

A primary concern for the XYO Network, like all decentralized trustless systems, is the security of the system. Vulnerabilities include, but are not limited to, design/architecture flaws, coding errors, incorrect economic motivation, and social engineering. For the purposes of this document, we will focus on design/architecture flaws and economic motivation.

2 Technical Considerations

2.1 Summary

In this paper we will discuss high level concepts and attacks against the XYO Network. This network is trustless, therefore we will assume that all participants in the network (sentinels, bridges, etc) are vulnerable. In this section we will detail out some of the known protocol level attacks along with industry standard protections against them. From here on out all other attacks assume the devices are compromised.

2.2 Bluetooth

Most Bluetooth devices use a ”Long Term Key” pairing setup that establishes a PIN used for encryption. If the key is discovered through intercepting the pairing process, all future traffic is easily decrypted. There are also tools that allow for brute forcing the PIN. Even well established schemes to establish a password outside of the protocol are usually done unecrypted. This provides multiple attack vectors for the protocol. There are easily sourced devices that expedite these approaches.

In order to prevent attacks of this nature, white-listing MAC addresses can prevent unauthorized devices from communicating with the sentinels and bridges. Another counter measure is to require physically pressing a ”reset” button in order to pair, this prevents attacks from users without direct physical access.

[*] XYO Network, `arie.trouw@xyo.network`

2.3 Over the Air

Sentinel's will need the ability to be updated via an "Over the Air" (OTA) update. OTA updates allow for quick patches to improve stability and security. A potential downside is an attack that spoofs this update and adds malicious code.

2.4 Hardware

These devices will be physically located in a range of places all across the globe. This means that there will be a constant ability to physically comprise the devices. This is a key reason for XYO Network to be a completely trust-less network. We will rely on complex algorithms that parse the history and content of the data coming into the system. Any data that doesn't pass as quality long-chain data will be disregarded and the devices will be penalized.

3 Poison the Well Attacks

3.1 Summary

A Poison the Well Attack is where a malfunctioning or malicious party is creating corrupt data which decreases the accuracy and/or certainty of results generated by the system.

3.2 Motivation

In this attack the bad actor is motivated to disrupt or *poison* the data that is going to a particular Sentinel or Bridge. This could allow them to cause both short term and long term financial disruption. The XYO Network is a trustless system which gives it a low tolerance for this bad data.

While there is no direct gain for the bad actor, often there are benefits to disrupting other people's financial and reputation standing. For instance, let's surmise that the XYO Network is being used to track parolees' locations to monitor for any infractions they commit by being somewhere against their parole terms. This could be as simple as not allowing a continual DUI offender to be in a bar past a certain amount of time. An enterprising parolee could poison the well in terms of feeding the bridge for the bar bad data until it is knocked off the network. Then they could come and go from the bar as they please. Even if the data showed them locating in the bar, the bad data could limit the ability to prosecute.

3.3 Technical Analysis

Location data of the sentinel could be affected by a GPS jammer or illegal radio frequency transmitters that are designed to interfere with authorized radio communications. GPS Spoofing devices [1] can send false data to GPS receiving radios to falsify their location.

Due to the Sentinels communicating via Bluetooth, this presents another vector for this attack. They are various documented ways to spoof a Bluetooth device to send bad data [2]. While the private keys are ephemeral, it is possible that a device could listen to the sentinel communicating with the bridge and copy the data it is sending across. Theoretically it could then send bad data as that sentinel which would begin to poison the data the bridge is sending to the Archiver.

3.4 Mitigation Strategies

While effective, a GPS jammer is easily recognized due to the pollution it causes to the general area. For instance, anyone will a cell phone in the area would notice a complete block out of many of the apps they use. It would be a fairly short amount of time until it was discovered that there was a jammer in the area. Given that the disruption is easily noticed and the FCC has explicit ruling that jammers are illegal [5], the likelihood of this attack is low. That being said, there are sophisticated GPS anti-spoofing techniques at the hardware and software level being developed. [1]

There are current technologies and strategies that allow us to protect against bluetooth spoofing and disruption, such as authenticated link key using secure connections. [3]

4 Assassination Attacks

4.1 Summary

An Assassination Attack is where a malicious actor tries to discredit (character assassination) or make non-functional (technical assassination) another node.

4.2 Motivation

In an Assassination Attack, an attacker is motivated to undermine the reputation of legitimate nodes in order to boost the relative credibility of other nodes controlled by the attacker. As the reputation of Sentinels on the XYO Network is fundamental for a functioning network, it is crucial that the reputation of nodes cannot be easily manipulated.

Consider a situation where an attacker aims to broadcast false location information on the XYO Network (as detailed further in the Force Field Attack). In this case, the attacker must first target individual nodes to harm their reputation. One method in which this can be accomplished is via selective signing, where an attacker selectively provides information to a legitimate Sentinel in order to make the node less consistent with other nodes on the XYO Network. This causes the Sentinel's reputation to be lowered relative to other nodes on the network.

Additionally, an attacker may engage in technical assassination of nodes in order to achieve similar results, rendering devices non-functional. This could be as simple as a physical attack destroying a device.

4.3 Technical Analysis

An Assassination attack on one Sentinel requires an attacker to deploy at least one device to selectively communicate with the target Sentinel. Since other devices on the network will not generate signatures with the malicious node, the malicious node is only visible onto the target node.

To Bridges, external to the network, the information broadcast by the target node is inconsistent with the rest of the network. This has the effect of the target node losing reputation with respect to the rest of the network, which are consistent in not recognizing the malicious node.

4.4 Mitigation Strategies

Fundamental to the protection against an Assassination attack is the establishment of punishing a node's reputation if it engages in selective signing. In this scenario, the malicious nodes engage in selective signing in order to make themselves appear invisible to other Sentinels on the network.

By establishing a reputation of each Sentinel according to its consistency with the rest of the network, it is possible to punish nodes that engage in selective signing. A reputable node may issue a query to a less reputable node on the network. If the node is legitimate, it would be in its own best interest to sign the query and make itself visible to the network, which would increase its own reputation. Thus, in the case that a node practices selective signing, the more reputable node may broadcast that the malicious node refused to sign its query (Note that this could not be exploited if a node does actually sign the query, as the node can broadcast its signature to disprove the selective signing punishment).

Punishing selective signing has the effect of mitigating character assassination attacks, as each Sentinel has a defense mechanism for receiving inconsistent information.

5 Deception Attacks

A Deception Attack is where a malicious actor tries to pass off incorrect yet valid data to be used in the system for personal gain.

One case of a Deception Attack occurs with Multi-Chain Forging, where an attacker maintains multiple versions of their own chain, essentially existing in multiple places at once.

5.1 Motivation

An attacker can benefit from false information by forking their own location chain. This can be accomplished by sending the private key for one chain link (generated during the creation of new local blocks) to one or more colluding adversaries in different areas, which proceed to create new location chains branching from the same point.

Consider a situation where an attacker wishes to spread false information about their location. This could prove advantageous in situations where accuracy of location is important, e.g. in establishing an alibi to attest that the attacker was present at a location at a given time. By having multiple chains, the attacker can wait for an opportune moment and then selectively report only the chain whose information is most advantageous to them.

5.2 Technical Analysis

A Deception attack is increasingly more difficult to execute as the chain grows longer. As time proceeds, information from a particular node is broadcast across the XYO Network. As a result, a feasible attack would allow at most a few small changes to a chain at some point in the past.

This does not completely diminish a potential for an attack. When syncing with a Bridge, a malicious Sentinel may choose one of its forked chains to share with the Bridge. As both chains are valid, the Bridge and other upstream devices cannot immediately conclude that the chain has been forked. Instead, it is necessary for nodes to cross-check with records of communication with other Sentinels on the network to verify that the Node has not existed in multiple locations at once.

5.3 Mitigation Strategies

The XYO Network, by nature, is not tolerant of Multi-Chain attacks. Any long-term fork of a node's chain will be inconsistent with the general consensus of the network. In order to prevent small modifications, when the integrity of location data is more important, a user may wait for more confirmations from Archivists containing signatures from distributed nodes. As time proceeds, any discrepancies resulting from a forked chain will become apparent.

6 Same-Machine Sybil Attack

A Same-Machine Sybil Attack occurs when a malicious actor creates multiple nodes from a single machine. Since devices aren't assigned unique IDs, this is easily achievable. The malicious actor builds up reputation by signing packets between the simulated nodes to portray the nodes as normal-looking nodes, and then lets the nodes each communicate with different groups of nearby nodes such that each simulated node keeps different information in their Proof of Origin chains, resulting in all having high Origin chain scores. This attack allows malicious actors to cheaply mass produce nodes that they can use to conduct Sybil attacks on the local or even global network.

6.1 Motivation

An attacker may seek to engage in a Same-Machine Sybil attack to increase influence over a particular region. By creating multiple fake nodes from the same device, this lowers the barrier for entry in executing a Sybil attack. It is much easier for an attacker to create many fake devices on one machine than create many malicious devices.

6.2 Technical Analysis

It is easy to spoof a bluetooth device's information in order to appear indistinguishable from the device [4]. Thus, an attacker can trivially create multiple devices from one computer that act and appear separate.

Once a number of virtual Sentinels have been created, the attacker can operate the Sentinels as if they were physically distinct. The Sentinels would proceed as normal to sign information related to other Sentinels in their proximity. Additionally, an attacker may create a virtual map of devices that are reflected in the signatures of the virtual Sentinels.

6.3 Mitigation Strategies

The key to defending against such an attack lies in detecting duplicate data as perceived in signal strength. A computer running many virtual Sentinels would appear to have the same RSSI for each Sentinel. As a result, to an external Sentinel, each virtual Sentinel operating on the computer would be close to each other, provided a certain fluctuation in signal strength. In order to prevent this attack, it is important for a legitimate Sentinel to recognize bundled devices and treat their information as one node.

7 Force Field Attacks

A Force Field attack combines an Assassination and a traditional Sybil attack in order to provide false data to a network. The attack is twofold: an attacker provides inconsistent information to legitimate nodes while simultaneously allowing the attacker's network of nodes to serve as a consistent network for outside observers.

7.1 Motivation

This approach takes the form of a local Sybil, where the attacker aims to completely control the authority of a certain physical location. However, a pure Sybil attack on the XYO Network would require a large number and history of distributed devices in order to outnumber the existing nodes in reputation. Instead, a Force Field attack is a hybrid approach, first targeting the reputation of existing nodes via Assassination Attacks in order to cause inconsistencies between legitimate nodes.

Consider a situation where an attacker wishes to have complete authority of a certain local region. In a Force Field attack, the attacker would first flood each legitimate node with inconsistent information. Thus, the reputation of nodes on the network would decrease, with the barrier for entry of reputation significantly decreasing. As such, an attacker would consequentially be able to supply their own network of devices to outnumber the reputation of legitimate devices, establishing singular authority for the targeted region.

7.2 Technical Analysis

In order to render an existing network inconsistent, an attacker makes use of selective signing in order to lessen the overlap between legitimate nodes. For instance, an attacker could bring malicious nodes into the local network, and then have each node only communicate with certain devices on the network. Each legitimate Sentinel will broadcast the location of the malicious node communicating with it, while the malicious node appears invisible to other Sentinels around it. At a large scale, this will cause each Sentinel to have a vastly different interpretation of the state of the network. To an outside source, such as a Bridge, the reputation of each node would be lowered.

From here, an attacker would take advantage of the reduced reputation of the entire system in order to enter their own network of Sentinels. Note that these devices may already have existed on the network, and simply become more powerful as the reputation of other Sentinels is lessened.

The attack is dependent upon the number of existing nodes in the region, and becomes increasingly more difficult as the number of nodes in a region grows.

7.3 Mitigation Strategies

As outlined when preventing Assassination attacks, mitigation for Force Field attacks relies on punishing selective signing. A Force Field attack uses selective signing with a cartel of malicious nodes to make target legitimate nodes inconsistent with the XYO Network.

Having reputable Sentinels poll less reputable nodes for signatures and broadcasting nodes that refuse to respond diminishes the ability of nodes to selectively sign with legitimate nodes.

This would make a Force Field attack much more difficult to execute, because any reputation built to execute the attack would quickly dissipate after engaging in selective signing.

8 Teleportation Attack

8.1 Motivation

A Teleportation attack occurs when someone is able to falsify their location by ”teleporting” to another location via the network. For instance if a phone or bluetooth beacon was being used as the sentinel that proves their location, they could falsify that location by sending the device with someone else. In the aforementioned example of needing an alibi, a bad actor could swap phones with someone else in order to create a fake location.

This can also be achieved from a software perspective by sharing your private keys with another individual. For instance if you wanted to have verified hotel reviews you would only let people leave reviews that had a trusted history on-chain. A bad actor could share their private key with an individual near the hotel and it would appear as if they are located there with the chain being non the wiser.

8.2 Technical Analysis

If the private key is able to be accessed by the user it can easily be shared to create a spoofed device that appears as that users device. Utilizing Software Defined Radio it would allow anyone with the means to appear to the network as your specific device. This will nullify attempts to validating a users location. This also has an implication for the data on the the blockchain, because it is theoretically difficult to discern what is valid device travel and what appears to be a teleportation attack.

8.3 Mitigation Strategies

Mitigation strategies for this approach are complex due to there being natural breaks in the chain. In this instance when a person boards a flight their devices no longer communicate with the network until they land. These gaps of information will require a sophisticated algorithm to discern what are natural gaps, and what are potentially bad data points that must be penalized.

9 Stealth Attack

A Stealth Attack occurs when a device hides itself from the network. Within various uses of the XYO Network it is important that devices have a solid chain history.

9.1 Motivation

A user could strategically turn on and off their location services using their phone or beacon to create bad chain data that would otherwise appear valid. This would allow them to essentially hide themselves from the network when they needed to and re-appear to the network as valid data. There are a myriad of use cases for this attack because it allows a user to have more control over the data they present.

9.2 Technical Analysis

In this attack the technical approach can be as easy as turning off a device. If you needed a more complicated approach you could build a Faraday cage that hid you, or a specific beacon, from the network. This approach could also be persisted through Denial of Service attacks.

9.3 Mitigation Strategies

Mitigation for this attack can be complex due to the nature of beacons and other Bluetooth devices being easy to disconnect from the networks. The main strategy to alleviate this potential would be a strong software layer that will penalize sentinels and bridges that broadcast broken chain data. These capabilities will grow over time as the algorithm gets better at understanding the subtle differences between valid and invalid data.

10 Denial of Service Attacks

A Denial of Service Attack (DoS) is when a malicious or dysfunctional actor causes a local, regional, or system wide outage.

10.1 Motivation

An attacker may seek to disrupt the XYO Network in order to prevent it from being used for Proof of Location.

10.2 Technical Analysis

Due to the nature of the Bluetooth protocol the beacons can only connect to one device at a time. This means any device that accepts unauthenticated commands can easily be knocked off the network. This can be achieved as simply as a mobile phone app. This opens up the ability to have one device that broadcasts Bluetooth commands out continually with relative ease. By sending hex values to the device for given parameters, such as the ”play sound” parameter on most beacons, it will create a connection with that device. If this connection is established it blocks any other device from communicating with it. This could be multiplied by the use of Software Defined Radio that could run scripts to continually broadcast out various hex values to any beacon in range.

10.3 Mitigation Strategies

In order to mitigate this risk, the Bluetooth device should only accept authenticated commands or utilize a MAC address white-list. Reducing the number of write authenticated commands will minimize the footprint of this attack vector.

References

[1] Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gerard Lachapelle. *GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques*. International

Journal of Navigation and Observation, vol. 2012. *Hindawai.com.*
`https://www.hindawi.com/journals/ijno/2012/127072/cta/`

[2] John Padgette John Bahr Mayank Batra Marcel Holtmann Rhonda Smithbey Lily Chen Karen Scarfone *Guide to Bluetooth Security.* NIST 2017. *NIST Special Publication.*
`http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf`

[3] JP Dunning *Breaking Bluetooth by being bored.* DefCon 2010. *Defcon Presentation.*
`https://www.defcon.org/images/defcon-18/dc-18-presentations-/Dunning/DEFCON-18-Dunning-Breaking-Bluetooth.pdf`

[4] haxf4rall *Spoofing a Bluetooth device.*
`http://haxf4rall.com/2016/05/11/spoofing-a-bluetooth-device/`

[5] FCC. *FCC Enforcement Advisory.* FCC 2014. *FCC.gov.*
`https://apps.fcc.gov/edocs_public/attachmatch/DA-14-1785A1.pdf`

Glossary

Bridge A Bridge is a heuristic transcriber. It securely relays heuristic ledgers from Sentinels to Diviners. The most important aspect of a Bridge is that a Diviner can be sure that the heuristic ledgers that are received from a Bridge have not been altered in any way. The second most important aspect of a Bridge is that they add an additional Proof of Origin metadata. 2

Sentinel A Sentinel is a heuristic witnesses. It observes heuristics and vouches for the certainty and accuracy of them by producing temporal ledgers. The most important aspect of a Sentinel is that it produces ledgers that Diviners can be certain came from the same source by adding Proof of Origin to them. 2