# XYO Network: 보안 리스크와 완화

Arie Trouw* (아리 트라우), Andrew Rangel (앤드류 란글), Jack Cable (잭 케이블)

2018년 2월

---

# 1 소개

XYO Network는 무신뢰성 및 탈중앙화된 암호 위치 네트워크이다. 이것은 위치 확인과 관련하여 높은 확실성을 설립하기 위해 영지식 증명(zero-knowledge proofs)을 사용한다. 모든 탈중앙화되고 무신뢰성의 존재와 함께하는 것과 같은XYO Network의 주요한 문제는 시스템의 보안이다. 취약성을 포함하여 디자인/아키텍처의 결함, 코딩 에러, 부정확한 경제적 동기부여, 그리고 소셜 엔지니어링과 같은 것까지 광범위하다. 이 문서의 주요 관심은 디자인/아키텍처 결함과 경제적 동기부여에 적용된다.

---

# 2 기술적인 고려

## 2.1 요약

본 문서는XYO Network를 향한 잠재적인 공격에 관하여 높은 수준의 개념을 다룬다. 네트워크가 신뢰성 없는 시스템을 이용한다는 사실은 네트워크 안의 모든 참가자가 취약하다는 것을 가정한다 (예를들어 Sentinels (데이터 수집자), Bridges (데이터 전달자) 등). 여기에서 공격에 대한 산업 기준 안전장치와 더불어 잘 알려진 프로토콜 수준의 공격들을 상세하게 다룬다. 모든 다른 공격들은 시스템 내에서의 디바이스들이 손상되었다고 가정한다.

## 2.2 블루투스

대부분의 블루투스 디바이스들은 암호화를 위해 사용되는 PIN을 구축한 “Long Term Key (롱텀키)” 페어링을 이용한다. 만약 페어링 과정의 차단을 통해 키가 발견된다면, 모든 미래의 트래픽은 쉽게 해독될 것이다. PIN을 강제로 풀 수 있는 존재하는 툴들이 있다. 심지어 프로토콜 밖에서 패스워드를 구축한 잘 만들어진 계획은 대체적으로 해독을 실행했다. 이것은 다양한 공격 벡터가 프로토콜에 접근하도록 한다. 게다가. 디바이스들은 이 접근을 신속히 처리하도록 쉽게 소스를 제공할 수도 있다.

이러한 환경에서 공격을 막기 위하여, 화이트 리스팅 MAC주소는 승인되지 않은 디바이스들이 데이터 수집자 및 데이터 전달자와 통신하는 것으로 부터 막을 수 있다. 이러한 공격을 막는 또 다른 방법은 사용자가 페어링된 디바이스의 “리셋” 버튼을 누르는 것이다. 이것은 디바이스와 직접적인 접근을 하지 않은 사용자들로부터의 공격을 막는 것이다.

*XYO Network, **arie.trouw@xyo.networK**

## 2.3 Over the Air (오버 디 에어) (OTA)

Sentinels은 “Over the Air (오버 디 에어)” (OTA)의 업데이트의 활용 능력이 필요하다. OTA 업데이트는 디바이스의 안정성과 보안성을 증진시키기 위해 빠른 패치를 허가한다. 이 특징의 불리한 점은 이러한 업데이트를 모방한 공격의 가능성과 더불어 악성코드를 덧붙이는 것이다.

## 2.3 하드웨어

XYO Network의 디바이스들은 세계적으로 광범위하게 물리적으로 분산되어 있다. 이것은 물리적으로 디바이스에 구성될 수 있는 잠재성이 지속적으로 있다는 것을 의미한다. 이것은 XYO Network가 완전하게 무신뢰성 네트워크가 되기 위한 필수 항목이다. 시스템 전체는 시스템 안에서의 데이터 흐름의 기록과 내용을 조심스럽고 성실하게 분석하는 복잡한 알고리즘에 의존한다. 높은 점수를 통과하지 않은 롱 체인 데이터 (long-chain data)는  무시되고 문제가 되는 디바이스는 처벌을 받는다.

# 3 Poison the Well Attacks (Poison the Well공격)

## 3.1 요약

Poison the Well 공격은 오작동 또는 악성 파티 (malicious party)가 만들어지고 오류가 생긴 데이터를 주입했을때 일어난다. 이것은 시스템이 만든 결과의 전반적인 정확도 및/또는 확실성을 감소시킨다.

## 3.2 동기 부여

Poison the Well공격에서 공격자의 목표는 특정 Sentinel 또는 Bridge에 보내진 데이터를 방해하거나 나쁜 영향을 주는 것이다. 이것은 단기간 및 장기간 경제적 방해를 야기시킨다. XYO Network가 무신뢰성 시스템이라는 것을 고려하면, 네트워크에 침입하는 이러한 잘못된 데이터들을 용인하기 어렵다.

공격자에게서 직접적인 획득은 없지만, 방해 및/혹은 다른 사람들의 데이터 평판을 갖추는 것에서의 이익은 존재한다. XYO Network가 가석방 기간동안의 위반사항들의 위치기반을 보고하기 위하여 가석방된 사람의 장소를 추적하기 위해 고용되었다고 가정해 보자. 만약 이것이 연쇄 음주운전자가 술집에서 보낸 모든 시간을 모니터하는것에 사용된다면, 술집 기반의Bridge에게 잘못된 데이터를 줌으로써 네트워크가 잠길때까지 가석방된 사람을 처벌하는 것은 Poison the Well이 될 수도 있다. 그러면 비행자들은 그들의 가석방 기간동안 폭력을 행사할 수도 있고 그가 만족할 때까지 술집에서 술을 소비할 수도 있다. 비록 제공된 데이터가 범법자가 술집 위치에 있다는 것을 보고했었을지라도 독이 들어있는 데이터 (poisoned data)는 확실성을 타당성이 주어진 지점까지 감소시킬 수 있다.

## 3.3 기술적인 분석

데이터 수집자의 데이터 장소는 GPS 방해전파나 공인된 무선통신을 방해하기 위해 설계된 불법적인 무선 주파수 송신기에 의해 영향을 받을 수 있다. GPS로 위장한 디바이스들 [1]은 위치를 조작하기 위해 잘못된 데이터를 GPS 무선 수용기에 보낼 수 있는 능력을 가지고 있다.

블루투스와 통신하는 데이터 수집자들은 이러한 공격 유형의 또 다른 벡터를 보여준다. 블루투스 디바이스가 잘못된 데이터를 보낼 수 있도록 조작될 수 있는 다양한 방법들이 있다 [2]. XYO Network가 만든 사적 키(private

key)들은 즉각적으로 제거되는 동안, 디바이스가 Sentinel와 Bridge 사이에 통신을 들을 수 있고 보내진 데이터를 복사할 수 있는 것을 가능하게 해준다.

## 3.4 프로토콜 완화 전략

활성화되는 동안, GPS 방해전파는 이것이 타겟(target)으로 삼은 일반 지역에 오염을 야기하기 때문에 쉽게 인지될 수 있다. 예를 들어, 타겟 지역의 휴대폰 사용자는 그들이 사용하는 많은 애플리케이션이 갑자기 중단되는 경험을 할 수 있을것이다. 다수의 작업자들이 비슷한 문제를 확인하고 방해전파는 범죄라는 것을 확신할 수 있기까지 단지 시간 문제일 뿐이다. 발생된 방해전파가 불법이라는 것을 FCC는 명쾌하게 규정하고 있다. 이 사실과 함께 이러한 종류의 방해가 충분히 발견될 수 있다는 것을 고려해보면 [5], 이런 공격과 동반하는 높은 리스크는 방해전파의 발생 가능성을 낮춰준다. 그렇기는 하지만, 보안을 첨부한 하드웨어와 소프트웨어 수준에서 현재 개발하고 있는 복잡한 GPS 반대 위장 기술이 있다 [1].

이러한 안전장치와 더불어, 우리를 블루투스 위장 및 방해로부터 보호할 수 있게 만드는 현재의 기술들과 전략들이 있다. 예를들어 보안 접속의 링크 키 (link keys)를 입증하는 것이다. [3]

## 3.5 XYO Network 완화 전략

Archivist (데이터 보관자) 네트워크는 Diviner (답변 집합자)가 의문을 제기한 입증된 데이터를 돌려주는 경쟁적인 네트워크이다. Archivist가 데이터를 받는 시점에서 (황서에 자세히 설명), 네트워크는 잘못된 데이터를 잘라내기 시작한다. 원천으로 회귀한 체인에 저장되어 있던 정보의 전달은 최근에 추가된 잘못된 데이터, 그리고 심지어 위장한 정보도 함께 감지하게 한다. 각각의 Archivist는 또한 네트워크의 타당한 합의를 만들기 위해 다른 데이터 보관자들의 데이타를 교차 점검을 한다. Bridges 와 Sentinel 와 더불어 Archivist가 돈을 받는다는 사실 때문에, 본질적인 암호경제학은 하위 수준의 성분들에게 독을 주는것을 억제한다.

## 3.6 결론

Archivist가 넓은 지역에서 데이터를 꺼내는 것과 해당 지역에 독을 주기위해 물리적으로 어디든 위치에 있는 필요성이 있다는 것을 고려하면, 네트워크는 이러한 공격을 한 공격자에게 벌을 줘야 할 것이다. 이것은XYO Network에서 이러한 공격을 수행하는 공격자들의 의욕을 경제적으로 꺾는다.

---

# 4 Assassination Attack (Assassination 공격)

## 4.1 요약

Assassination 공격은 노드의 신용의 훼손 (캐릭터 훼손) 또는 또 다른 노드를 제대로 기능하지 못하도록 (기술적인 훼손) 하려는 공격자에 의해 규정된다.

## 4.2 동기 부여

Assassination 공격 안에서, 공격자들에 의해서 통제되는 다른 노드들의 상대적 신용을 신장시키기 위해 공격자는 타당한 노드의 평판을 약화시키도록 동기 부여 된다. XYO Network에서의 Sentinels 평판은 작동하는 네트워크를 위해 필수적이기 때문에, 노드의 평판이 쉽게 조작될 수 없게 하는 것은 매우 중요하다.

공격자가 XYO Network에서 잘못된 위치 정보를 알리려고 하는 상황을 고려해보자 (Force Field Attack에서 자세히 설명). 이러한 경우에는 공격자가 개별적 노드의 평판에 해를 끼치기 위해 반드시 맨 먼저 그들을 타겟으로 삼을 것이다. XYO Network의 다른 노드들과의 해당 노드의 연관성을 적게 만들기 위하여, 공격자들이 선별적으로 잘못된 정보를 타당한Sentinels (이런 테이터를 아웃라이너에게 줌)에게 제공하는 곳에서 선택적 신호를 통해 이뤄진다. 이것은 네트워크에 있는 다른 노드들보다 데이터 수집자의 상대적으로 낮은 평판을 야기한다.

덧붙여서, 공격자는 아마 물리적으로 디바이스를 파괴하는것과 같은 노드의 기술적인 훼손 (technical assassination) 관여할 것이다. 이러한 공격 유형은 또한 네트워크의 위치 정보를 조작하고 비기능적 디바이스 (non-functional devices)의 결과를 초래한다.

## 4.3 기술적인 분석

Sentinels에서의 Assassination 공격에서 공격자는 지정된Sentinels와 선택적으로 통신하는 적어도 하나의 디바이스를 배치하는 것이 필요로 한다. 네트워크의 다른 디바이스가 악성 코드에서 서명을 생성하지 못하기 때문에, 악성코드는 오직 타겟이 된 노드에서만 볼 수 있다.

네트워크 외부에 있는Sentinels에게는, 타겟이 된 노드에 의한 정보 수신은 다른 네트워크에서는 맞지 않는다. 이것은 타켓이 된 노드가 악성코드를 알아보지 못하고 일치시켜버린 다른 네트워크에서 평판을 잃는 결과를 가져온다.

## 4.4 프로토콜 완화 전략

Assassination 공격으로부터 보호할 수 있는 핵심은 만약 노드가 선택된 사인에 연관되어 있다면 해당 노드의 평판을 응징하도록 하는 것이다. 이러한 시나리오에서, 악성노드는 다른 데이터 수집자에게 그들을 숨기기 위해 선택적 사인에 관여한다.

각각의 데이터 수집자의 평판을 다른 네트워크와의 일관성에 따라 구축하는 것은 선택적 사인에 관여된 노드를 응징하는 것을 가능하게 한다. 평판이 좋은 노드 (reputable node)는 아마도 네트워크에서 상대적으로 평판이 좋지 않는 노드 (less reputable node)에게 쿼리(query)를 요구할 것이다. 만약 상대적으로 평판이 좋지 않은 노드가 타당하다면, 쿼리에 서명을 하는 것에 최고로 관심을 둘것이고 해당 노드를 네트워크에서 볼 수 있게 만들 것이다. 이것은 해당 노드의 평판을 증진시킨다. 그러므로 만약 노드가 선택적 신호를 실행 했었다면, 상대적으로 높은 평판을 가지고 있는 노드는 악성노드에 쿼리에 서명하는 것을 거부하라는 신호를 보낼 수 있다. 타당한 노드가 이것의 서명을 선택적 서명 협의 (selective signing accusation)가 틀렸음을 입증하기위해 보낼 수 있기 때문에, 이러한 실행은 노드가 실제로 쿼리에 서명하는 곳의 경우에는 부당하게 이용될 수 있다.

각각의Sentinels가 불일치한 정보를 받는 방어 메커니즘을 가지게 됨으로써, XYO Network 내에서 선택적 서명에 응징하는 행동은 캐릭터 훼손 공격을 완화한다.

## 4.5 XYO Network 완화 전력

각각의Sentinels들의 평판을 구축하는 것은 선택적 서명에 연관되어 있는 노드를 막는다. 이것은Sentinels가 선택된 서명을 응징할 수 있게 함으로써 캐릭터 훼손 공격을 완화한다. 물리적인 Assassination 공격 (예를들어, 디바이스 파괴와 같은)을 네트워크 수준에서 막는 것은 점점 힘들어지고 있다. 하지만, XYO Network는 하나의 디바이스를 타켓하는 공격에 탄력적이다.

## 4.6 결론

펑판 시스템의 구축은Sentinels가 서로 좋은 위치에 있도록 하고 공격자를 근절한다. 이것이 XYO Network가 Assassination 공격을 완화시키는 방법이다.

---

# 5 Deception Attack (Deception 공격)

## 5.1 요약

Deception 공격은 공격자가 부정확하지만 개인이 이득을 위한 시스템에서 사용되는 타당한 데이터를 실행하려고 할 때 일어난다.

Deception 공격의 하나의 형태는 Multi-Chain Forging(다중 체인 구축)에 의해 일어난다. 다중 체인 구축은 공격자가 다수의 장소에서 한번에 기본적으로 존재할 수 있는 다중 버전을 유지하는 곳이다.

## 5.2 동기 부여

공격자는 그들의 위치 체인을 포킹(forking)함으로써 정보를 조작할 수 있다. 이것은 한개의 체인 링크(chain link)에 개인 키(private key)를 보냄으로써 이뤄진다. 즉 새로운 지역 블록의 구축 동안 다른 장소에서 하나 혹은 좀 더 많은 담합된 적수들(colluding adversaries)을 만들어낸다. 이것은 같은 원천으로부터 분기된 새로운 장소의 체인의 계속된 구축을 허가한다.

공격자는 위치의 확실성이 명령된 그들의 위치에 대해 잘못된 정보를 퍼트림으로써 이득을 얻을 수 있다. 공격자들이 주어진 시간 동안에 특정한 지역에 있었다는 것을 증명하기 위한 알리바이 구축을 예시로 들어보자. 다중 체인(multiple chains)을 보유함으로써, 공격자들은 정보를 전달하고 있는 체인만이 최고로 그들에게 유리했다고 선별적인 보고를 할 수 있다. 이것은 알리바이가 된다.

## 5.3 기술적인 분석

체인이 좀 더 길어질수록 Deception공격은 점점 실행하기 어려워진다. 시간이 경과함에 따라서, 특정 노드의 정보는 XYO Network를 통해 내보내진다. 이것은 실행 가능한 공격이 기껏해야 과거에 주어진 지점에서의 체인에 약간의 작은 변화를 주는 것을 의미한다.

이러한 과정은 잠재적인 공격을 완전히 사라지게 하지 않는다. Bridge와 동기화될 동안, 악성 데이터 수집자(malicious Sentinel)는Bridges와 공유하기 위해 포크된 체인(forked chains) 중 하나를 선택할 수 있다. 두 체인 모두 타당하기 때문에, Bridge와 다른 디바이스들의 업스트림(upstream)은 체인이 포크(forked) 되었는지 즉각적으로 결론을 내릴 수 없다. 대신에, 노드들은 네트워크의 다른 데이터 수집자와의 통신 기록에 대해 교차 점검을 하는 것은 매우 중요하다. 이것은 한번에 다수의 위치에 노드가 존재하지 않다는 것을 입증하기 위함이다.

## 5.4 프로토콜 완화 전략

선천적으로 XYO Network는 다중 체인 공격(Multi-Chain attacks)을 감지할 수 있다. 노드 체인의 장기적인 포크(fork)는 네트워크의 일반 합의에 상반될 것이다. 위치 데이터의 완전성이 가장 중요할 때 작은 변경을 막기 위하여, 사용자들은 분산된 노드로부터 서명을 가지고 있는 Archivists의 추가적인 확인을 아마 기다릴 것이다. 시간이 경과함에 따라, 포크된 체인 (forked chain)에서 발생된 불일치는 분명해질 것이다.

## 5.5 XYO Network 완화 전략

데이터는 Sentinel 사이에서 통신의 서명 장부 (signed ledgers) 포함한Archivists를 통하여 분산된다. 이러한 실행으로, 심지어 존재하는 체인의 (타당한) 약간의 수정도 감지할 수 있다. 만약Sentinels가 다중 체인 공격을 하려한다면, 상반되는 기록들과 함께하는  다른 노드들은 네트워크에 충돌할 수 있다. 결과적으로, 악성 데이터 수집자의 평판은 떨어지면서, 해당 체인을 네트워크에서 제거하라고 명령할 것이다.

이와 같이, XYO Network는 이러한 공격 유형에 대한 안전장치로써 통신이 교차 점검할 수 있도록 설계됐다.

## 5.6 결론

XYO Network에서 데이터 중복은 어떠한 위반 행동을 한Sentinels의 평판을 네트워크상에서의 무시하는 정도까지 낮춤으로써 불일치한 데이터의 송신을 하지 못하도록 한다.

# 6 Same-Machine Sybil Attack (Same-Machine 시빌 공격)

## 6.1 요약

Same-Machine 시빌 공격은 공격자가 하나의 기계로부터 다중 노드를 만들었을 때 일어난다. XYO Network의 디바이스들이 할당된 특정 ID가 아니기 때문에, 이것은 쉽게 일어날 수 잇다. 공격자는 노드들이 유기적이고 완전하다고 보이는 가장된 노드들 사이에서의 패킷(packet)에 서명함으로써 평판을 강화한다. 그리고 나서 공격자는 노드들을 각각 근처에 있는 다른 그룹의 노드들과 통신하게 만들고 원천증명 체인 (Proof of Origin Chains)안에서의 다른 정보를 가진다. 이것은 높은 원천 체인 스코어(Origin Chain Scores)를 획득한 모든 가장된 노드들의 결과를 낳는다. 이러한 공격은 공격자들에게 노드를 값싸게 대량 생산할 수 있도록 한다. 이러한 노드들은 지역 네트워크 심지어 글로벌 네트워크에서 시빌 공격을 수행하는데 사용된다.

## 6.2 동기 부여

공격자는 아마 특정 지역에서의 영향을 확대하기 위하여 Same-Machine 시빌 공격에 관여하는 것을 추구할 것이다. 같은 디바이스에서 다중 가짜 노드들 (multiple fake nodes)을 만듦으로써, 시빌 공격을 실행하기 위한 장벽은 낮아질 것이다. 이것은 공격자들에게 다량의 악성 디바이스를 만드는 것보다 한 기계에서 가짜 디바이스들을 많이 만드는 것을 훨씬 더 쉽게 한다.

## 6.3 기술적인 분석

디바이스로부터 구별하기 어렵게 보이기 위해 블루투스 장치의 정보를 위장하는 것은 어렵지 않다 [4]. 그러므로, 공격자는 분리된 디바이스처럼 활동하거나 보이는 하나의 컴퓨터로부터 다중 디바이스를 만들 수 있다.

일단 무수한 가상의Sentinels이 만들어지면, 공격자는 마치 그들이 물리적으로 분별력 있는 것처럼Sentinels를 운영할 수 있다. Sentinels는 유기적이며 그들에게서 근접한 다른Sentinels과 연관된 정보에 서명하는 것 같이 보일 것이다. 게다가, 공격자들은 가상Sentinels의 서명을 반영한 디바이스의 가상 지도 (virtual map)를 만들 수도 있다.

## 6.4 프로토콜 완화 전략

Same-Machine 시빌 공격에 대한 방어에 있어서 핵심은 신호 강도를 분석함으로써 복제된 데이터를 감지하는 능력이다. 대량의 가상 Sentinels을 운영하는 컴퓨터는 각각의 Sentinel에 같은 RSSI를 가지고 있는 것처럼 보일 것이다. 결과적으로, 컴퓨터에서 운영하는 각각의 가상 Sentinel는 외부의 Sentinel에게 서로 가까운 것처럼 보일 것이다 (신호 강도 안에서 특정한 파동이 제공되어짐으로써). 이러한 종류의 공격을 막기 위해서, 타당한 Sentinel를 위해 번들 디바이스(bundled devices)를 감지하고 하나의 노드로서 그들의 정보를 다루는 것이 중요하다.

## 6.5 XYO Network완화 전략

Same-Machine Sybil 시빌 공격을 감지하기 위한 XYO Network의 주요 지표는 블루투스 신호 강도 (RSSI)이다. 이것은 두개의 노드가 합의하는 투 웨이 메트릭(two-way metric)이다. 결과적으로, Same-Machine 시빌 공격을 운영하는 한 개의 노드는 이것의 가상 노드들과 같은 신호 강도를 가진 것처럼 보일 것이다. Archivists에 의해 잘라내진 노드 데이터의 중복 제거는 모든 가상 노드들은 하나의 노드로 다뤄진다. 이것은 하나의 기계에서 몇 개의 가상 노드처럼 보여지는 Same-Machine 시빌 공격을 무효하게 만든다.

## 6.6 결론

데이터의 중복을 제거하는 능력이 결부된 XYO Network의 블루투스 신호 강도 감지는 클러스터(cluster)를 하나의 노드로 다룸으로써 가상 노드의 클러스터를 만든 기계로부터의 공격을 완화한다.

---

# 7 Force Field Attacks (Force Field 공격)

## 7.1 요약

Force Field 공격은 잘못된 데이터를 네트워크에 제공하기 위해 Assassination과 전통적인 시빌 공격을 결합한 것이다. 공격은 두 요소로 이루어져 있다: 동시에 공격자의 노드 네트워크가 바깥의 관찰자에게 일치하는 네트워크를 서비스하도록 함으로써, 공격자가 불일치한 정보를 타당한 노드에 제공한다.

## 7.2 동기 부여

이러한 접근은 지역적 시빌 형태를 가진다. 이것은 공격자가 특정 물리적 위치의 권한을 완전하게 통제하는 목표로 하는 곳이다. 하지만, XYO Network에서의 순수한 시빌 공격은 존재하는 좋은 평판의 노드들에게 수적으로 우세하기 위해 확장 기록들과 함께 커다란 분산된 디바이스들을 필요로 할 것이다. 이러한 장애물을 회피하기 위해, Force Field 공격은 하이브리드식 접근을 한다. 이것은 타당한 노드들 간의 불합치를 만들기 위해 Assassination 공격을 통해 존재하는 노드의 평판을 첫째로 타겟을 잡는다.

공격자들이 특정 지역의 완전한 권한을 가지길 원하는 상황을 고려해보자. Force Field 공격을 이용하면서, 공격자들은 첫번째로 불일치한 정보를 가지고 있는 각각의 타당한 노드들을 넘치도록 한다. 네트워크에서 이러한 노드들의 평판은 결과적으로 감소할 것이며 평판 자격 장벽 (reputation qualification barrier)은 낮춰질 것이다. 이렇게 낮아진 장벽과 함께, 공격자들은 타당한 디바이스의 낮춰진 평판에 수적으로 우세한 자신의 디바이스 네트워크를 공급할 수 있다.

## 7.3 기술적 분석

공격자들은 타당한 노드들 사이의 중복을 감소시키기 위하여 선택된 서명을 이용한다. 이것은 존재하는 네트워크를 불일치하게 하기 위함이다. 이것은 악성 노드를 지역 네트워크에 가져온 후, 각각의 노드가 오직 네트워크에 있는 특정 디바이스와 통신할 수 있도록 함으로써 이뤄진다. 각각의 타당한 선택된 Sentinel은 이것이 통신하고 있는 악성 노드의 지역을 송신할 것이다. 반면에 악성 노드들은 Sentinel 주변에서 볼 수 없는 상태로 있을 것이다. 큰 규모에서, 이것은 이러한 네트워크 상태에서 Sentinel가 완전히 다른 해석을 하도록 할 수 있다. Bridge 와 같은 외부의 소스에서 각각의 노드 평판은 낮아질 수 있다.

일단 이것이 이루어지면, Sentinels 자신의 네트워크를 주입하기 위하여 공격자들은 전체 시스템에서 낮아진 평판을 이용할 수 있다. 이것은 디바이스들을 네트워크에 이미 존재하게 하는 것을 가능하도록 만들면서, 다른 Sentinels의 평판이 낮아졌기 때문에 그들은 단순하게 좀 더 중요해진다.

이러한 공격 방식은 지역안에서 존재하는 노드의 수의 여하에 달렸고 이 숫자가 증가할 수록 점점 더 어려워진다.

## 7.4 프로토콜 완화 전략

Assassination 공격의 방지와 유사하게, Force Field 공격의 완화는 선택된 서명 응징에 의존한다. Force Field 공격은 타겟이된 타당한 노드를 XYO Network와 불일치하게 만들기 위하여 악성 노드 연합과 함께 선택된 서명을 이용한다.

평판이 좋은 Sentinels풀은 상대적으로 적은 평판의 노드를 가지고 있고 반응에 거절하는 노드를 보고하는 것은 선택된 서명에 관여하는 노드의 능력을 약화시킨다.

선택된 서명에 관여한 후 공격을 실행하기 위해 만들어진 평판은 빠르게 소멸할 것이기 때문에, 이것은 Force Field 공격을 실행하기 훨씬 더 어렵게 만든다.

## 7.5 XYO Network 완화 전략

XYO Network는 다른 시스템에 순응하지 않은 곳에서 선택된 서명을 시도하려는 노드를 응징한다.
이것은 사인 요청에 반응하는 노드와 XYO Network에 헌신하는 테이터에게 인센티브를 보강한다.
순응하지 않는 노드는 더 낮은 평판의 형태에서 신용성을 잃어, Force Field 공격의Assassination 구성요소가 경제적으로 실행 불가능하게 만든다. 이것은Force Field 공격을 전통적인 시빌 공격으로 바꾸며 과도한 양의 디바이스 및 연산능력을 필요로 한다.

## 7.6 결론

XYO Network에서의 Force Field 공격안에서Sentinel의 평판에 대한 상당한 비용은 공격을 경제적으로 불가능하게 만드는 것이다.

---

# 8 Teleportation Attack (Teleportation 공격)

## 8.1 요약

Teleportation 공격은 공격자들이 네트워크를 통하여 그들의 위치를 다른 위치로 “순간이동” 함으로써 조작할 수 있을 때 일어난다. 만약 스마트폰 또는 블루투스 비콘(beacon)이 공격자의 위치 데이터를 제공하는 Sentinel 처럼 사용된다면, 공격자들은 그들의 Sentinel을 다른 사람에게 보냄으로써 그들의 위치를 조작할 수 있다. 만약 네트워크가 알리바이를 만드는데 사용된다면, 공격자들은 그들이 보고한 위치를 조작하기 위헤서 그들의 Sentinel과 다른 사람의 것을 바꿀 수 있다.

## 8.2 동기부여

이러한 공격 유형은 또한 개인키를 하나 이상의 개개인과 공유하는 공격자들에 의해 소프트웨어 수준에서 이뤄질 수 있다. 만약 네트워크가 호텔 리뷰를 입증하는데 사용된다면, 이것은 사람들에게 온 체인 기록 (on-chain history)에서 신뢰하는 리뷰만을 남기도록 할 것이다. 공격자는 멀리서 그들의 개인 키를 호텔에 있는 개개인과 공유할 수 있고 마치 그들이 지역에서 물리적으로 가깝게 있지 않는 곳에 위치한 것처럼 보이게 할 수도 있다.

## 8.3 기술적인 분석

만약 개인키가 사용자에게 제공된다면, 이것은 이용자의 디바이스에서 보이는 것 그대로 위장된 디바이스를 만들기 위해 공유될 수 있다. 디바이스가 디바이스의 개인 키와 관련되어 있다면, Software Defined Radio의 이용은 적임 파티에게 네트워크에 있는 구체적인 디바이스를 보여줄 것이다. 이것은 사용자의 위치를 입증하려는 시도들을 무효화할 것이다. 이것은 이론적으로 Teleportation 공격에 있는 타당한 디바이스를 분간하는 것이 어렵기 때문에, 또한 블록체인에 있는 데이터에 영향을 끼칠 수 있다.

## 8.4 프로토콜 완화 전략

체인에서의 자연스러운 단절때문에, 이러한 공격 유형에 대항하기 위한 감지 전략은 복잡하다. 예를들어, 만약 핸드폰이 Sentinel로써 사용했고 전원을 껐다면, 이것은 전원을 다시 켤 때까지 네트워크에 통신하지 않는다. 보내진

정보의 차이는 처벌을 받아야만 하는 잠재적으로 잘못된 데이터 시점으로부터 자연스러운 차이를 분간할 수 있도록 복잡한 알고리즘을 필요로한다.

## 8.5 XYO Network 완화 전략

Teleportation 공격 가능성은 Archivists가 서로 정보를 공유할 수 있고 데이터의 실행 가능성을 입증할 수 있는 시점에서 주춤한다. 타당한 디바이스의 수는 서버들에게 넓은 지역에서 데이터를 비교하는 것이 현실적이게 만드는 Network의 업스트림(upstream)을 더욱더 감소시킨다. 이것은 Diviners 에게 복제된 위치 및 Teleportation에서 잘못된 데이터를 관찰하게 한다. 이것은 여과될 수 있고 알고리즘 사용에 의해 처벌을 받을 수도 있다.

## 8.6 결론

Teleportation 공격은 프로토콜 수준에서 알아차리는 것이 어려운 반면에, Archivist와 같은 XYO Network의 더 높은 수준에서의 서버들은 네트워크 상의 악성 데이터를 감지하고 처벌할 수 있다. 서버들간의 정보 교류는 시스템에서 잘못된 데이터를 거르기 위하여 지속적으로 신뢰할 수 있는 정보를 만들며 첨부할 수 있다.

---

# 9 Stealth Attack (Stealth 공격)

## 9.1 요약

Stealth 공격은 네트워크로부터 디바이스 자신을 감추는 것으로 정의된다. XYO Network의 다양한 사용 사례는 견고한 체인 기록을 가지는 네트워크의 디바이스를 필요로한다.

## 9.2 동기 부여

XYO Network에서 Stealth 공격을 수행하는 공격자를 위한 인센티브는 거의 없다. 네트워크는 아무곳에서나 무엇인가 있다는 것을 증명하는 것이 아닌 주어진 위치에서 그것이 존재한다는 확실성을 제공하는 것을 목표로 한다. 이것은 노드가 신뢰되지 않으면 프로토콜 수준의 데이터가 부정확할 수 있다는 것이기 때문에, 이것은 중요한 차이이다.

그렇기는 하지만, 공격자는 타당하게 보일 수도 있는 잘못된 체인 데이터를 만들기 위해 전략적으로 그들의 휴대폰 혹은 비컨(beacon)의 위치 서비스를 켜고 끌 수 있다. 이것은 공격자들에게 그들이 데이터를 보고하고 싶지 않아서 네트워크로 부터 그들 자신을 본질적으로 숨길 수 있도록 한다. 또한 네트워크가 그들에게 유리할 때 네트워크에 다시 나타날 수 있도록 한다.

## 9.3 기술적인 분석

Stealth 공격은 네트워크에서 디바이스를 끔으로써 이뤄질 수 있다. 좀더 복잡한 접근은 네트워크에서 디바이스를 숨기는Faraday cage (패러데이 케이지)를 사용할 수 있다. 이러한 공격 유형에 비물리적으로 접근하는 것은 Denial of Service Attack (Denial of Service 공격)을 통해 지속될 수 있다.

## 9.4 프로토콜 완화 전략

Stealth 공격에 대항하기 위한 조치는 블루투스 및 다른 디바이스들이 네트워크로부터 쉽게 접속을 끊을 수 있기 때문에 복잡할 수 있다. 이러한 취약성을 완화하기 위한 주요 전략은 강한 소프트웨어 층을 구축 및 사용하는 것이다.

이러한 소프트 웨어는 망가진 체인 데이터에 송신하는 Sentinels 및 Bridges를 처벌한다. 알고리즘이 타당한 데이터와 타탕하지 않은 데이터간에 미묘한 차이점에 더 잘 이해할 수 있게 되면서, 시간이 지날수록 감지 능력은 성장할 것이다.

## 9.5 XYO Network 완화 전략

노드 기록안에서의 차이는 XYO Network에서의 지속적인 Proof of Location (지역 증명)을 필요로 하는 경우에는 즉시 의심을 받을 것이다. 데이터가 Archivists에 닿을때, 이것은 엄격한 가지치기 (rigorous pruning)과 이러한 차이를 감지하고 불일치를 응징할 수 있는 여과 과정을 겪는다. XYO Network의 이런 주요한 특징은 물리적인 세계의 데이터가 엉망인데도 불구하고 좀 더 정확한 위치를 제공하도록 한다.

## 9.6 결론

XYO Network를 사용하는한 Stealth 공격은 경제적으로 살아남을 수 없다.

---

# 10 Denial of Service Attacks (Denial of Service 공격)

## 3.1 요약

Denial of Service 공격( DoS)은 악성이거나 사용자들이 지역적, 시스템 범위의 야기시킬 때 일어난다.

## 3.2 동기 부여

공격자는 Proof of Location (지역 증명)을 입증할 수 있는 것을 막기 위하여 XYO Network를 방해하려고 할 것이다.

## 3.3 기술적인 분석

블루투스 프로토콜의 환경 때문에, 블루투스 비컨은 한번에 오직 하나의 디바이스에만 연결할 수 있다. 이것은 인증되지 않은 명령어를 받아들이는 디바이스는 쉽게 네트워크에서 중단될 수 있다는 것을 의미한다. 이것은 블루투스 명령어에 송신하는 하나의 디바이스를 비교적 쉽게 끊임없이 이용하도록 하는 모바일 애플리케이션을 사용함으로써 이루어질 수 있다. 대부분 비컨에 있는 “소리 실행” 파라미터(parameter) 처럼, Hex 값을 주어진 파라미터의 디바이스에 보내는 것은 디바이스와의 연결을 만든다. 만약 연결이 구축된다면, 다른 디바이스가 이것에 송신할 수 없도록 한다. 이것은 지속적으로 다양한 Hex 값에서 사정 거리내에서의 네트워크 비컨으로 지속적으로 송신하기 위한 스크립트를 운영할 수 있는Software Defined Radio 사용에 의해 증폭된다.

## 3.4 프로토콜 완화 전략

XYO 네트워크에서 블루투스 디바이스는 오직 입증된 명령어만 받아들일 수 있으며 화이트 리스팅 MAC 주소만 사용될 수 있다. 서면으로 입증된 명력어 수의 감소는 이러한 공격 벡터 접근을 최소화한다.

## 3.5 XYO Network 완화 전략

XYO Network는 Archivist 및 Diviner 서버를 운영하는 사용자들로 구성된다. 이러한 두개의 구성원들은 그들의 동료들과 정보와 타당성을 공유한다. 이것은 구성원들의 “스택(stack)”에서 선택된 쿼리(query)가 대답을 되찾아 오도록한다. 프로토콜 수준의 네트워크 서비스의 작은 부분을 부인하는것은 가능하지만, 네트워크의 넓이와 크기는 경제적으로 실행 불가능하게 만든다.

### 3.6 결론

XYO Network의 분산된 환경 때문에, Denial of Service 공격에 시도됐음에도 불구하고 네트워크는 작동된다.
DoS는 무거운 연산력과 전체 스택 (entire stack)을 공격하기 위한 물리적인 접근을 필요로하기 때문에, 심지어 XYO Network의 작은 부분의 타게팅은 비싸고 경제적으로도 비합리적이다.

---

## 11 감사의 말씀

본 적서(red paper)는 XYO Network의 백서와 XYO Network의 녹서에 따르는 보안에 대한 것이다. 우리는 세부적 검토 작업과 최고의 실행 능력을 보여주신 Christine Sako에게 감사의 말씀을 드린다.

---

## 참조문헌

[1] Jafarnia-Jahromi, Ali. Ali Broumandan, John Nielsen, and Gerard Lachapelle. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. https://www.hindawi.com/journals/ijno/2012/127072/cta/ International Journal of Navigation and Observation, Alberta, Canada, May 2012.

[2] Padgette, John, John Bahr, Mayank Batra, Marcel Holtmann, Rhonda Smithbey, Lily Chen, and Karen Scarfone. Guide to Bluetooth Security. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf U.S. Department of Commerce, National Institute of Standards and Technology, May 2017.

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

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

[5] Chief, Enforcement Bureau. FCC Enforcement Advisory. https://apps.fcc.gov/edocs public/attachmatch/DA-14-1785A1.pdf FCC.gov, December 8, 2014.

## 용어 설명

**정확도(accuracy)**
어떠한 데이터 포인트 또는 휴리스틱(heuristic)이 구체적인 오차 한계 내에 있음에 대한 신뢰성 척도.

**Archivist**
Archivist는 모든 이력 장부들을 저장하기 위하여 분산화된 데이터 세트의 일환으로 휴리스틱을 저장한다. 일부 데이터가 소실되거나 또는 일시적으로 이용 불가능할 경우에도 시스템은 정확도만 약간 낮아질 뿐 기능을 지속한다. Archivist는 또한 장부들을 색인화하여 필요 시 장부 데이터 열을 반환할 수 있다. Archivist는 로우 데이터(raw data)만을 저장하며 데이터의 검색에 대하여만 지불을 받는다. 저장은 항상 무료이다.

**Bridge**
Bridge는 휴리스틱 트랜스크라이버(transcriber)이다. 이는Sentinel로부터 Diviner로 안전하게 휴리스틱 장부를 전달한다. Bridge의 가장 주요한 측면은 Diviner는 Bridge로부터 받은 휴리스틱 장부가 그 어떠한 식으로든 변경되지 않았다는 안심을 할 수 있다는 점이다. Bridge의 두번째로 중요한 측면은 오리진 메타데이터(metadata)의 추가적인 증명을 더해준다는 점이다.

**확실성(certainty)**
어떠한 데이터 포인트 또는 휴리스틱(heuristic)이 오염이나 조작으로부터 안전할 것이라는 가능성의 척도.

**암호경제학(cryptoeconomics)**
분산화된 디지털 경제에서 재화와 서비스의 생산, 분배 및 소비를 관장하는 프로토콜에 대하여 연구하는 공식적 분야. 암호경제학은 이러한 프로토콜의 설계 및 특징화에 집중하는 실제 과학이다.

**Diviner**
Diviner는 XYO Network에 의하여 저장된 이력 데이터를 분석함으로써 주어진 쿼리에 대하여 답변을 한다. XYO Network에 저장된 휴리스틱은 해당 휴리스틱의 타당성과 정확도를 결정하기 위한 높은 원천증명 수준을 갖추어야 한다. Diviner는 그 원천증명을 토대로 증인을 판단함으로써 답변을 확보 및 전달한다. XYO Network는 무신뢰성 시스템이기 때문에 Diviner는 정직한 휴리스틱 분석을 제공하도록 유도되어야 한다. Sentinel 및 Bridge와는 달리 Diviner는 작업 증명을 이용하여 블록체인에 대한 답변을 추가한다.

**원천 체인 점수(Origin Chain Score)**
T원천 체인에 대하여 그 신뢰성을 결정하기 위하여 배정된 점수. 이 평가는 길이, 얽힘, 오버랩, 및 중복을 고려한다.

**작업증명 체인(Proof of Origin Chain)**
일련의 연결 증인(Bound Witness) 휴리스틱 장부 엔트리를 함께 연결하는 잠정 키 체인(Transient Key Chain).

**Sentinel**
Sentinel은 하나의 휴리스틱 증인이다. Sentinel은 휴리스틱을 관찰하며 잠정적 장부를 생산함으로써 그 확실성과 정확성을 보증한다. Sentinel의 가장 중요한 측면은 Diviner들이 원천증명을 더함으로써 동일한 소스로부터 온 것이라는 점을 확신할 수 있는 장부를 Sentinel이 생산한다는 점이다.

**무신뢰성(trustless)**
시스템 내의 모든 당사자들이 정규적(canonical) 사실이 무엇인가에 대한 합의에 도달할 수 있는 특성. 파워 및 신뢰가 그 어느 개인이나 주체(예: 은행, 정부, 금융기관 등)에 집중되기 보다 네트워크의 관련 당사자(예: 개발자, 마이너, 소비자 등) 사이에 배분이 된다. 이 개념은 매우 오해하기 쉬운 일반 용어이다. 블록체인은 사실상 신뢰를 배제하지 않으며, 대신에 시스템 내의 제반 단일 행위자로부터 요구되는 신뢰의 양을 최소화하는 것이다. 이는 행위자들이 프로토콜에 의하여 정의된 규칙에 협조하도록 장려하는 경제적 게임을 통하여 시스템 내에서 여러 행위자들 간에 신뢰를 배분함으로써 이뤄진다.

**XYO Network**
XYO Network은 “XY Oracle Network”를 의미한다. 이 네트워크는 Sentinel, Bridge, Archivist 및 Diviner가 포함된 XYO 실행 구성요소/노드의 전체 시스템으로 구성된다. XYO Network의 주요 기능은 디지털 스마트 계약이 실제 세계의 지형 위치(geo-location) 검증을 통하여 실행될 수 있는 포털로서 기능을 하는 것이다.