Computer Science Department, Technion
Project in Computer Security (236349)
Spring 2018-2019

Project Proposal: Trusted Network for Anonymously Sharing Cyber Security Information over Blockchain

Advisors: Amir Schwartz, amir.schwartz@citi.com, 054-3055607
Danny Tylman, danny.tylman@citi.com, 050-9386265

Goal

The goal of the project is to build a prototype of a system for anonymously sharing sensitive information on cyber security attacks, breaches and incidents based on a DLT (Distributed Ledger Technology) platform.

Several key characteristics of the solution are:

1. Only pre-approved participants can share and use the data – to prevent any malicious parties from feeding false information, obtaining intelligence, etc.
2. Sharing is done anonymously (following enrollment) – to allow participants to share information safely, securely and comfortably, without disclosing their identity.
3. Information should be trusted – to ensure authenticity and validity.

Background

Organization are reluctant to share sensitive information on cyber security attacks, breaches and incidents they experienced. There are various reasons for adopting a discreet policy when it comes to cyber security, such as risk of exposing information on security tools and disclosing security issues, avoiding negative PR (Public Relations), regulatory and compliance limitations, and more. Yet it is evident that there is a lot of potential value in real-time sharing of such information. For example – getting alerts and heads-up from trusted peers who encountered attacks, allowing time to prepare in advance and prevent similar incidents, helping to detect attacks and improve the triage and IR (Incident Response) processes, providing post-factum statistics and analytics on attacks and attackers, etc.

It seems that DLT might be a suitable solution in this case for the following reasons:

- Decentralization: No single entity should control and “own” the network and the data.
- Anonymity: Publishing of information must be done anonymously to protect the identity of the participants.
- Transparency: Each participant should be able to use the information independently and transparently, without relying on a central authority or other participants.
- Immutability: Once reported, data cannot be changed by any participant.

Delivery

The solution should have two layers:

1. Infrastructure layer – based on an existing enterprise-grade DLT platform.
2. Application layer – built on top of the infrastructure layer.

The application layer should allow a participant to connect to the infrastructure layer, share information and view information shared by other participants. The onboarding process of a new participant can be implemented as part of the solution itself, or externally.

Several open questions that should be addressed during the project:

- Define the onboarding and validation process – during enrollment the identity of a new participant should be known and validated.
- Maintain complete anonymity while sharing information – there should be no way to link the data reported with the reporter.
- Which DLT platform to use: permissioned/permission-less, private/public, etc.

Shared information can include (among other things) the following: short free-text description of the attack/breach/incident, TTPs (Tactics, Techniques and Procedures), IOCs (IP addresses, domain names, file hashes, email addresses, etc.), false positive alerts, etc.

The solution should not be based on the public Blockchain, instead the following enterprise-grade DLT platforms should be considered (other platforms can be reviewed as well):

- Corda: https://www.r3.com/corda-platform/
- Hyperledger Fabric: https://www.hyperledger.org/projects/fabric
- Quorum: https://www.jpmorgan.com/global/Quorum

The following enhancements to the basic solution can be considered:

1. Provide a mechanism to automatically sanitize shared information to make sure it does not identify the reporter in any way.
2. Calculate a “grade” for published information based on its communality.
3. Provide a secure private communications channel for peers if they wish to continue interacting directly, potentially consider using TLP (Traffic Light Protocol).
4. Provide a mechanism to allow updating confidence level per peers.

High-level breakdown to phases/tasks:

1. Research and define the onboarding process for a new participant.
2. Research and define how information can be shared with absolute anonymity.
3. Choose the underlying DLT platform.
4. Define and design the application layer: architecture, functionality, UI, etc.
5. Build the end-to-end solution prototype.

Prerequisites

- Students should have sufficient background in DLT/Blockchain.

Remarks

- We have no specific preferences for the programming language you use.