Howard Poston

Blockchain & Cyber Security

Threat Modeling for the Blockchain

July 02, 2019

Blockchain technology is an exciting new technology with a great deal of potential. With this potential comes the need to explore the security of this new technology. There has been a great deal of work in this space; however, no comprehensive threat model exists that classifies all potential threats and attack vectors within the blockchain ecosystem. When discussing potential security threats to a system and attempting to analyze whether a system is secure by design, it' is extremely useful to have a framework to use in classifying known attacks and pointing out ones that potentially have been overlooked. In this post, blockchain security threats are mapped to STRIDE, a well-known threat model developed by Microsoft, to create an effective threat model for the blockchain.

STRIDE and the Blockchain

The STRIDE framework was developed by Microsoft to help in threat modeling. Each letter in the STRIDE acronym is designed to refer to one of the most common threats in cybersecurity:

- Spoofing: Spoofing refers to the ability of the attacker to masquerade as another on the system.
- Tampering: Tampering attacks violate the integrity of the data stored on the protected system.
- Repudiation: Repudiation is the ability of a user to deny that they have taken a certain action.
- Information Disclosure: Breaches of confidentiality fall under information disclosure.
- Elevated Privileges: If a user manages to gain unauthorized levels of control over the system, this is a privilege escalation attack.
    - In the context of the blockchain, we can break up elevated privileges based upon whether the attacker has unauthorized access to a user's account, an elevated level of control over the blockchain system (i.e. in a 51% attack), or unauthorized permissioned access to a smart contract.

The STRIDE framework is useful for defining the potential effects that certain vulnerabilities or attacks can

Howard's Blog

Check in to stay current on blockchain and cybersecurity information.

Featured Posts

Blockchain Security vs. Crypto Hacks
Jul 3, 2019

Threat Modeling for the Blockchain
Jul 2, 2019

Mapping the OWASP Top Ten to Blockchain
Feb 12, 2019

Howard Poston

Blockchain & Cyber Security

have on the security of a system. However, blockchain systems are a complete environment, including everything from the cryptographic primitives that underpin their security to the smart contracts that extend the functionality of the blockchain system.

In order to have a meaningful discussion about a blockchain threat model, it's useful to break up the blockchain ecosystem into its various levels. For the purposes of this post, the following breakdown is used:

- Fundamentals: The underlying components used to build the blockchain.
  - Cryptographic Primitives: The hash functions and public key cryptography used to ensure data integrity and provide user authentication.
  - Data Structures: The structure of the blocks used to store transaction data and the hash functions used to chain them together.
- Protocols: The definitions of how blockchain nodes should interact when working to maintain the shared distributed ledger.
  - Consensus:
  - Block Creation:
- Infrastructure: The nodes that work to maintain the distributed ledger and the network that they use to communicate.
  - Nodes: Computers running the blockchain software and maintaining a copy of the distributed ledger.
  - Network: The underlying network that the nodes use to communicate and the protocols that define how communications occur within the blockchain ecosystem.
- Advanced: Many blockchain solutions do not limit themselves to the basic blockchain protocol defined in the Bitcoin whitepaper. These advanced components are an important component of these blockchain's security and their threat model.
  - Smart Contracts: Smart contracts allow third-party code to be uploaded to and executed on the distributed ledger.
  - Blockchain Extensions: The basic blockchain technology can be extended by systems built either on top of it (state channels, side chains,

Howard Poston

Blockchain & Cyber Security

etc.) or through connections to external systems via APIs.

With the STRIDE threat model and the framework of the blockchain ecosystem, we have what we need to begin threat modeling for the blockchain.

Blockchain Threat Modeling

The blockchain threat model is presented in the table below. Using the STRIDE model and the levels of the blockchain ecosystem, it's possible to classify each attack vector based upon its potential effects. Each cell shows the different attacks that can be used to affect a given component of the STRIDE model at a level of the blockchain ecosystem. Each attack vector includes mouse-over text that describes how the particular effect can be accomplished by that attack.

		Spoofing	Tampering	Repudiation	Information Disclosure	
Fundamentals	**Cryptographic Primitives**	Private Key Phishing Shor's Algorithm	Grover's Algorithm		Private Key Shor's Algorithm	
	Data Structure		Transaction Malleability			
Protocol	**Consensus**		51% Long-Range Nothing at Stake	51% Long-Range		51 Ar Di In Lo
	Block Creation		Frontrunning			Tr Fl
Infrastructure	**Nodes**	Malware	Malware		Malware	Fa Up M
	Network		Eclipse/Routing Network Design		Network Design	Ec Ne De Ph At Po M
Advanced	**Smart Contracts**	Delegatecall	Arithmetic			Ac O

			Bad Randomness Reentrancy Short Addresses Timestamp Dependence Unchecked Returns			
	Blockchain Extensions	Insecure APIs				

This blockchain threat model represents my personal attempt to classify the currently known attack vectors against blockchain systems and is designed to be a constant work in progress as new attack vectors are discovered against blockchain systems. I plan to continue to update and refine this model and would appreciate any comments or input.

❤ *1 Likes*

Prev / Next