Security Challenges of Blockchain-Enabled Environments

Our Mission: Hacking Anything to Secure Everything

Christopher Thomas
Senior Managing Consultant, IBM X-Force Red

Who is X-Force Red?

X-Force Red is an autonomous team of veteran hackers, within IBM Security, hired to break into organizations and uncover risky vulnerabilities that criminal attackers may use for personal gain.

X-Force Red offers offensive security services which includes penetration testing, vulnerability management programs, red teaming, code review, static analysis and vulnerability assessments.

Their goal is to help security leaders identify and remediate security flaws, covering their entire digital and physical ecosystem.

170 people globally & counting

Industry renown hackers such as:

- Space Rogue
- Evilmog
- Q
- Videoman
- Q0phi
- retBandit
- keybored

and more…

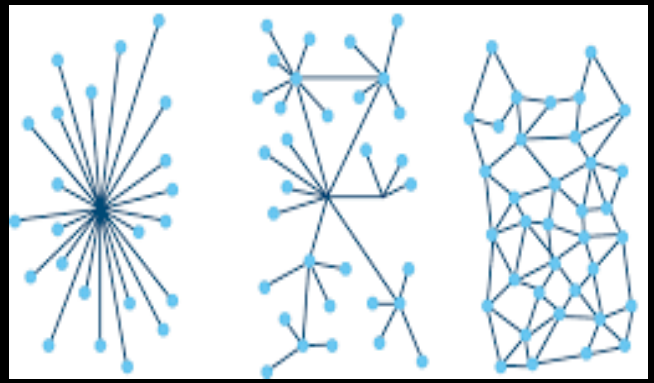
About Me

- Senior Managing Consultant, IBM, X-Force-Red
- Been Hacking Systems Since I Was 11
- Penetration Tester of 11 Years
- Writing Code Since I Was 10
- Design/Architect Solutions To Problems
- Manage & Maintain The EMEA Penetration Testing Network For XFR
- Got Into Cryptocurrencies in 2012
- Started Researching Blockchian Technology In 2016

What is Blockchain?

Blockchain is an immutable distributed ledger technology that changes the way in which organizations share, process, and secure transactions.

- Its Transparent
- Ensures a Level of Trust
- Decentralized
- Immutable



History of Blockchain Technology

Concept was steadily built upon over a decade by various people:

- 1982: “eCash” - David Chaum
- 1991: “How to Time-Stamp a Digital Document” - Haber and Stornetta
- 1996: “How To Make A Mint: Cryptography of Anonymous Electronic Cash” - NSA
- 1997: “Hashcash” - Adam Back
- 1998: “B-Money” - Wei Dai
- 2004: “Reusable Proofs of Work” - Hal Finney
- 2005: “Bit Gold” - Nick Szabo
- 2008: “Bitcoin: A Peer to Peer Electronic Cash System” - Satoshi Nakamoto
- 2014: “Ethereum Yellow Paper” - Vitalik Buterin & Dr. Gavin Wood
- 2015: “HyperLedger” Announced – Linux Foundation
- 2017: “HyperLedger Fabric” Announced

Blockchain Security Definition:

Security in blockchain can be defined as the protection of transaction information and data in a block against internal, peripheral, malevolent and unintentional threats.

Public vs Private Blockchains

Let The Battle Commence!

Public Blockchains

Possible Candidates
- Ethereum
- NEO
- IOTA
- NANO

- Limited Side-Chain Capability
- Focused Around Monetary Transactions
- Completely Open/Public
- Little/No Granular Access Controls
- 100% Distributed
- Trustless Architecture

Private Blockchains

Possible Candidates
- HyperLedger
- R3 / Corda
- Multichain

- Can be Completely Private
- Ability To Create Side-Chains/Channels
- Granular Access Controls
- Requires a Level of Trust
- Introduces Centralisation

Is Blockchain Inherently Secure?

Yes… AND … No!

Blockchain is theoretically secure insofar as its fundamental concept:

- Data is Secured in a Cryptographical Manner.
- Highly Tamper Proof.
- Records/Data Is Seen By Participants.

So Where Do The Insecurities Come From?

- One Chain Does Not Fit All.
- Blockchain Frameworks Are Highly Customizable / Modular.
- “The Meat Factor” / People.

Security Challenge Areas

- Architecture
- Cryptography / PKI
- Smart Contracts / Chaincode
- Governance
- Application Security
- Identity
- Consensus
- Privacy & Access of Data
- Off-Chain Data Access

Security Challenges: Architecture

Decentralization

On-Premise Risks:

- Shared Infrastructure
- Infrastructure Is As Only Secure As The Providers Standards

Off-Premise Risks:

- Security is Only As Good As The Applied Standards

- Centralization of Key Functions
  - Orderers & Peers (HyperLedger)
  - Mining/Pools (Cryptocurrencies)
  - Masternodes (Cryptocurrencies)
  - Development Process

- It’s About Finding A Happy Medium Between Centralised and Decentralised.

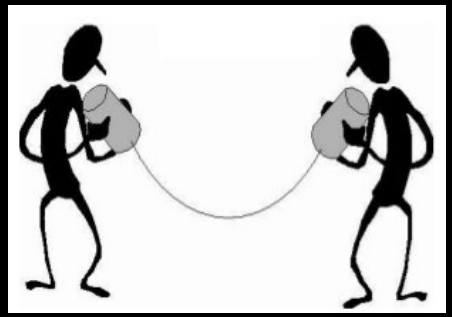
Communication Channels

Network

- How will systems communicate?
  - From a Network/IP Perspective?
  - From an Application Protocol Perspective?
- What Services Will Be Exposed & Who Has Access?

Channels / Side Chains

- How Has The Organization Mapped Their Data?
- Who Has Access To What?
- Where is The Data Stored?



Blockchain Interfaces

Any Available Service is A Potential Avenue For Attack

- HyperLedger Interfaces
  - API (Fabric)
  - gRPC
- Cryptocurrency Interfaces
  - P2P Protocol
  - Masternode Registration & Management Functionality
- Off-Chain Data Access
- Ingress/Egress Points of External Systems (Application Bridges)

Risk Inheritance

If You Build A House on Sand It Will Inherently Be Insecure.

- Standard Hardening Practices Still Apply
  - Physical/Hardware
  - Networking
  - Operating Systems
  - Application Services

- Mapping of Organizational Structure
  - Roles/Accounts
  - Certificates / PKI

Potential Solutions

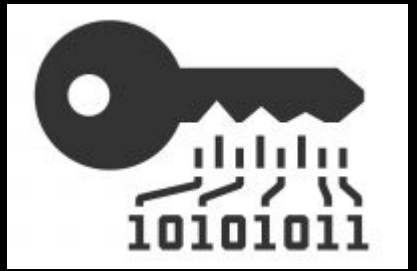
- Apply The Principle of “Defense in Depth”
- Environment Hardening, Bottom Up Approach:
  - Network
    - VLANS
    - Firewalls (Host based & Network)
    - TLS (or similar) Communication
  - Operating System & Application Services
    - Apply Existing Hardening Standards
- Penetration Tests
- Enhanced Threat Detection & Response Capabilities
- Redundancy Testing
- DevOps Flow
  - Code Review & Publication
  - Architecture Deployment

Cryptography / PKI

Why Is It Important?

Cryptography is a Key Foundation of Blockchain Technology

- Cryptography Is Used Throughout The Blockchain:
  - Signatures
  - Hashing
  - Identity
- Ensures Past Records Cannot Be Tampered With
- Securing The Identity of Users & Systems
- Enhances Privacy of Data Stored on the Chain
- Enforces Non-Repudiation



Challenges

- Encryption Protocols
- Standard Certificate Practices
  - Issuance / Provisioning
  - Revocation
  - Certificate Authorities
- Certificate Structure
  - Intermediary CA’s
  - Mapping of Organizations Structures
- Storage of Key Material
  - HSM’s
  - KeyStore's
  - Off-Chain Encryption
  - Sharing of Key Material

Potential Solutions

- Defining & Enforcing Minimum Encryption Requirements
  - Hashing/Signing Algorithms
  - Key Size
- Utilize HSM’s
- Consider Utilizing Zero-Knowledge-Proofs (ZKP) or Similar
- Strict Enforcement of Policies:
  - Key & Lifecycle Management
  - Key Handling
  - Exchanging Key Material

Security Challenges: Identity

Why Is It Important?

Identity is a Fundamental Part of The Blockchain

- Identifies Users and Who Is Able To Participate on The Network
- Provides Non-Repudiation Through The Use of Signatures
- Provides Privacy Through Cryptographically Secure Transactions
- Establishes Roles and Entitlements

At What Level?

- Identity Can Take Multiple Forms Within a Blockchain Environment:
  - User
  - Role
  - Peer
  - Organization
- Member/Organization Management & Provisioning
- At What Level Are User Permissions Implemented?
  - MSP / Blockchain
  - Application
  - Federated
- How Does The Blockchain Handle off-chain Authentication? (e.g. OAUTH)
  - How Are The User Identifiers Tied to The on-chain Data?

Challenges

- Life Cycle Management
  - On/Off Boarding
  - Entitlements / Roles
  - Change Control
- Application Identities
  - How Do They Map To The Chain
  - Session Management
- Verification Responsibilities
  - High-Privileged / Administration Accounts
  - Do Organizations Manage Their Own Users?

Potential Solutions

- Well Defined Lifecycle Management Policy
- Membership Service Provider (MSP)
- MSP Identity Mixer
- Utilize Mature External Authentication Services & Protocols
- Ensure Sufficient User Identification Information is Stored on The Chain
- Strong Access Controls
- Well Defined User Mappings Between The Blockchain & Front-End Environment

Security Challenges: Application Security

Why Is It Important?

Blockchain Only Accounts For a Small Portion of The Overall Environment

- Applications Interact With The Underlying Blockchain
- Contains A Large Amount of Business Logic
- Standard Attack Vectors Apply
- Compromise Could Result Negatively on Integrity & Availability of Chain Data

Challenges

Applications are Centralized Where the Underlying (Blockchain Data Is Decentralized)

- Enforcing Data Integrity When Committing Information to The Chain
- Ensuring Secure Programming Practices Are Followed
- Ensure Sufficient Controls Are Applied Across All Trust Boundaries
- Granular User Controls – Enforcing Strict Access Controls & Separation of Privileges.
- Complexity of Multiple Components

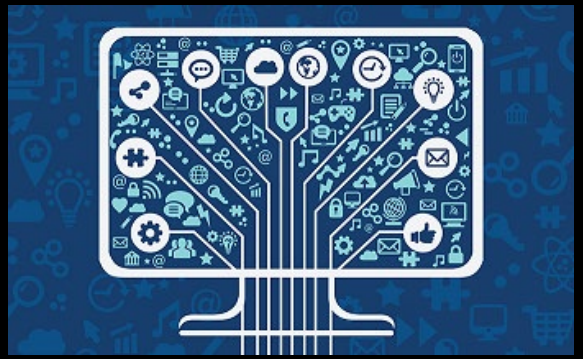
Potential Solutions

- “Full Scope” Penetration Testing
- Secure Coding Practices
- Integrating Static Code Analysis (or similar) Into The DevOps Pipeline
- Web Application Firewalls
- Treat Infrastructure As Unknown
- Regularly Patch The WORLD!
- Secure Back-End Network Connections
- API Security Strategy
- “Full Scope” Penetration Testing (I SAID IT AGAIN!)

Security Challenges: Privacy & Access of Data

Why Is It Important?

- Compliance & Regulation Requirements, Such As:
  - GDPR
  - HIPAA
- Disclosure Information Could Negatively Impact on The Business/Organization
- Secure Storage of Data
- Need To Get It Right First Time
  - Data on The Chain Is Immutable



Challenges

- Privacy Leakage
- Ensuring Confidential Data Is Encrypted
- Mapping Application User Permissions To Blockchain Permissions
  - Lifecycle Management
  - Are Roles Used To Govern Access?
- Ensure Any Data Committed Is Valid and Not Malicious
  - Data on The Chain Is To Be Trusted Right?
- Partner/Third-Party Vetting

Potential Solutions

- Implement Zero Knowledge Proofs (ZKP)
- Zero Knowledge Asset Transfer (ZKAT)
- Identity Mixer
- Ensure Strict Access Controls & Auditing
- Encrypt All Data At Rest

Security Challenges: Off-Chain Data Access

Why Is It Important?

Not All Data Can Be Stored on the Chain

- Too Costly
- Additional Privacy Concerns/Requirements
- Chain Data Is Immutable – Multiple Instances of Documents/Data
- Size of Data is Prohibitive

Challenges

- Keeping Data Deterministic
- Ensuring Data Is Decentralized
- Modification of Data
- Handling Key Material if Data Is Encrypted
- Mapping Off-Chain Access Permissions To On Chain Accounts/Chaincode

Potential Solutions

- Oracles
- Data-Lakes
- Sharding of Information
- IPFS
- State Channels

Security Challenges: Smart Contracts / Chain Code

Why Is It Important?

Chaincode/Smart-Contracts Encapsulate Business Logic on The Chain

- Controls the Basis on Which Users Are Able To Read/Write To the Chain
- Maps Attributes and Role-based Entitlements
- Shared Among All Participants
- Executed on All Peers Within a Channel
- Chaincode / Smart Contracts Are Trusted
- Chaincode / Smart Contracts Are Autonomous

Challenges

- Human Error
- Poor Code Design
- Code Vulnerabilities
  - Injection
  - Error Handling
  - Business Logic
  - Code Supply Chain
- Data Manipulation and/or Denial
- Keeping Third Party Libraries Up To Date
- Publication of Malicious Contracts / Code
- Mapping Complex Processes Can Be Difficult

Potential Solutions

- Secure Programming Practices
- Ensure Third-Party Libraries are Up to Date
- Secure Code Review
- Strong Change Control Process
- Penetration Testing

Security Challenges: Governance

Why Is It Important?

How Do You Agree Across Multiple Organizations?

- Each Organization / Participant Has Their Own:
  - Risk Profile
  - Compliance Requirements
  - Policies/Procedures

- Possible Conflicts on Direction or Operation
  - Reduced Implementation / Rollout Timeframes
  - Possible Legal Scenarios

- May Cause Inconsistencies Between Participants
  - Introduce Weaknesses to The Chain/Environment

Challenges

- Define and Agree Upon a Common Framework That Includes:
  - Change Management
  - Compliance
  - Operational Details
  - Identity Management
  - Security / Hardening Processes
  - Incident Handling & Auditing
  - Sharing of Relevant Information
  - Security Assessments / Penetration Testing
- Time Consuming
- Needs to Be Defined During The Design Phase

What's Next?

What Are We Lacking?

- Architectural & Design Patterns
- More Security Research:
  - Risk Models / Attack Vectors
  - Security Assessment Methodologies
- Use Cases & Implementations Have To Mature
- Compliance / Regulations / Standards
- Maturing of Technology
- Cross-Chain Idea Exchange & Development (Enterprise <-> Cryptocurrency)
- Investigate Bleeding Edge Ideas


Q & A

X-Force Red

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM