Security Vulnerabilities in Applying Decentralized Ledger Systems for Obfuscating Hardwares

Jaganath Prasad Mohanty , Kamalakanta Mahapatra
National Institute of Technology, Rourkela, India

Abstract

Security in daily transactions, not only in the financial sector, but also in various upcoming Industrial smart application areas needs a generic solution, out of the cat and mouse race, where frequently vulnerabilities are pointed out and a quick patch is fabricated to resolve the issue temporarily. An impromptu solution to this protracted issue will not be enough to solve on the long run, thus dedicated researchers have been putting efforts to their best for finding the real problem by asking the right questions. Through this paper authors have attempted to trace the current issues in handling decentralised ledger system using blockchain technology and discussed state of the art management in auditing hardware obfuscation techniques.

Keywords: Blockchain; Privacy, Distributed Ledger, Hardware, Security, Consensus

1. Introduction

Decentralized Ledger systems using the decade old Blockchain technology are a massive turnaround for not only the digital cryptocurrency but also governmental data handling and industrial as well as smart devices. This technology in a generic statement consists of a chain of blocks to hold records of transactions and data in a cryptographically sensitive tamper resistance style. A necessary implementation of this technology needs hashes of previous block for linking, digital timestamps and a nonce as unique numbers for each block to authenticate its merit [4]. It asserts power to participating nodes in a decentralized pattern to assure no single entity being responsible for a system failure. As authority is shared by all participants, this technology is distributed by architecture.

An intermediary amid communicating parties enhances data breach and augments uncertainty in between them. The immutability nature of the triple entry auditing ledger system conveys assurance amid nodes and protects them from utilizing extra resources. Through consensus mechanism with a set of agreeable protocols, basic standards are set to build new nodes in order to prove authenticity and hence establish proof-of-work [6]. Cryptographic functions are used to sign linearly connected blocks for prevailing security. Permissioned and permission-less categories are set to control the creating and writing data in the blocks of public and private entities. In digital cryptocurrency, miners are incentivized to create authentic blocks with their proof of work, proof of stake or upcoming methods to be broadcast to other nodes for acceptance.

Hash functions are created to link between blocks as well as authenticate each node with digital signs. Protocols aid in observance of the systems security and integrity, as well as defining the difficulty for creation of new nodes. Nonce is used to generate this special blocks and bred mathematically solving the difficulty that needs huge computational resources. This should be below a particular threshold value, to be accepted as new block by other valid nodes in the chain. Thus a single honest node will be sufficient to maintain consensus in the system and report any discrepancy. The di□culty of hostile takeovers provides an interesting new lens for comparing decentralized consensus protocols [5]. A weakness and strength can be assumed when an imperative change in one of the blocks disturbs the linearity of the sequence and can be viewed by the changed hash values, hence difficult to incorporate.

A basic contribution of this paper would be to point out relatively certain areas of hardware manufacturing stages, where the early adoption of decentralized ledger system using blockchain technology would assist in preventing the malicious tampering of devices to look around for frequent vulnerabilities. The manuscript is a starting point for further modeling and discussion on implementing blockchain technology in the area of VLSI design fabrication process.

2. Security vulnerabilities

Manufacturing hubs in the electronics supply chain management is an area of data breaches and an uncertainty looms over each stage. The figure 1 depicts the insecurity at various stages of the chain. Assumption about the root of trust in hardware lays an unstable base due to the oligopoly environment of the chip fabrication industry. Quick patches for any resolved hackable vulnerability in a device will only deteriorate the merit of the industry, let alone the frequent upgradation in software. Recently a few researchers have been putting efforts to find a solution towards the cat mouse race of resolving issues through

frequent patches. The main zest is that at each stage various participating nodes will share the responsibility of validating the process and ensure the trust of end product with minimal governance of centralized enforcement.

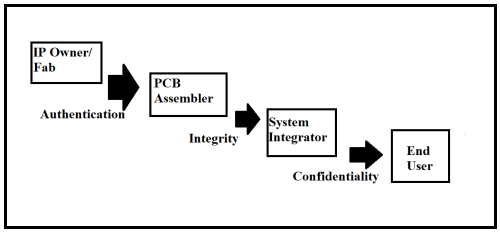

Figure 1 Electronic Supply Chain Stages

The validation of data when passed from one stage to the other will be observed by each participating nodes in a safer and private way with least interference from non-permissioned nodes to create blocks of model. A model with weak consensus mechanism can be escrowed by decent computational resources that can be rented out for creating nodes later added to a block [5]. A few many accounts have been reported in literature like the Mt. Gox cyber-attacks on cryptocurrencies [1], smart contracts vulnerabilities exploitations [2], mining hacked computers [3], etc. This displayed the weakness in forming even the core value of a system like digital assets. A certain level of testing and verification needs to be incorporated in standardizing the consensus before applying it practically.

Assumable, and tested practically to a large extent, the smart contracts have been set as a safer way to share data. Various applications are circling around using this model [7] to be a tamper proof substitute for a stable deployment post rigorous testing. Yet quite a number of findings have been reported [8] which states otherwise. Arguably a main part of data share in hardware depends on secure storage. A taxonomy of security in all abstraction layers linked to threat models, root of trust and design activities is reported [10].The microarchitecture attacks like Spectre, Meltdown and Foreshadow, opened an area of vulnerabilities to explore lacunas in the lowest layer of trusted boundary between software and hardware [9], Instruction Set Architecture. A set of hardware vulnerabilities in the physical platform through reported leakages due to faulty implementation [11] are listed in figure 2.

The confidentiality, integrity and authenticity of data in communication channels in ASIC implemented embedded processor at architectural level have advanced through decades A few of them are worth mentioning; hardware accelerated Advanced Encryption Standard (AES) crypto-engine in the ARMv8 [12], x86 [13], and Atmel [14] platforms are a few processors that leverage hardware primitives to perform operations such as Advanced Encryption Standard (AES), Rivest Shamir Adleman (RSA), and Secure Hash Algorithm (SHA) to handle command and control signals on the factory floors as well as home.

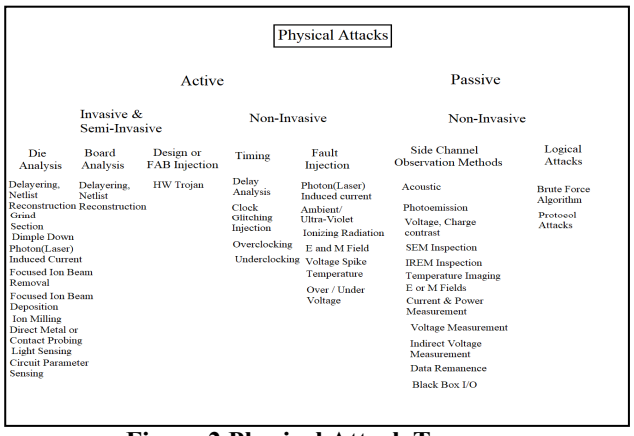

Figure 2 Physical Attack Taxonomy

The resource constrained devices are deployed for years together, many a times at places which cannot be accessed easily, so it needs cryptographic engines flexible enough to achieve high performance as well as energy efficient configurations. Counteracting attacks on systems these devices are vulnerable to is the current wave of field on which many researchers are investing, a few of which has been discussed in cf. [15]. A lot of this can be handled through auditing at the manufacture level, since the area is a vast surface to cover. Biasing is visible when there is patches easily available to software domain towards security enhancement as compared to hardwares, like smartphones and servers, debatably due to lack of skilled professionals.

Hardware professionals need to have an understanding of the basic structure of opportunities for hardware attacks like Hardware Trojans (HT) insertion, IC overbuild, reverse engineering, side-channel analysis, and IC counterfeiting [16]. Consistent with previous work, our analysis suggests bribery is a particularly troubling avenue of attack. We further suggest here that miner revenue is inherently low compared to the total value of the system and hence feasible for a Goldfinger attacker to match with relatively small bribes. It remains unclear what rate of miner revenue is required to ensure stability in practice.

3. Contribution

In the product life cycle of an IC, blockchain technology can be used at intermediate steps to make the data tamper resistant with time stamped hashes to authenticate the owners. An algorithm has been proposed to mitigate the hardware attacks relatively easier without manpower intervening in the process. As an IC Vendor, the specifications needs to be authenticated, verified with the IP owner's credentials, and not tampered with during transmission. Initially a special block, the genesis block owned by the IP owner will need to be transferred to fabrication vendor. A prior key exchange model between

the communicating parties should be standardized for authentication. The mentioned protocol will be having smart contracts to verify the merit of participating fabless chip vendors and manufacturers, as nodes. Eventually with every participating nodes, the data will be stored in blocks, briefing about the merits, with growing heights, as nonces which should be maintained by the nodes.

As the verification request arrives, the assembler sends an identity verification request to the auditor, which broadcast the request to all nodes to get their feedback. After ensuring its receipt by all nodes, the assembler will be intimated of the identity and a time stamp will be updated by all the nodes. If identity mismatch occurs, the transaction request will be failed and the merit list be denounced. The auditor will send the full-verification result to the assembler. If the chips are genuine, then the owner will be intimated and the assembling will be going on in the desired fashion.

Algorithm

Target: Verifying steps in electronics supply chain

1. If IP_Owner == verified(sign_hash_stamped)
2. Then goto PCB_Asm else verify IP-own and intimate
3. If PCB_Asm == verified(sign_hash_stamped)
4. Then Sys_Int else verify PCB_Asm and intimate
5. If Sys_Int == verified(sign_hash_stamped)
6. Then end_usr else verify Sys_Int and intimate
7. If end_usr == verify(sign_hash_stamped)
8. Then update Time_Stamp else broadcast invalid_usr
9. Update Database
10. Go to next node in merkle tree

Mutual verification can be established by each auditor, depending on the feedback from nodes for each IP owner. This information will be broadcasted upon validation by the nodes and thus updated in the database. This step will fail if any verification is not accepted by each node. Any discrepancy will be reported and traced with the ongoing timestamp. This work will result in diminishing the hardware Trojan insertion to a relatively large extent. The concept work defines a methodology to be used at each stage of verification, as depicted in figure 3.

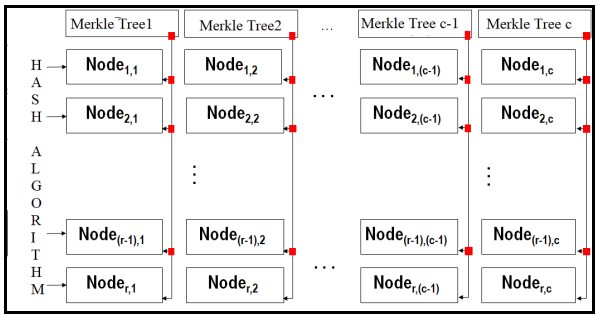

Figure 3. Timestamp and Blockchain Structure

3. Discussion

The figure 3 model depicts in its entirety a concept and a work in progress for briefing the action needed to verify the authenticity of an owner by the participating nodes in an ASIC fabrication, and integrating this merger in all sections of the VLSI design process for chip fabrication. The timestamp and blockchain structure was derived from a work on genomic sequencing [17]. In this work, nodes represent IP owners or fabless vendors who send their designs to be fabricated using third party manufacturers. With huge amount of production, the manufacturers need to maintain a database to verify credentials of the incoming designs. The hashed signatures of the IP owners will be associated with each design request, for time stamping.

The blocks will be consisting of these hashed values nodes with timestamp and height for getting an estimation of the reputation of the outsourced fabrication company which will be responsible for attesting the no overbuilding ICs. Moreover the nodes will be attested by designers who will be responsible for authorizing that the designs are tamper proof and resilient against valid hardware Trojans. The triple entry accounting will aid in maintaining database not through any intermediaries but by customers, nodes, themselves, hence no single point of centralized power and reduced uncertainty. More the participating fabless vendors as nodes, better the resilience to malicious attackers interfering in the design process. As long as there is a single honest node authenticating the block, tampering and duplicating a design will be difficult.

The cryptographic function is the hashed algorithm; for example SHA 256, depending on the application. Through this digital mechanism compressing the data into a specific format of a specific length will be suited. This value will be useful in linking all previous blocks such as any change will be detected within the chain, thus tamper proof and solves the issue of trustless intermediaries. A digital signing will be incorporated in the Merkle tree to attest the transactions of number of ICs to be produced by a manufacturer. Validity of the block can be set up by participating nodes or vendors through protocols set as standard, equivalent to consensus mechanism. Consensus as a concept is fundamental to any system where more than one entity is participating. This protocol will be an agreement with a set of rules that allows multiple machines that are connected together to work together while tolerating some machines providing incorrect data or failing completely.

A robust proof of our concept is yet to be idealized, but a beginning in this direction has already been initialized by cf. [6]. With the concept in the working direction of the paper about how cryptographically secure hardware obfuscation can be achieved, this work has been theorized and a practical set up is on its inception. The numerous hardware security features needs to be considered for

making a robust claim in the fabrication process, which this work is trying to emphasize. An appropriate communication needs to be emphasized for an error free one to one dialogue between nodes. Various application areas considering a part of this work can be configured for testing and analyzing the energy consumption in a system.

4. Conclusion

This paper work contributes in its entirety a proof of concept towards counterfeiting the various hardware attacks in the fabrication industry with a brief discussion in the ongoing research on blockchain as a decentralized facility and its applicability in improving the hardware security root of trust. A detailed work is yet to be produced as it includes a thorough look up at various layers of stages. Even if this technology is in its infancy, yet the mutual distrust of individuals with banks, governments and oligopoly corporations will be mitigated to a relatively superior extent by its adoption, not only in the financial sector, but also in different areas. A vital part of merging blockchain and fabrication methods is the energy consumption required which is significant.

5. References

[1] R. McMilan, "The inside story of Mt.Gox, Bitcoin's $460 million disaster, 2014," [Online]. Available: https://www.wired.com/2014/03/bitcoin-exchange/. [Accessed 2 9 2019].

[2] D. Siegel, "Understanding the DAO attack, 2016," [Online]. Available: https://www.coindesk.com/understanding-dao-hack-journalists/. [Accessed 2 9 2019].

[3] A. Mak, "How scammers steal your computing power to mine cryptocurrencies," 2018. [Online]. Available: https://slate.com/technology/2018/02/what-is-cryptojacking-thebitcoin-and-monero-mining-process-that-steals-your-computing-powerexplained.html. [Accessed 2 9 2019].

[4] Haber, S. & Stornetta, W.S. J. Cryptology (1991) 3: 99. https://doi.org/10.1007/BF00196791.

[5] Bonneau J. (2019) Hostile Blockchain Takeovers (Short Paper). In: *Zohar A. et al. (eds) Financial Cryptography and Data Security. FC 2018*. Lecture Notes in Computer Science, vol 10958. Springer, Berlin, Heidelberg

[6] Ganji, Fatemeh & Tajik, Shahin & Seifert, Jean-Pierre & Forte, Domenic. (2019). Blockchain-enabled Cryptographically-secure Hardware Obfuscation. 10.13140/RG.2.2.26673.33123.

[7] N. Kolokotronis, K. Limniotis, S. Shiaeles and R. Griffiths, "Secured by Blockchain: Safeguarding Internet of Things Devices," in *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 28-34, May 2019. doi: 10.1109/MCE.2019.2892221

[8] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen, A survey on the security of blockchain systems, *Future Generation Computer Systems, 2017*, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.08.020.

[9] C. Canella, J. V. Bulck, M. Schwarz, M. Lipp, B. von Berg, P. Ortner, F. Piessens, D. Evtyushkin, and D. Gruss, "A systematic evaluation of transient execution attacks and defenses," *CoRR*, vol. abs/1811.05441, 2018. [Online]. Available: http://arxiv.org/abs/1811.05441

[10] Ingrid Verbauwhede, "Hardware Security Knowledge Area", *The National Cyber Security Centre* 2019.

[11] M. Tehranipoor, S. Brown and S. Aftabjahani, "The Vulnerability Database," 2018. [Online]. Available: http://www.trust-hub.org/vulnerability-db/physical-vulnerabilities

[12] Armv8, "*ARMv8 technology Review*," 2016. [Online]. Available: https://bit.ly/2KzT7WW.

[13] Intel, "Intel advanced encryption standard instructions (aes-ni)," 2016. [Online]. Available: https://intel.ly/2UtXdEy.

[14] AVR, "Avr1318: Using the xmega built-in aes accelerator," 2016. [Online]. Available: https://bit.ly/2UHPxhf.

[15] S. Moein, T. A. Gulliver, F. Gebali and A. Alkandari, "Hardware attack mitigation technique analysis," *International Journal on Cryptography and Information Security (IJCIS)*, pp. Vol. 7, No. 1, pg 9 - 28, March 2017

[16] M. Tehranipoor, "A survey of hardware trojan taxonomy," *IEEE design & test of computers*, pp. 27(1):10-25, 2010

[17] Ram Prasad Mohanty, Hasindu Gamaarachchi, Andrew Lambert, and Sri Parameswaran. 2019. SWARAM: Portable Energy and Cost Efficient Embedded System for Genomic Processing. ACM Trans. Embed. Comput. Syst. 18, 5s, Article 61 (October 2019), 24 pages. DOI: https://doi.org/10.1145/3358211