EasyChair Preprint

№ 10627

Towards Security Issues in State-of-the-Art Signal Transmission

Debasis Gountia, Bijay Srinibas Nag, Swarnalata Pati, Manjit Kumar Nayak, Subrat Kumar Acharya, Neelamani Samal, Amitav Mahapatra and Rakesh Ranjan Behera

July 27, 2023

Towards Security Issues in State-of-the-Art Signal Transmission

Debasis Gountia
Department of Computer Sc. & Application, Odisha University of Technology & Research (OUTR), Bhubaneswar
Email: dgountia@cet.edu.in

Bijay Srinibas Nag, Research Scholar
Department of Computer Sc. & Engineering, OUTR, Bhubaneswar, India.
E-mail: bijaynag@gmail.com

Swarnalata Pati, Assistant Professor,
Department of Computer Sc. & Application, OUTR, Bhubaneswar, Odisha, India.
E-mail: spati@cet.edu.in

Manjit Kumar Nayak, Asst. Professor,
Department of Computer Sc. & Application, OUTR, Bhubaneswar,
E-mail: manjitcsa@cet.edu.in

Subrat Kumar Acharya
Head - Bhuvan Systems & Networks,
ISRO Hyderabad, India.
E-mail: subrat001@gmail.com

Neelamani Samal
Research Scholar, Department of Computer Sc. & Engineering, SOA, Bhubaneswar, India
E-mail: neelamani.samal@gmail.com

Amitav Mahapatra,
Faculty in CSA Dept,
OUTR, Bhubaneswar,
E-mail: amitavmahapatracse@cet.edu.in

Rakesh Ranjan Behera,
TCS Bhubaneshwar
rakesh006ranjan@gmail.com

Abstract— **Signals are generated when data or command is communicated to a device. It is having a tremendous implementation in both electronic and electrical components, but it normally refers to both digital and analog communication technologies and the devices. Each individual signal carries some important information in a form that may be confidential. The information is embedded into the signal using analog modulation techniques or digital modulation techniques, depending on the source device and/or medium device and destination device. Many technologies have been developed in recent years for storing and sharing valuable information regarding a signal. This paper pertains to security challenges with potential defenses in the signal transmission for more honorable and reliable in-state-of-the-art communication technology.**

Keywords— Hardware Trojan, Locking, Obfuscation, Signal, Side-channel fingerprinting, Trigger

Abbreviations – MITM: man-in-the-middle; IP: intellectual property; RE: Reverse engineering; HT: Hardware Trojan; DoS: Denial of Service.

I. INTRODUCTION

In the field of communication system, electrical engineering and signal processing, a signal may be an electrical or electromagnetic current that is being used for carrying data regarding the behavior or attributes of some phenomenon from one device or network to another network [1]. In its frequent general usage, in electronics and telecommunication engineering, signal is a time varying voltage, current or electromagnetic wave that can be used to communicate information [15, 16]. The IEEE Transactions on Signal Processing states that the term "signal" refers to speech, video, audio, image, transmission, geophysical, sonar, radar, medical and musical signals [6, 7]. In the physical real world, any quantity revealing variation in time or variation in space (such as an image) is potentially a signal which might convey a message between observers, among other possibilities, or provide information on the status of a physical system. Signaling also occurs in organisms to the cellular level, with cell signaling. In evolutionary biology, signaling theory proposes that a remarkable driver for flowering is the capability for animals to broadcast with one other by developing multiple ways of signaling. From the human engineering point of view, signals are generally provided by a sensor, and most of the time the originative of a signal is converted to different form of energy using a transducer. For example, an acoustic signal is converted to a voltage waveform by the microphone, and a speaker does the reverse process [9].

Signal is the main component behind virtually all: transmissions, electronic devices, and networking [11]. Signals can be either digital or analog. A signal is generally characterized by its amplitude, frequency, and phase. The information in a signal is generally go along by noise. In general, the term noise indicates an unsuitable random disturbance, but is commonly extended to include undesired signals conflicting with aspiring to signal (like crosstalk). The signal integrity part covers the noise prevention [8].

Engineering disciplines like the electrical engineering has pilot the way in the study, design, and implementation of systems involving storage, manipulation and transmission, of signal information [10]. In the last part of 20th century, electrical engineering has itself classified into many disciplines, study intensively in the analysis and design of systems that manipulate physical signals; computer engineering and electronic engineering as examples; while the design engineering has been developed for dealing with the functional design of user machine interfaces.

As the signal carries important information [12], may be confidential data regarding any scientific, military, or personal usage, malicious people tries to attack on the transmission system becomes a serious threat to such system. Therefore, it is quite important to do research on the security issues of signal transmission.

The remaining contents of the article is arranged as follows. Part II presents various effective attacks related to signal transmission. Hardware Trojan is elaborated in Section III along with their potential defenses in Section IV. Comparisons and results analysis are presented in Section

V. Finally, conclusion and future scope are drawn in Section VI and Section VII, respectively.

II. VARIOUS SECURITY ISSUES IN SIGNAL TRANSMISSION

Though signal transmitted through antenna, radar, and satellite transmission system successfully marked a remarkable position in today communication world, there are some security aspects in transmission [13] which need attention for consideration.

1) **Man-in-the-middle-attacks:** In the field of computer security, a man-in-the-middle (MITM) assault occurs when an attacker, i.e., an unscrupulous person, secretly relays and modifies the signal communicated between two parties who believe these are directly transmitting without interference [1]. For example, active eavesdropping, in which an attacker establishes a separate connection between relays signal and victims in order to instil trust that they are transmitting directly to each other over a private network [18], when in fact the entire transmission is under the control of malicious people, as shown in **Figure 1**. These attackers intercept all relevant transmissions passing between their victims and either throw new malicious transmissions or modify the previously mentioned transmission signals.

2) **Single bit flipping attacks**: This kind of attack is based on the substitution principle or replacement principle [2]. In single bit flipping attack, at the end of receiver, one transmitted bit is changed, causing a fatal error.

3) **Sequence attacks**: This type of attack is also working on the principle of substitution or substitution. In such attack, n-bit in transmission can either be inserted, deleted, or modified by unscrupulous people. An intelligent adversary could normally manipulate the proceeds of the transmission process.

4) **Complete substitution-attacks:** This type of attack is also based on the replace/replace principle. Such attacks are the attacks in which the intended transmission is completely replacement of an alternate for a malicious target [19, 17]. These attacks are the most dangerous adversary in the transmission world.

5) **Attacks on the control software:** Pernicious representative can alter the mistake recuperation programming in straightforwardness to sidestep the blunder recuperation instrument. This is feasible for both satellite and radar streams of signs.

6) **Information leakage:** An unscrupulous people may unauthorized disclose the privileged information involving in the transmission. Such examples consider privileged information about research data, secret password, defense data, or proprietary protocol, etc.

7) **Piracy attacks:** For different transmission methods, there are different protocols. They are referred to as transmission Intellectual Property (IP). Unscrupulous attackers can take advantage of these IP addresses by duplicating prior broadcasts and re-transmitting them frequently. Piracy of a transmission is a significant unique aspect of proprietary satellite/radar that necessitates a great deal of effort and billions of dollars. Their piracy, however, is not guaranteed to be secure against attackers. As a result, traditional systems are vulnerable to the IP thief danger since an attacker may readily extract test transmission protocols.

8) **Modification of functionality:** Maliciously staff can pressurize to pursue an unintended operation in radar or satellite. For example, an employee can subtly lower the performance and reliability services of a transport function. As a result, it reduces end-customer trust and confidence in radar/satellite.

9) **Brute-force attacks on the transmission**: Unscrupulous users can do their best to crack secret transfer passwords (if any) using any combination of alphanumeric characters and special characters. These are known as Brute-force attacks. The higher security aspects of guarantee are attainable by hardening the protection to brute-force attacks with high diffusion and confusion.

10) **Counterfeiting:** Counterfeiting transmissions are those which are repeated the previous transmissions over and over in order to create disturbance in the whole system. Therefore, counterfeits are of threats to radar/satellite like other aforementioned attacks.

11) **Reverse-engineering:** Reverse engineering (RE) is the process to analyze models, discovering their components and internal structures, connections, etc., and generating a top-level representation of the model in a different form or abstraction [3]. RE is used many times to decompose a model into various suggestions such as duplication, duplication, duplication, and so on. This subsection captures the RE of a transmission system obtained by extracting the internal physical structure and information using destructive confidential information sniffing technology by a foreign malicious attacker.

12) **Hardware Trojans:** Hardware Trojans (HTs) can alter deadly the embedded circuit system of transmission channel of signal or maliciously insert a circuitry into the channel design to destroy entire transmission system for a specific given input and/or time. These HTs can change the designed transmission circuit during either fabrication or design and result unintended behavior. They create denial of service, disclosure of confidential signal information, and changes in system functionality. An attacker can insert HT at any level, from general system design specifications to the transistor level of the IC design flow [4].

Figure 2 depicts the various sorts of growing vulnerabilities, threats, and assaults against signal

transmission. The majority of the challenges and solutions presented in this research study are natural in nature; we extend these problem statements to our best knowledge of how the current transmission system operates and extrapolate from the existing security techniques.

Nonetheless, our thoughts explained in this article are not expected to substitute any current works. All things being equal, these equipment based countermeasures can be utilized to reinforce transmission framework security or give better confirmation of safety that would some way or another be not feasible to the transmission world.

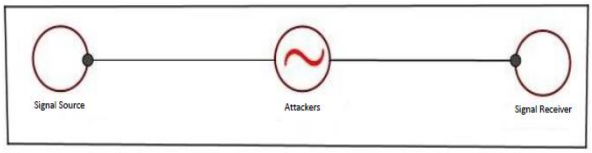

Figure 1: Scenario of Man-in-the-Middle-attacks.

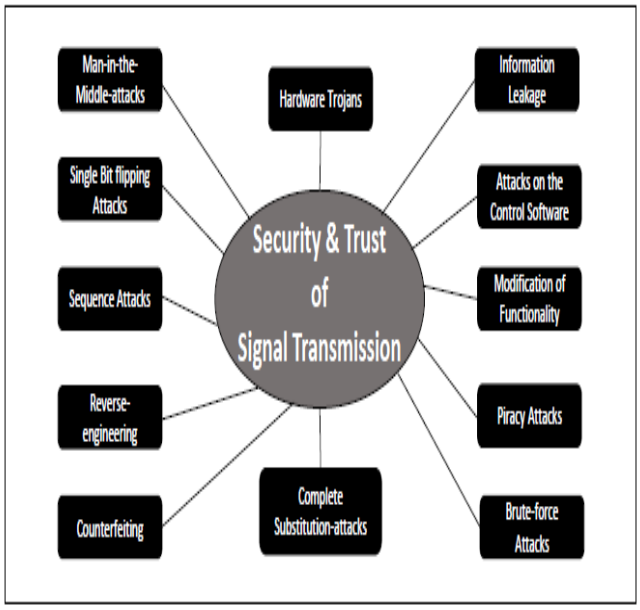

Figure 2: Security and trust of signal transmission consisting of a diverse array of vulnerabilities, threats, and attacks.

III. DESCRIPTION OF HARDWARE TROJANS

A typical structure of malevolent hardware Trojans which could be maliciously inserted into signal transmission channel is presented in **Figure 3**. Some important key terms linked to hardware Trojans and their normal meanings are:

- **Trigger:** a malevolent event that initiates the activities of Trojan. When this deterministic event starts, the HT system circuit is auto-activated for deadly functionality
- **Payload:** a malevolent event that activates the Trojan, which is responsible for implementing HT effects, and thus degrades the reliability and trustworthiness of the signal transmission channel system, resulting in serious deadly incidents such as secret information leakage, Denial of Service (DoS), and thus degrades the reliability and trustworthiness of the signal transmission channel system.

Trojans may maliciously be inserted into signal transmission system as per the following categories:

- Insertion phase: Signal transmission channel HTs can be embedded in any of the accompanying stages.
  1) Specification: The signal transmission channel Trojans can maliciously alter the specification(s), e.g., frequency during run-time to incorrect the signal.

  2) Design: Signal transmission channel designer can modify the system to change the signal result.

  3) Assembly: During the components assembly of channel, an Integration malevolent engineer wrongly arranges components to generate erroneous signal outcome.

  4) Fabrication: A HT may be inserted into the transmission channel during its fabrication by tampering in the foundry.

  5) Calibration and testing: A wicked channel Tester may also insert malevolent Trojans during testing and calibration phase to overcome the testing standard of signal to be communicated to the receiver.

  6) In-field: In the signal transmission channel field, attackers falsify the transmission protocol by altering the agreements among different involved parties in the transmission.

- Abstraction level: HTs may embed at the following phases of abstraction level of transmission channel:
  1) Physical level: Each physical component of signal transmission channel, e.g., hardware connection wiring and other components, chip platform and their locations and dimensions are expressed at physical level. HTs may be added by modifying any of above physical components and/or their specified accurate dimensions.
  2) System level: System engineer mentions different elements of individual domain and their inter connections at system level. Signal transmission channel can be altered with to produce erroneous outcome in its transmission.

- Activation mechanism: Such mechanism elaborates both the external and internal triggering mechanisms of Trojan that may be inserted into the channel.

  1) External trigger: Such trigger is externally executed for the outcome of a specific operation.

  2) Internal trigger: Such a trigger is run internally for a specific instance of the time slot.

- Effect: The effects of hardware Trojans are to alter channel functionality, disclose secret signal information, cause DoS attacks, result degradation in performance, defecate reliability, trustworthiness, and so on.

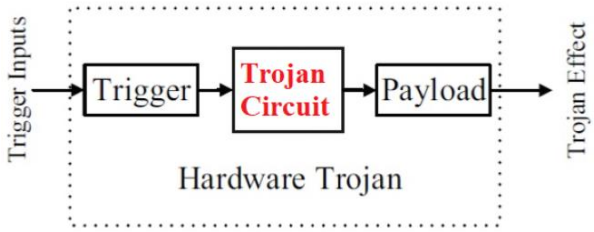

Figure 3: A typical structure of malevolent hardware Trojan.

IV. DESCRIPTION POTENTIAL DEFENSES AGAINST SECURITY THREATS ON SIGNAL TRANSMISSION SYSTEM

Potential defense mechanisms which guarantee the security and trust against different attacks like man-in-the-middle attacks, hardware Trojans, etc., assume the following preventive schemes:

- **Watermarking:** In this technique, the original sender's digital signature is embedded with the signal. Watermark can articulate a potent approach to assure ownership as this technique is much difficult to identify and modify. Unfortunately, watermarking technique cannot guarantee to provide security prospect against hardware Trojans.

- **Metering:** In metering, both the public signature of sender and the receiver's digital signature are inserted to the communicated signal as processing constraints. This metering scheme cannot also assure protection against Trojans as the malicious people is able to create and hide a malevolent Trojan in the transmitted circuit due to the availability of the design functionality.

- **Code analysis:** Code of signal transmission is examined thoroughly to analysis for the detection of any Trojans embedded into the channel. Any effective secured encryption scheme and hash functions may be used for the confidentiality of signal and hence prevent from hardware Trojan attacks on system. Code analysis is not able to protect the signal transmission channel against piracy, counterfeiting, and reverse-engineering attacks.

- **Locking:** A signal sender may insert locks (i.e., digital multiplexers) which manage and control the flow of signal among different parties of signal transmission system. If MITM attack happens, then attacker cannot proceed to get the original signal further in a correct manner if the correct secret key is not applied. This secret key should be safeguarded in a carefully designed memory to shield from weaknesses as this key is eradicated during figuring out time. Hardware Trojans may not be able to embed as the signal transmission channel functionality is hidden by aforementioned key. Locking can forestall assaults like theft, picking apart, and falsifying assaults, Trojans after manufacture, aside from Trojans embedded during chip creation of sign transmission direct in the business.

- **Obfuscation:** Code-obfuscation approach may be used by the signal sender for the mystification of transmission. Such obfuscation can indirectly prevent HT attacks as unscrupulous won't be able to embed the stealthy and meaningful HTs in such an obfuscated signal sequences. Obfuscation prevents Trojans and reverse-engineering, but unfortunately neither piracy nor counterfeiting.

- **Side-channel fingerprinting:** Such methodology can recognize equipment Trojans effectively as the made parametric qualities, like power, region, postponement, and part attributes of the transmission are contrasted and those of measurable (conventional) model. A hardware Trojan is defined as any major deviation or alteration. Side-channel fingerprinting alone may not be enough to protect against piracy, reverse engineering, and counterfeiting.

- **Reverse Engineering (RE):** This plan can likewise productive be used to identify hardware Trojans. For RE, signal transmission channel should aware by research fellows to get successful in the detection of HTs inserted by malevolent foreign attackers. A regular RE stream should go through de-bundling, delayering, and picture handling of a sign transmission channel. Mainly, its design and components are disclosed by this technique following the above steps is compared with a golden one (that is, where no attacks). Such RE scheme is both time-consuming and also destructive in nature. Hence, RE approach is less applicable for Trojans detection [5]. RE is commonly used to assure a Trojan-free signal transmission applied in the golden signal transmission channel development needed for test time and run-time golden signal transmission channel models.

V. COMPARISONS AND RESULTS ANALYSIS

Table 1 sums up every one of the expected guards alongside the measurement of examinations among safeguards. For security trust and reliability in signal transmission channels, this Table confirms that the 'Locking' defence provides the best assurance, followed by the obfuscation defence.

Depending upon their budget and business strategy, industry firms and companies can select any one or multiple aforementioned defense mechanisms to secure the signal transmission from different known, existing, also unknown

vulnerabilities, threats, and attacks [14]. As each of the aforementioned techniques has its own merits and demerits, one suggested solution is to apply each for the highest Trojans coverage. One suited example, Reverse Engineering-based approach assures the golden signal transmission channel needed for run-time and test time golden signal transmission models. Side-channel and functional testing schemes can detect large and small Trojans, respectively, which were embedded during chip fabrication. Run-time technique finally concludes the work as a last scheme of defense mechanism.

Symbols used in **Table 1** indicates:

- Yes indicates both detection and prevention are possible.
- Yes* shows both distinguish and forestall those Trojans embedded solely after manufacture, however not those before creation.
- No indicates both detection and prevention are impossible.
- No* indicates only detection, but no prevention.

Table 1: Summary of potential defenses

Defense Mechanism	Name of Attack			
	Hardware Trojans	Authenticity /Piracy	Reverse-engineering	Counter-feiting
Watermarking	No	No*	Yes	No*
Metering	No	No*	Yes	No*
Code analysis	No*	No	No	No
Locking	Yes*	Yes	Yes	Yes
Obfuscation	Yes	No	Yes	No
Side-channel fingerprinting	No*	No	No	No
Reverse Engineering	Yes	No	-	No

VI. CONCLUSION

In this article, we have performed a study on various possibility known attacks on signal transmission. This article has proposed different defense techniques for handling such attacks with relative comparisons among them for a better sustainable world.

VII. FUTURE WORK

Future work is to formulate hardware- and cyber physical-enabled protections against attacks like [20] on signal transmission with error handling mechanism like [18].

REFERENCES

1. M. Conti, N. Dragoni, and V. Lesyk (2016). A Survey of Man-in-the-Middle attacks. IEEE Communications Surveys Tutorials, 18(3): 2027-2051.
2. J. Tang, M. Ibrahim, K. Chakrabarty, R. Karri (2018). Secure randomized checkpointing for digital microfluidic biochips. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 37(6): 1119-1132.
3. S. E. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, and M. Tehranipoor (2016). A Survey on Chip to System Reverse Engineering. ACM Journal on Emerging Technologies in Computing Systems (JETC).13(1): 6:1-6:34.
4. N. Jacob, D. Merli, J. Heyszl, and G. Sigl, (2014). Hardware Trojans: Current Challenges and Approaches. IET Computers Digital Techniques (CDT). 8(6): 264-273.
5. C. Bao, D. Forte, and A. Srivastava (2014). On Application of One-class SVM to Reverse Engineering-based Hardware Trojan Detection. IEEE International Symposium on Quality Electronic Design (ISQED), pp. 47-54.
6. Aims and Scope. IEEE Transactions on Signal Processing. IEEE. Archived from the original on 2012-04-17.
7. Signal. [Online]. Available: https://www.techopedia.com/definition/14154/signalelectronics
8. R. Priemer (1991). Introductory Signal Processing. World Scientific. p. 1. ISBN 978-9971509194. Archived from the original on 2013-06-02.
9. P. Chakravorty (2018). What Is a Signal? [Lecture Notes].IEEE Signal Processing Magazine. 35(5): 175-177. https://doi.org/10.1109/MSP.2018.2832195
10. T. H. Wilmshurst (1990). Signal Recovery from Noise in Electronic Instrumentation (Second Edition). CRC Press. pp. 11 ff. ISBN 978-0750300582. Archived from the original on 2015-03-19.
11. Digital Signals. www.standrews.ac.uk. Archived from the original on 2017-03-02. Retrieved 2017-12-17.
12. Analog vs. Digital - learn.sparkfun.com. learn.sparkfun.com. Archived from the original on 2017-07-05. Retrieved 2017-12-17.
13. Proakis, J. G.; Manolakis, D. G. (2007-01-01). Digital Signal Processing. Pearson Prentice Hall. ISBN 9780131873742. Archived from the original on 2016-05-20.
14. M. J. Roberts (2011). Signals and Systems: Analysis Using Transform Methods & MATLAB. New York: McGraw Hill. ISBN 978-0073380681.
15. Signal. [Online]. Available: https://en.wikipedia.org/wiki/Signal
16. M. H. Hayes. (1999) Digital Signal Processing. McGraw-Hill Publisher.
17. J. G. Proakis, D. K Manolakis (2006). Digital Signal Processing. 4th Edition. Prentice Hall Publisher.
18. D. Gountia, S. Roy. "Design-for-Trust Techniques for Digital Microfluidic Biochip Layout with Error Control

Mechanism", IEEE/ACM Transactions on Computational Biology and Bioinformatics, vol. PP, no. XX, 2022.
19. D. Gountia, R. Champati, A. K. Pradhan, and B. Mohanta. "Towards Security Aspects of Secret Key Transmission", International Conference on Information Technology (ICIT), pp. 57-60, 2018
20. Debasis Gountia and S. Roy, "Security Model for Protecting Intellectual Property of State-of-the-Art Microfluidic Biochips", Elsevier Journal of Information Security and Applications (JISA), vol. 58, pp. 1-15, 2021.