American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-9, Issue-3, pp-181-185
www.ajer.org
Research Paper Open Access

Hardware Based Internet-of-Things Security Architecture For Communication Between Machines

Daniel Ekpah[1], Kamalu .A. Ugochukwu[2], Prince .O. Asagba[3],
Department of Electrical & Electronic Engineering University of Port Harcourt, Nigeri.

***ABSTRACT**: This paper examined the Field Programmable Gateway Array (FPGA), a major hardware security device with minimal security features using Technical, design and Simulation methods to uncover veiled viruses and prove the absence of susceptibilities in hardware communication devices. The firmware was developed using Very High Speed Integrated Circuit (VHSIC) Description Language as blueprint for the chip to analyse possible threats emanating from the dynamic partial reconfiguration capabilities of the FPGAs at IoT terminals, and providd solution techniques based on Physically Unclonable Function (PUF) circuits to prevent threats such as side-channel attack based on square and multiple algorithm exponentiation. The new design protocol-stack was certified using the open group architectural framework and open web application security project to ascertain its reliability. Experimentally, we benchmarked the execution of two comparable trials making 2000 Http requests distributed in 20 threads, with 1000 requests per thread; this yielded throughput degradation close to zero after using up to 50 of our new firmware rules. The firmware architecture showed high throughput capabilities with a minimal packet loss of twenty-six percent as against the default firmware with packet loss of 32 percent.*

***Keywords:**Internet-of-Things,Machine-to-MachineCommunication, Field Prorammeable gateway array, Physical Unclonable Function, Authentication, Security*

Date of Submission: 25-02-2020 Date of acceptance: 08-03-2020

I. INTRODUCTION

The Internet of Things (IoT) is all over us and expeditiouslyincreasing. We are starting to understand the advantages of the IoT. Better approaches to utilize associated things are being grown every day[1]. The IoT innovation gives outstanding chances to interconnect individuals just as device-to-device correspondence, arranged sensors and systems enable everything to communicate with one another to share information and enable us to have a mechanical driven society where precise information is promptly accessible to settle on educated and important choice. This upset depends on a steady advancement of the Internet, innovations and programming, correspondence conventions, implanted sensors, brilliant physical items ready to gather information continuously. It is the future Internet, it will drastically change our method for living as the Internet impacts on instruction, wellbeing, homes, correspondences, transportation, urban communities, business, science, government and men when all is said in done ('third Generation Partnership Project", 2012).

In any case, a few issues are undermining the IoT advancement, similar to the protection and security in this innovation, the change from IPv4 to IPv6, having a typical arrangement of models and dealing with the huge measure of information that will be put away, got to, and broke down. One of the serious issues confronting the Internet of things is the issue of security. Coordinating security into the framework ought not be left till after the arrangement of the framework; it ought to be consolidated during the underlying arrangement of the framework. In the IoT, in light of the fact that data is transmitted over the system in type of double information, existing programming encryption calculations can extraordinarily upgrade the insurance and confirmation of directions gave to remote IoT gadgets over the system[3]. This will help forestall unapproved access to the IoT gadgets and wipe out the plausibility of an interloper seizing the IoT empowered gadgets. This procedure lessens the weight on having an absolutely secure system, which is practically unimaginable. It likewise assists spare with costing of usage by utilizing a promptly accessible channel (the web), which in spite of the fact that not verify, can wind up transmitting information safely. Various kinds of machines or gadgets can address one another or to some outer server by means of some correspondence arrange with no human intervention. The correspondence organize utilized can be either fixed wired, remote or cell. The benefits of

utilizing a cell arrange for M2M correspondence incorporates all-round inclusion, developed security highlights, dependable conveyance and so on. M2M correspondence has totally different highlights contrasted with standard H2H communication. A portion of the remarkable highlights of M2M incorporates enormous number of gadgets, little and inconsistent information transmission, low controlled and modest gadgets, low/confined portability and so on.(third Generation Partnership Project", 2012).

II. HARDWARE LEVEL SECURITY ISSUES

The security issues in IoT are not limited to data authentication, access control, client privacy, and other attacks like data leakage. Hardware level insecurity is also grabbing the attention of authors nowadays and it is becoming a growing problem day by day. To get a complete hardware secured IoT system, we need to secure the ICs (better to say NoCs [Network on Chip] or SoCs [System on Chip]) in the IoT enabled devices first. With tremendous growth in integration density with the ever increasing logical complexity of today's nano-scale electronic systems design and fabrication of VLSI chips have become a completely distributed system. Due to very high cost of fabrication process the IC (integrated circuit) designer companies need to depend on other vendors. This brings us to a comparatively insecure environment to design the IC's. Use of third party Intellectual Property (IP) core [7] and other design tools (CAD tools) make the situation more complicated. Because a single malicious circuit can be injected at any stage of the design process invisible to the designers at that time. Threats can also be injected during the running of a chip after successful fabrication. In first case that particular threats can run and force the IC to malfunction after the chip is fabricated and started working. As a result confidential information can be leaked or important instructions can malfunction. Hardware Trojan is one of them. In the next section we have discussed hardware Trojan in details. Figure 1 presented the different possible attacks.

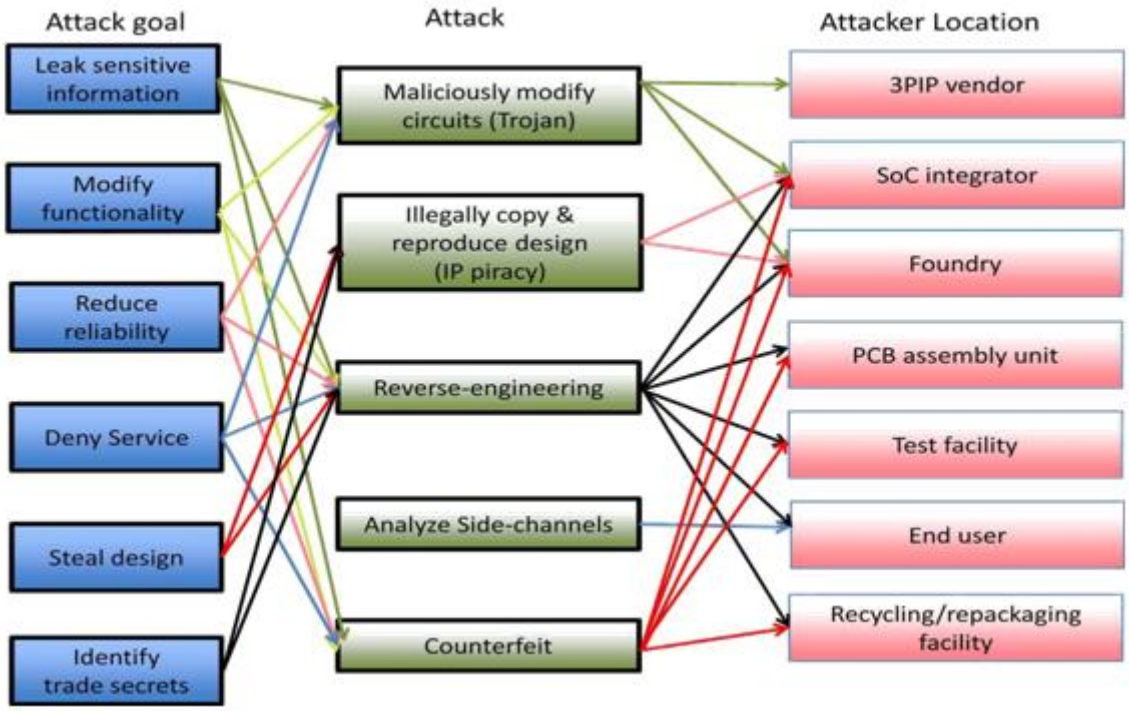

Figure 1: Systematization of hardware security around the attack method

III. OUR APPROACH

The approached taken in this work to bring about the needed improvement in IoT security, is the integration of a new firmware to the Linux-Ubuntu Operating kernel embedded in Raspberry PI 4 defense mechanism to mitigate against IP cloning and Directory traversal Vulnerability, capable of exposing the communication path-flow of IoT devices during exchange of data between M2M. Figure 1 described the block diagram of the IoT security architecture approach taken in this work while Fig 3.5 further revealed the communication components involved in the transfer of bits challenge in the Physical Unclonable Function a key circuit in modern day communication hardware security.In our approach, we further provided more insight on the analysis methods and technical design background of the work in the subsequent sections of this work.The concept of having an integrated circuit generate its own unique digital signature has broad application in areas such as embedded systems security, and IP counter-piracy. Physically unclonable functions (PUFs) are circuits that compute a unique signature for a given IC based on the process variations inherent in the IC manufacturing process. This work presents the PUF design specifically targeted for field-programmable gate arrays (FPGAs). Our design makes use of the underlying FPGA architecture, and unlike prior published PUFs, the proposed PUF can be naturally embedded into a design's VHDL, consuming very little area, and does not require the use of "hard macros" with fixed routing. Measured results on the Xilinx Virtex-5 65 nm FPGA demonstrate PUF signatures to be both unique and reliable under temperature variation. Figure 2 provided an architecturial view of our design.

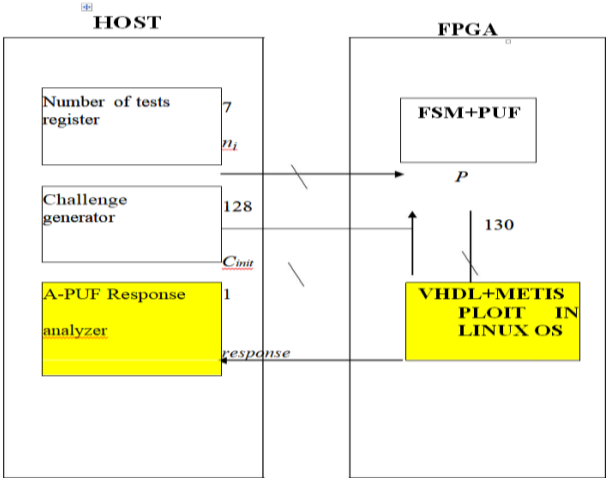

Figure 2: Hardware Security Architecture

IV. PROTOCOL DESIGN

Protocol Design linking a safe communication between a device and a host processor requires a safe convention. Confirmation and key foundation are the two key parts that were accomplished by the cryptographic convention structured. Confirmation is required for guaranteeing that the character of an IoT device that is attempting to convey to the host processor is genuine. This we accomplished by utilizing PUF innovation and also through experimental evidence. We established that noxious devices can't be totally discounted, on the grounds that even a confirmed device can be malevolent, a device that was hacked. As one of the prerequisites, the PUF equipment security primitive was utilized as the foundation of-trust, which gives confirmation of the silicon. Moreover, to keep the information transmission secret and available just by approved gatherings, it is essential that the correspondence is scrambled. To accomplish this, symmetric cryptography can be utilized. In any case, as we probably aware at this point, symmetric cryptography necessitates that a duplicate of a similar key is accessible on the two finishes of the communication channel, which can be accomplished by a key-established protocol. In whatever is left of the segment, we demonstrate the means in determining a convention that sets up a safe shared key between the IoT gadgets and the host processor, and validates gadget's silicon utilizing PUF, thusly building up a safe communication.We evaluated the performance of the two protocols on two die rent hardware platforms - Altera DE2-115 and TI MSP430. The Altera FPGA implementation is based on a NIOS II soft-core whereas the TI MSP430 implementation uses the MSP430F5438A processor. The Altra DE2-115 combines a large number of logic and I/O devices and can be used for a wide variety of applications. The logic devices on the board include an FPGA, SDRAM, SRAM and Flash. The I/O devices include an LCD display, LEDs, switches, RS-232 interface as well as connections to other devices.The Hardware Architecture of our prototype design integrates the Nios-II softcore processor with SRAM, SDRAM, UART and several FPGA components(RO PUF, SRAM controller and SDRAM controller).The hardware components in our design are connected using the Avalon Memory Mapped Interface which is an address based interface with master-slave

connections. The Nios-II processor controls the signals of the data slave components (SRAM Controller, RO-PUF, SDRAM Controller, JTAG) and of instruction slave components (SDRAM Controller). The PUF data was collected by the software using Memory Mapped Registers. The hardware collects the input arguments to the PUF from these registers and the output is placed back into the memory registers corresponding to the PUF. We demonstrate the Fusion PUF as a combination of the SRAM PUF and Ring-Oscillator PUF(RO-PUF).SRAM PUF Design: The SRAM PUF is based on the preferred power-up state of transistor cells in an SRAM. Our implementation uses the SRAM on the Altera DE2-115 board (ISSIIS61WV102416BLL) and an FSM controller. The SRAM controller was interfaced to the SoC as a slave, and it handles communication between the Nios-II processor and the 1024k x 16 bit CMOS SRAM chip. The controller receives the address of a memory location in SRAM, reads the start-up value at that address location and transmits the values to the processor through the Avalon Fabric. RO-PUF Design: The RO-PUF exploits delay variations in the logic elements to produce a unique n-bit identifier. The design works by chaining an odd number of inverters and connecting the output of the last inverter to the input of the rst inverter. This way, each RO produces an oscillating output with a frequency dependent on how quickly the looping signal propagates through the logic elements. The output (frequency) of an RO (A) was compared to the output of another RO (B), and either a 1 or a 0 is produced depending on whether A or B has a faster frequency. In our design, we used 256 ROs to generate a 255 bit PUF output. To read stabilized RO frequencies, the system waits for 100 ms before starting the measurement. Then, it starts counting the
oscillations for 250 ms. We used the same Hardware Architecture to demonstrate the operation of both the protocols. Table 1 shows the various outcomes after simulation.

V. RESULTS

Table 1: New Firmware to mitigate CVE-2018-17173 vulnerability.

NFW	assembler values			Bytecodes
(10.00) ldh	[12]			22
(10.01) jeq	#0x800	jt 2	jf 21	40 0 0 18#
(10.02) ldh	[16]			21 0 19 2048#
(10.03) jgt	#0x8a	jt 4	jf 21	40 0 0 6#
(10.04) ldb	[23]			37 0 17 138#
(10.05) jeq	#0x6	jt 6	jf 21	48 0 0 23#
(10.06) jeq	#0x6	jt 7	jf 21	21 0 15 6#
(10.07) ldh	[20]			21 0 14 6#
(10.08) jset	#0x1fff	jt 21	jf 9	40 0 0 20#
(10.09) ldxb	4 ([14]&0xf)			69 12 0 81#91
(10.10) ldh	[x + 16]			177 0 0 1#
(10.11) jeq	#0x2378	jt 12	jf 21	72 0 0 16#
(10.12) ldb	[x + 46]			21 0 9 9080#
(10.13) jeq	#0x47	jt 14	jf 21	80 0 0 46#
(10.14) ld	[x + 91]			21 0 7 71#
(10.15) jeq	#0x3d253237	jt 16	f 21	64 0 0 91#
(10.16) ld	[x + 95]			21 0 1025847863#
(10.17) jeq	#0x25323 2d	jt 18	jf 21	64 0 0 95#

Iptables commandsiptables - t channel - An INPUT - m bpf - bytecode "22,40 0 12,21 0 19

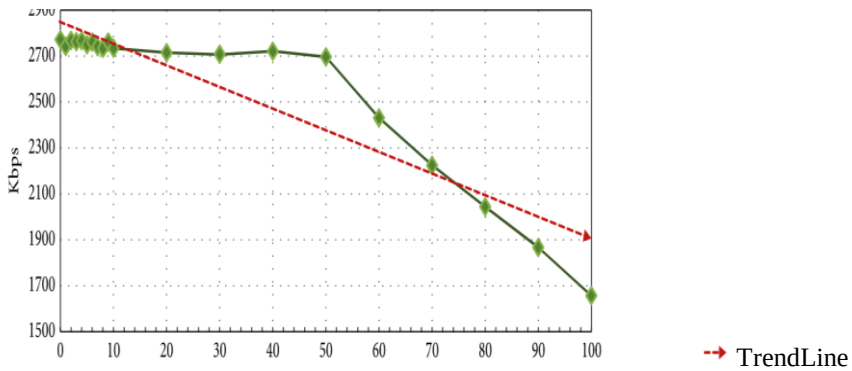

Figure 2: impact of theNFWrules in throughput

Results of the Impact Throughput

The results compiled in Table 1shows that the performance impact when using NFW filters is quite limited and will not severely affects the overall operation of IoT devices. We analysed the impact progressively by adding NFW rules to the filter and added up to 1000 new rules and measured the transfer rate after each NFW expression was added. As long as the performance is highly influenced by the presence of additional traffic in network and other processes consuming CPU, we plotted a trend line to observe the degradation. As seen in Figure 2, the throughput degradation is close to zero when using up to 50 (nonfitting) NFW rules. However, the inclusion of more than 50 rules clearly damages the performance of GNU/Linux firewalling system and would require the usage of additional iptables speedup strategies, such as the creation of additional chains and counters-based optimizations.

VI. CONCLUSION

As the Internet of Things begins to scale up, the number of devices continues to increase; more automation will be required for both the consumer and industrial environments. In the near term, data from IoT hardware sensors and devices will be handled by proxy network servers (such as a cellphone) since current end devices and wearables have little or no built-in security. The security of that proxy device will be critical if sensor information needs to be safeguarded. The number of sensors per proxy will eventually become large enough so that it will be inconvenient for users to manage using one separate app per sensor. This implies single appls with control many ―things,‖ creating a data management (and vendor collaboration) problem that may be difficult to resolve.An exponentially larger volume of software will be needed to support the future IoT. The average number of software bugs per line of code has not changed, which means there will also be an exponentially larger volume of exploitable bugs for adversaries. Until there are better standards for privacy protection of personal information and better security guidelines on communication methods and data/cloud storage, security of wearable and other mobility devices will remain poor. More work needs to be spent on designing IoT devices before too many devices are built with default (little or no) security. Physical security will change as well.

REFERENCES

[1]. Abomhara, M., &Køien, G. M. (2015). Cyber security and the internet of things:Ennigma - journal of information security and cryptography, vol. 4, no. 4, 2017

[2]. Aggarwal,C.C. N. Ashish, A.P. Sheth, The internet of things: a survey from the data-centric perspective, in: C.C. Aggarwal (Ed.), Managing and Mining Sensor Data, Springer US, Boston, MA, 2013, pp. 383–428.

[3]. Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and MoussaAyyash, ―Internet of Things: A Survey on Enabling Technologies, Protocols and Applications‖, doi:10.1109/comst.2015.2444095, vol. 1553-8777X(p), June 2015.

[4]. Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and MoussaAyyash, "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications", doi:10.1109/comst.2015.2444095, vol. 1553-8777X(p), June 2015.

[5]. Al-Fuqaha, A. M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, pp. 2347-2376, 2015.

[6]. Ali, S., Bosche, A., & Ford, F. (2018). Cybersecurity Is the Key to Unlocking Demand in the Internet of Things. Bain and Company.

[7]. Alur, R. E. Berger, A. W. Drobnis, L. Fix, K. Fu, G. D. Hager, et al., "Systems Computing Challenges in the Internet of Things," arXiv preprint arXiv:1604.02980, 2016.