Author's version accepted for CSR-2024; the final publication is available at https://ieeexplore.ieee.org/document/10679465

Stealth attacks on PCBs: an experimental plausibility analysis

Ievgen Kabin[1], Jan Schaeffner[1], Alkistis Sigourou[1], Dmytro Petryk[1], Zoya Dyka[1,2], Dominik Klein[3], Sven Freud[3], and Peter Langendoerfer[1,2]
[1] *IHP GmbH – Leibniz Institute for High Performance Microelectronics, 15236 Frankfurt, Germany*
[2] *Brandenburg University of Technology Cottbus-Senftenberg, 03046 Cottbus, Germany*
[3] *Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn, Germany*
{kabin, schaeffner, sigourou, petryk, dyka, langendoerfer}@ihp-microelectronics.com; {dominik.klein, sven.freud}@bsi.bund.de

***Abstract*—This paper reports – inspired by the Bloomberg article "The Big Hack" – on experiments researching the possibilities to manipulate Printed Circuit Boards (PCB) and the chances that such a manipulation can and will be detected. We used non-functional devices to showcase manipulations and are providing optical and X-ray pictures to illustrate how good or difficult it is to detect such manipulations. We researched hiding dies in parts of a PCB and under a BGA package. Our experiments clearly show that such manipulations are feasible and extremely hard to detect if done thoroughly.**

Keywords—PCB manipulation, trustworthy IT devices, supply chain security, Bloomberg, "The Big Hack", "The Long Hack", Chips Act, X-raying

I. Introduction

Globalization is a reality today that impacts the supply chain of many products. While this is economically beneficial it may pose significant risks to our societies. Currently, the political situation is especially tense if not highly critical. Even though efforts are underway to expand control of the supply chain [1], the issue of supply chain risks remains paramount. Especially for information technology devices, press articles such as "The Big Hack" [2] and "The Long Hack" [3] articles published by Bloomberg raise the question, which steps in the supply chain are trustworthy. A thorough review of the whole supply chain as well as associated risks can be found in [4]. Here, we are focusing on the feasibility of Printed Circuit Board (PCB) manipulations as those reported in [2]-[3].

In this paper, we are showcasing different approaches to manipulate a PCB. Our special attention is on the question of whether or not the manipulations can be detected by optical inspection or by X-raying the PCBs. Our main contributions are:

- Practically evaluating the feasibility of hiding chip dies within and under coils
- Identifying the impact of the bond wire material for the detection probability of implanted malicious chips, clearly showing that aluminum bond wires are best suited for stealth attacks
- Showing that even the back-side of Ball Grid Array (BGA) packages can be used to implant and hide malicious implants
- Providing optical and X-ray images to illustrate all our findings

Our focus was investigating the physical aspects of manipulating PCBs, hence note that despite the fact that we used real devices, none of the manipulations was functional. In addition, we want to stress that this paper does not support or deny the claims mentioned in [2]-[3] and whether the alleged events occurred or not. Our findings hint however, that from a technical perspective, the alleged manipulations seem not to be impossible.

The paper is structured as follows. Section II describes PCB design steps as well as the PCB vulnerabilities reported in the past. Section III describes our experiments of implanting a chip into a PCB. Section IV concludes this work.

II. Implants in PCBs

A. (In)secure PCB design?

PCB design is an essential step in the realization of a particular product and according to the reports [2]-[3], it is a critical step from a security perspective. During the design of PCBs, additional chips can be integrated into the overall circuit. These can fulfil different functions like espionage, implementation of backdoors or sabotage. For this, adaptations of the schematics by an attacker are necessary. Fig. 1 shows the steps from designing the schematic of the PCB via layout and creating Gerber files down to the PCB fabrication and assembly.

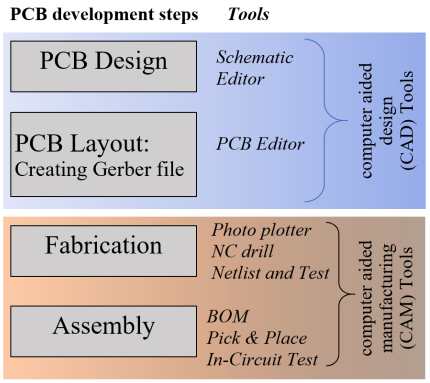


Fig. 1. PCB design steps and tools applied

The result of the PCB Design and PCB Layout steps are Gerber files, which can be created using different editors. The Gerber data format is the standard file format for designing PCBs. It is a set of 2-D ASCII files containing the complete information about the PCB, i.e. the routing of the layers and the connections between the layers, extracted from a Computer-Aided Design (CAD) file. Alternatively, a CAD file can be used. PCB NC drill files consist of PCB drilling and routing information. The NC formats were originally designed by Computer Numerical Control (CNC) drill and route machine vendors as proprietary input formats for their equipment; hence there are many different NC formats. Production and assembly of PCBs can be carried out by a single or by different companies. In both cases, additional chips can be integrated into the overall circuit, with all the aforementioned consequences to product reliability and security. Fig. 2 represents a layer model of a PCB showing the connections between different layers with the intended Application-Specific Integrated Circuits (ASICs) on the top and the bottom as well as a potentially malicious ASIC embedded between the PCB layers, shown as a grey rectangle. This very stealthy hiding method might require more effort from the attacker but is technically feasible.

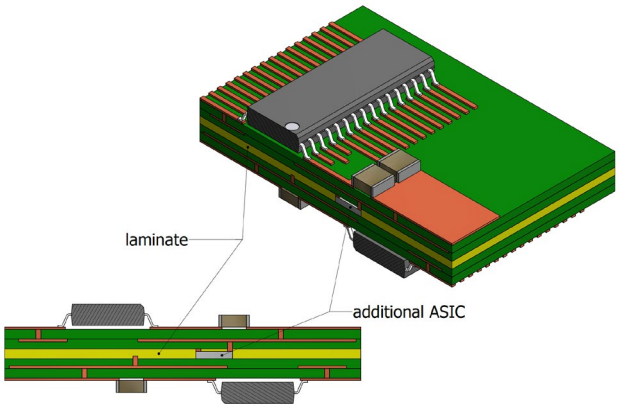


Fig. 2. Layer model of a PCB: the intended ASICs on top and bottom and the potentially malicious ASIC are shown as grey rectangles. There the potentially malicious ASIC is shown embedded between the PCB layers.

For complex manipulations of the PCB, the attacker needs the schematics. If we consider the PCB manufacturer as the attacker, schematics might already be at hand or can be restored using the Gerber files. The level of information provided to a PCB manufacturer is usually reduced, i.e. only PCB-pads (soldering pads) and the connections between the pads are provided. So, assessing the intended functionality might become very challenging. But for some chips, e.g. Peripheral Component Interconnect (PCI) interfaces, the footprints are quite unique providing additional information that was not directly given. This can help attackers make conclusions about the purpose of the board and the functionality of at least some chips on the board. Considering the assembly company as a potential attacker, altering the PCB becomes more challenging in comparison to the PCB manufacturer because the assembly companies obtain a readily manufactured PCB, the list of its components and their soldering places. The PCBs' circuit, layout and other information are missing. However, the assembly company knows which ASICs to put in which place and has the chance to integrate additional malicious ASICs by integrating those with the originally planned ones into a "system in package". This means that multiple ICs are covered with a common plate or filling. These then fulfil their function in the package and the malicious ones are therefore optically undetectable or at least very difficult to detect. An example of multiple chips inside a package can be found in [5].

B. Bloomberg's reports and PCB manipulations: a review

In recent years, the vulnerability of PCBs within the global supply chain has garnered significant attention from both industry experts and cybersecurity researchers. Malicious actors now have multiple entry points to introduce hardware implants due to the complexity and global nature of today's electronics manufacturing. These implants can be embedded during various stages of the production process, from the fabrication of silicon chips to the final assembly of electronic devices. The risks associated with these hardware Trojans are profound, potentially enabling unauthorized access, data exfiltration, and system manipulation without detection.

PCB manipulations mentioned in [2] were not confirmed, but the threat itself was discussed as feasible and potentially highly dangerous. Thus, Bloomberg's report triggered different studies of the feasibility of PCB manipulations [6]-[7]. Scholarly studies have highlighted several instances and theoretical frameworks for understanding how and where these vulnerabilities can be exploited. Notably, one survey [8] proposes a new taxonomy, reviews and categorizes PCB countermeasures and board-level Trojans from 75 references, to mitigate the vulnerabilities. One of the analyses provides a comprehensive table of 24 Trojans extracted from 19 distinct sources, categorizing them based on the nature of the modification to the PCB, their location, integration methods, triggers, and the effects of their presence. We represented the main facts from this table graphically in Fig. 3 to give a short overview. 19 references discussing PCB Trojans are grouped into 3 sets: 13 academic proposals, 9 real-world experiments and 2 references discussing theoretic possibilities of the Trojan implants. These 3 sets are represented as blue and green circles in Fig. 3. We represented different kinds of Trojans we as red, orange and yellow ovals. The numbers indicate how many references from each set discuss a particular type of Trojan.

The survey [8] revealed that nearly 60% of the analysed Trojans appeared to be additions to the original design, and over 65% were located on the surface of the PCB while almost half of them combined both, see the set of the Trojans denoted as "Add-on component on the PCB surface" in Fig. 3. This finding aligns with the claims made in [2].

Although more than 60% of the references in the survey predate the "Big Hack", it is evident that the issue of exploiting the surface of PCBs has been a concern for researchers for several years. This underscores the ongoing need for heightened vigilance and advanced security measures in the electronics manufacturing industry to mitigate the risks posed by hardware Trojans.

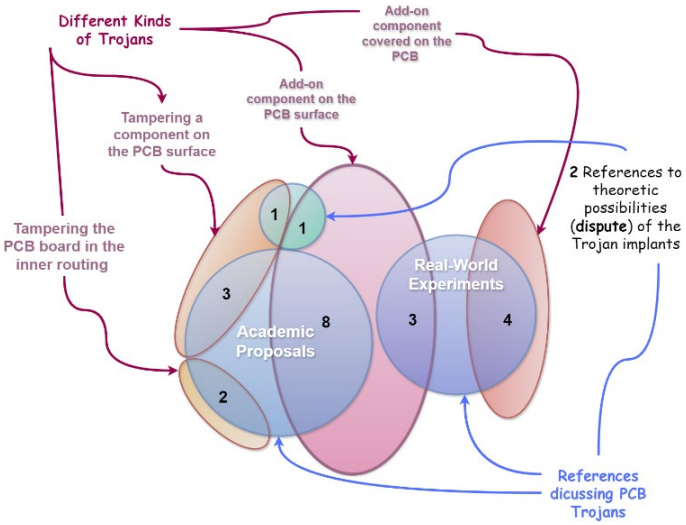


Fig. 3. Summary of PCB Trojans identified in [8]: a graphical visualization. For the real-world experiments two unclassified instances are not shown

The method proposed in [9] aims to address the threat of PCB-level hardware Trojans being inserted into devices post-shipment, requiring lifetime monitoring. In [10] the authors introduce PRISTINE, an emulation platform for PCB-level hardware Trojans, enabling the insertion and observation of Trojans on custom and commercial PCBs. The paper [11] introduces a novel Chip-PCB hybrid Physically Unclonable Function (CPR PUF) by combining a Weak PUF on the PCB with a Strong PUF inside the chip, enhancing security and authenticity verification.

Inspired by the discussion about Bloomberg's article "The Big Hack" and considering the research articles on PCB manipulations we decided to thoroughly investigate the practical plausibility of such attacks and especially the fact whether or not they may go undetected. The results of our experiments are discussed in the following section.

III. Our Experiments

A. *Suitable places on PCB for malicious chip insertion*

The aim of the experiments is to provide an experimental assessment of the attacks reported in [2]-[3]. So, the task performed was implanting a (small) chip into a PCB in order to assess the feasibility, cost and time of such manipulations as well as the conspicuousness of the manipulated areas. There are many possibilities to manipulate a PCB e.g. by hiding an IC within the layers of the PCB or using an IC that looks like a regular component, for example a capacitor, or to place the malicious IC under another component. In this experiment, we implanted a small chip in the compound of a certain coil as well as under the housing of a second coil.

We selected the following four chips[1] as implants in our experiments:

- NXP A1006UK/TA1NXZ – secure authenticator [12]
- NXP A1006TL/TA1NXZ – secure authenticator [12]
- Infineon OPTIGATM Trust B Authentication IC (SLE952500000XTSA1) – authentication solution for improved security and reduced system costs [13]
- an IHP Chip (due to the IHP IP properties the chip die is shown pixeled) manufactured in the IHP 250 nm technology [14]

Optical and X-ray pictures of the 4 chips selected for experiments are shown in Fig. 4.

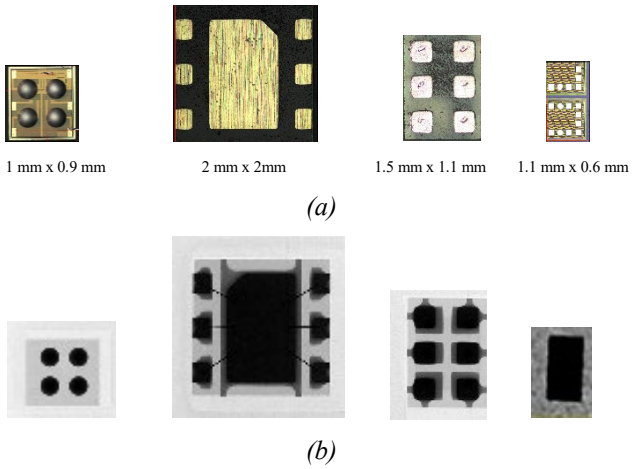


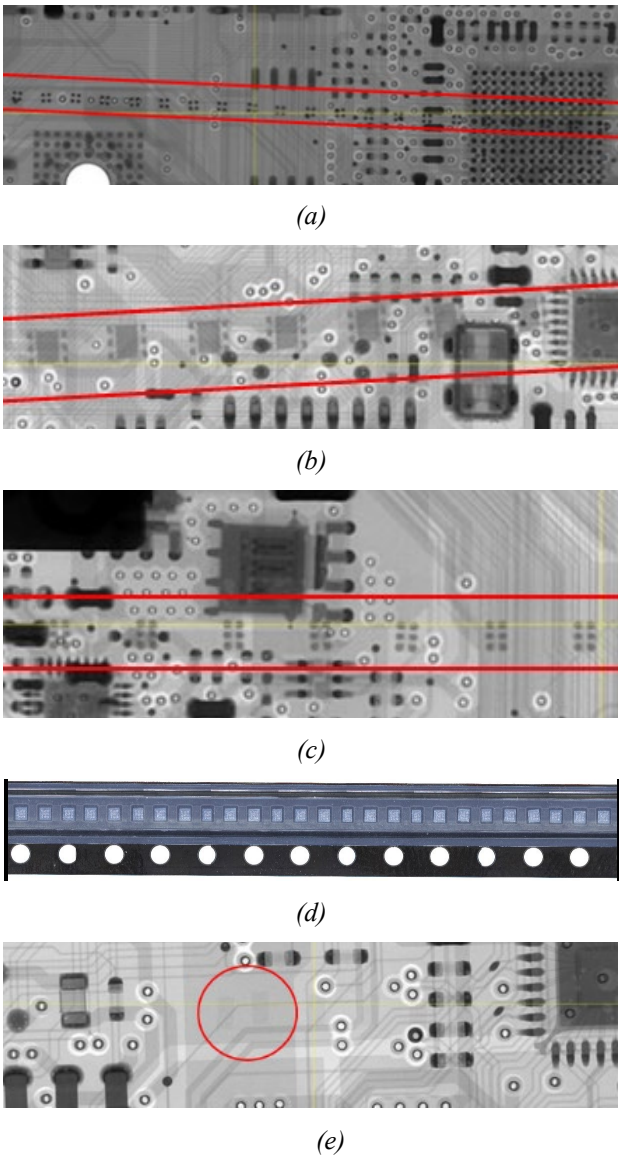
Fig. 4. Optical and X-ray pictures of chips selected for the experiments: NXP A1006UK/TA1NXZ (left), NXP A1006TL/TA1NXZ (2nd from left), Infineon SLE952500000XTSA1 (3rd from left), an IHP Chip (right, optical picture pixelated, due to intellectual property issues).

In order to have a rather large selection of hiding places, we selected a relatively large PCB[2] consisting of a variety of different components such as inductors, capacitors, chips, connectors, etc. for the experiments as the board into which the IC had to be implanted. The places on a PCB, that are suitable for manipulations and not noticeable during a normal visual inspection, are e.g. the places under larger components or glob-top potting material, etc. In addition to give a better insight, the board was also examined in the X-ray machine: we tested which chips might go undetected when X-raying the manipulated PCB. All four chips were placed on the PCB and X-ray pictures were taken. All chips except for the IHP chip are clearly visible, see Fig. 5.

In Fig. 5 the IHP chips are almost invisible. The NXP A1006TL/TA1NXZ chip was excluded from further experiments because it has internal gold wires that are clearly visible in the X-ray images.

1 These chips have relative complex functionality but are small and have only few pins for connecting power supply as well as input/output signals. Assuming that malicious implants have to be small and easy-to-connect we selected these chips as suitable implant candidates for our experiments.

2 A non-functioning motherboard from a Dell Latitude E6410 laptop



(a)

(b)

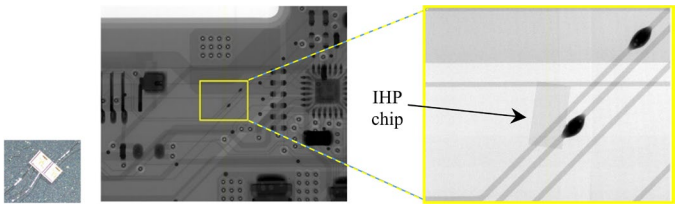
(c)

(d)

(e)

Fig. 5. X-ray images of the PCB with the chips selected for the experiments: the NXP and Infineon chips in tape and reel packaging were placed on the PCB and X-ray pictures were taken, see *(a)-(c)*; the optical picture of the NXP chips A1006UK/TA1NXZ in tape and reel package are shown in *(d)*. The red rectangles in *(a)-(c)* show the area with clearly visible chips in the X-ray pictures. The area in the X-ray picture with two IHP chips is marked with a red circle, see *(e)*; the IHP chips are almost invisible and would also disappear in the noise if placed in the right spot.

Please note that aluminum wires are not well visible by X-raying [3]. Due to this fact, we performed additional experiments with IHP chips to determine whether the aluminum bonding wires would show up in the X-ray image. The IHP chip with aluminum wires was placed on the board and X-rayed, see Fig. 6. The chip outlines were slightly visible while the aluminum wires were not visible. Thus, this chip would also disappear in the noise if placed in the right spot.



(a) *(b)*

Fig. 6. Optical *(a)* and X-ray *(b)* images of the IHP chip with aluminum bonding wires, on the right side of *(b)*: zoomed in.

Fig. 5 demonstrates clearly that implanting the chips into the "relatively free" PCB areas will be easily noticed by analysing the X-ray picture. The places on the PCB where the chips are not noticeable are the very dark areas in the X-ray pictures. The PCB has many of these areas with a lot of metal or materials with a high density, e.g. coils or capacitors. Places, which are suitable for the manipulation are those that remain inconspicuous in both cases, i.e. normal optical inspection and X-ray inspection. Two locations that were selected based on the preliminary investigations are Coil 1 and Coil 2 marked by yellow circles in Fig. 7.

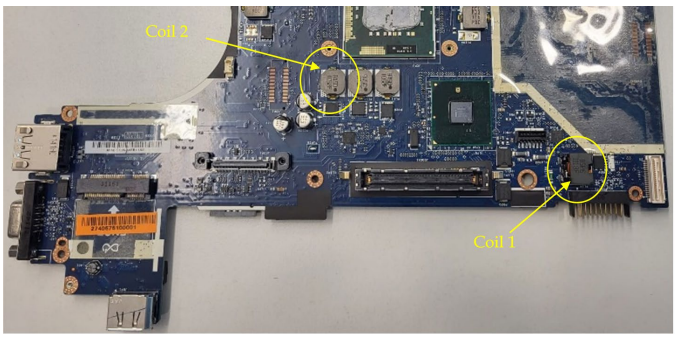


Fig. 7. Coil 1 and Coil 2 on the PCB were selected for the manipulation experiments.

B. Chips implanted in coil's compound material

Fig. 8. displays the steps taken to implant two chips, the IHP chip and the Infineon authentication chip, into the compound material of Coil 1 in the order of their execution. The potting compound was carefully milled open and the chips were glued into the milled holes. After that, the openings were closed with potting compound.

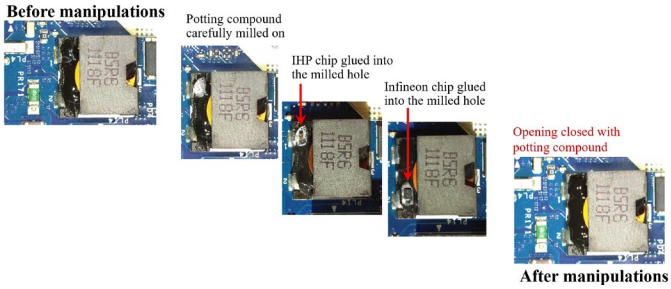


Fig. 8. Experiments with Coil 1: hiding chips in the coil compound.

[3] Copper is visible, gold is well visible.

Fig. 9 shows X-ray images of the PCB area with Coil 1 after these manipulations. The two manipulated places are marked with yellow rectangles in the coil picture (middle). Both yellow rectangles are shown on the left and right side, zoomed in. The Infineon chip can be easily seen and is marked with a red rectangle.

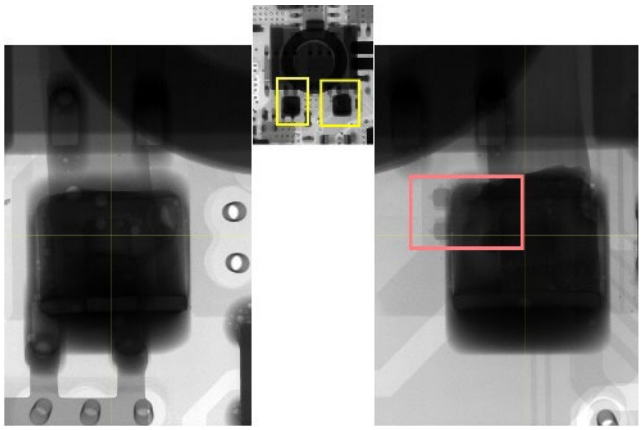


Fig. 9. X-ray after implanting the IHP (left side) and the Infineon (right side) chips: the IHP chip is not visible, while the Infineon chip is visible.

C. *Chips implanted in coil's metal housing*

Our experiments with Coil 2 differ slightly from the experiments described above. We made an attempt to hide the implanted chips under the metal housing of the coil. Fig. 10 (a) shows the optical picture of the PCB with Coil 2 before and after the manipulations. Coil 2 was unsoldered, the IHP chip was placed next to the solder tag and glued on it. On the other side, the coil was milled open a little to be able to implant the 0.4 mm thick chip. This step prevented the manipulated coil from being higher than the original. The NXP secure authentication chip was glued on it and Coil 2 was soldered back on the PCB. The manipulation steps are shown in Fig. 10 *(b)*. Fig. 10 *(c)* shows the X-ray picture of the PCB with the manipulated Coil 2.

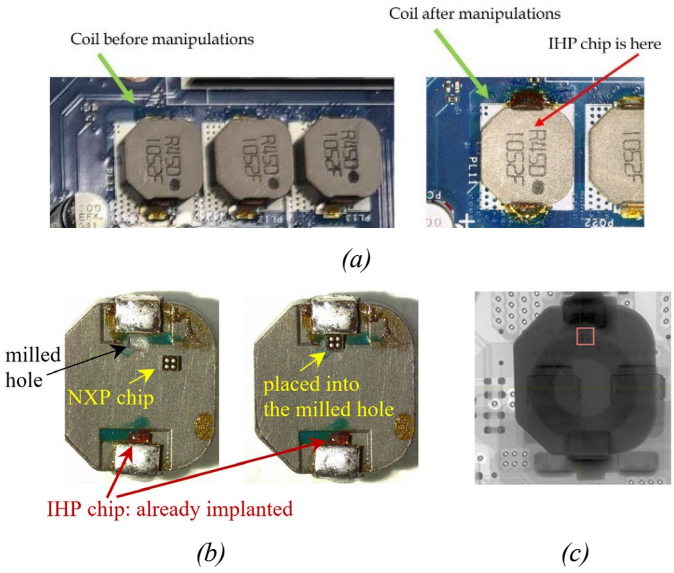


Fig. 10. Experiments with Coil 2: hiding chips under the coil's housing.

The X-ray images revealed only the NXP chip (see red rectangle in Fig. 10 *(c)*). The IHP chip was not visually detectable on the X-ray image. Please note that the visible difference in the solder (see Fig. 10 *(a)*) can be easily obfuscated by an attacker, e.g. by re-soldering all three coils or by artificially aging the soldering points.

Our experiments showed that detecting the implemented chip can be extremely difficult. Even X-raying the PCB does not guarantee the detection of all PCB manipulations. A chip can be implanted into a PCB and hidden under components of the PCB or underneath PCB labels (e.g. as a "repair"). Even though re-soldering of components by hand can in principle always be detected because it is optically distinguishable from machine soldering, such manipulations can be well camouflaged so that only experts see the re-soldering. Additionally, malicious chips can be implanted into an intended chip package, or into a coil from the back, i.e. the PCB's components can be manipulated. If a chip hidden in this way is "soldered in", it will be difficult to find it visually. Even after X-ray imaging such manipulations may be not noticed, due to (for example) aluminum wiring. Possibly a computed tomography scan with high resolution can help to detect the implants. The challenge and complexity of such PCB manipulation attacks is not only the implantation of a chip into the PCB and camouflaging the manipulation place but also the power supply of the implanted malicious chip. These manipulations require some preparation steps, which are also not easy to perform after PCB manufacturing, i.e. manipulations of the PCB's layout before its manufacturing can be required – and that assumes involving a corrupt assembly company or corruption in early PCB designing steps. Please note that if an attacker can invest enough time and costs, the PCB can be analysed, and reverse engineering of at least some parts of the PCB can be performed. It cannot be excluded that a suitable place for the manipulation can be found, including the possibility to contact the malicious chip electrically to all required power supplies as well as signal lines.

In conclusion, attacks such as the manipulation of a motherboard as described in [2] are technically feasible and most probably will go undetected. Of course this feasibility from a technical perspective does not give any hint if the allegations made in [2] are correct or not.

D. *Malicious chips between PCB and chips*

One of the most suitable places to implant a malicious chip into a PCB is the room between the PCB's surface and the chips mounted on the PCB. In this case the malicious chip can be relatively easy connected to the power supply pins of the attacked chip as well as to its input/output pins. As mentioned in the sections above, the dies of chips are not well visible in X-ray pictures. The placement of malicious chips between a PCB and the intended/attacked chip hides the malicious chips from optical inspection. Using aluminum wires to establish the electrical connection to the selected pins of the attacked chip is not observable by X-raying. An additional advantage of this kind of implantation is the fact, that it is not necessary to modify the PCB layout by preparing "hidden" wires in its inner layers to provide the electrical contacts for the malicious chip, which can then be implanted – possibly – in the future.

Fig. 11 shows schematically the possibility of inserting such a malicious chip in the backside of a Spartan-6 Field Programmable Gate Array (FPGA). The black rectangles represent the potential malicious chips: these can be up to 0.65 mm x 0.65 mm in size, while another can be 0.31 mm wide and have almost any length.

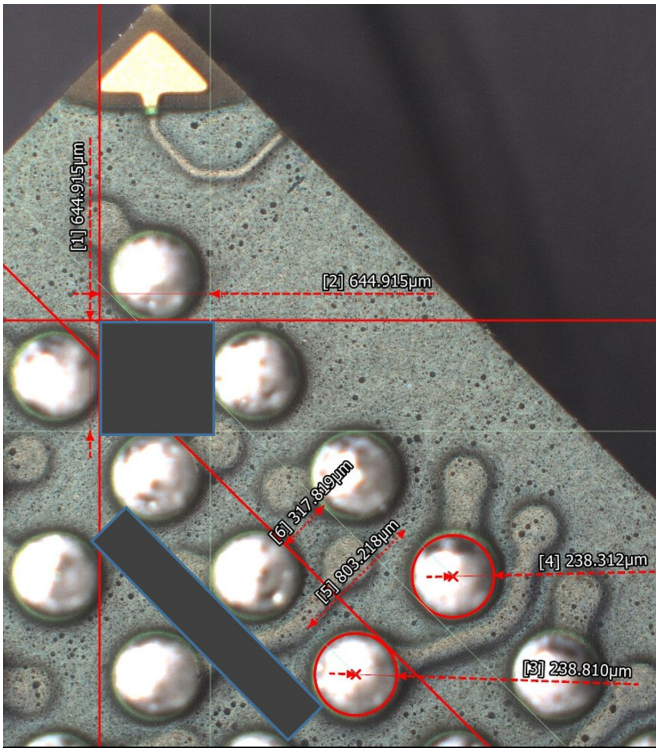


Fig. 11. Spartan-6 in a BGA package, backside: the black square (size 0.6 mm x 0.6 mm) and the rectangle (0.3 mm x 1.6 mm) represent theoretically possible placements of malicious chips between the contacts of the BGA package.

If the malicious chip die can be thinned sufficiently for such insertion, it can be placed between any BGA pins as shown in Fig. 11. For non-thinned malicious chips, the attacked chip – such as an FPGA in a BGA package - can be milled open a little if no wires in the BGA package are destroyed. However, such a manipulation is not always possible.

BGA packages are normally regarded as a kind of countermeasure, for example against optical backside fault injection, because such packages are difficult to decapsulate or tamper with. To hide a malicious chip, BGA packages are less suitable than Quad-Flat-Packages (QFP) due to the pins of the BGA package: each pin must be soldered to the PCB, and the distance between the pins is usually small. But even in this special case, a malicious chip can be inserted, as shown in Fig. 12.

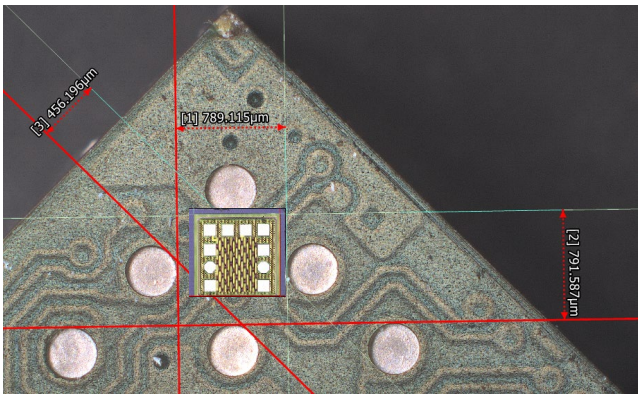
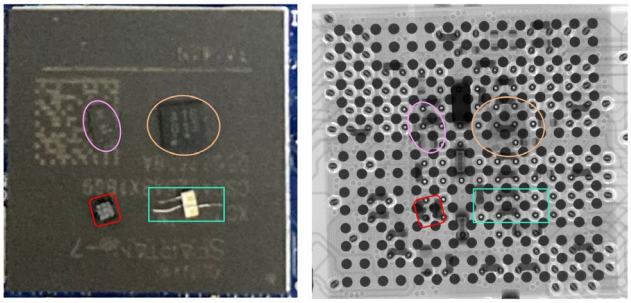


Fig. 12. Backside of a Spartan-7 in a BGA package: the distance between the pins allows to implant a chip of about 0.7 mm x 0.7 mm. The IHP chip used for the experiments in this work consists of two designs, one of which is about 0.6 mm x 0.7 mm. Here this IHP chip is "placed" on a Spartan-7 FPGA using image processing tools considering the relations between sizes and pins of the chips. This demonstration illustrates only a theoretical possibility of chip placement.

Fig. 13 shows optical and X-ray images of a PCB part with a Spartan 7 FPGA with the four chips selected as "implants" (see Fig. 5) placed on its surface. These pictures demonstrate that the chip die is not easy to see, only the chip pins manufactured with gold (Au) are visible in the X-ray picture. Fig. 13-*(b)* is given in Appendix, zoomed in.



(a) *(b)*

Fig. 13. Experiments with a PCB with a Spartan-7 FPGA and 4 chips selected for experiments in this work: *(a)* – optical picture; *(b)* – X-ray picture: the small IHP-Chip with aluminum wires is not visible, but generally all chips are not easy to see. If the pictures are sufficiently magnified they can be identified, especially when using additional knowledge of their placement (see Appendix).

Fig. 14 shows optical as well as X-ray pictures of an IHP board with an IHP chip with cryptographic accelerators for AES as well as for ECC. The IHP chip has a Quad-Flat-Package, and the 4 chips selected as "implants" (see Fig. 5) are placed on its surface. On the back-side of the PCB below the IHP chip a quartz is placed. The quartz is especially well suited to hide the "malicious" chips. Fig. 14-*(b)* is given zoomed in, in the Appendix.

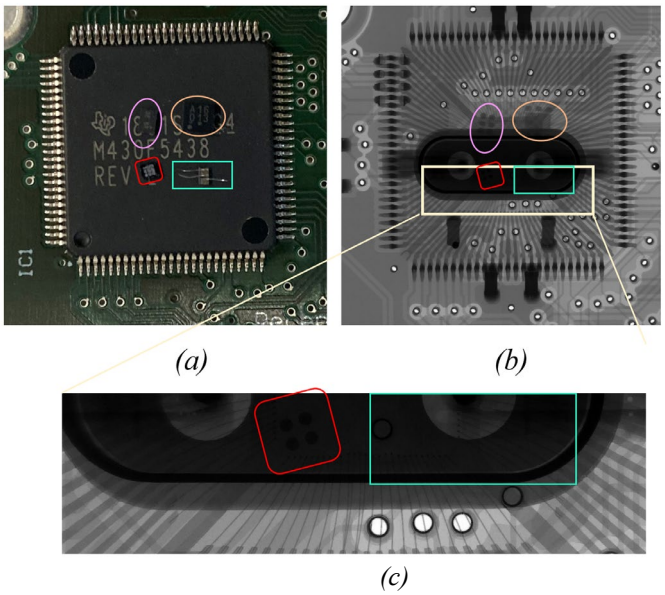


Fig. 14. Experiments with an IHP cryptochip and the 4 chips selected for experiments in this work: *(a)* – optical picture; *(b)* – X-ray picture; *(c)* – the selected part of the X-ray picture, zoomed in, the small IHP-Chip with aluminum wires is not visible.

IV. Conclusion

In this paper we reported on our experiments researching PCB manipulations while focusing on the issue of how difficult it is to detect such manipulations, if the attacker works carefully and puts sufficient effort in hiding his manipulations. Our experiments clearly show that:

- such manipulations are technically feasible and
- extremely difficult to detect, as even X-raying is not sufficient to identify all types of manipulations

The latter especially holds true for malicious dies implanted in chip packages, in or under coils. Especially unsettling is the fact that malicious dies might also be hidden between the pins on the backside of a BGA package, which makes such manipulations almost invisible even on X-ray images. Especially dangerous are implants on the backside of chips due to the fact that the connection of the malicious chips to power supply (as well as to input/output pins of the intended chips) can be done using aluminum wires; this does not require any additional steps for manipulation/preparation of the PCB layout for implanting malicious chips

While our experiments do neither confirm nor refute the allegations mentioned in [2]-[3], they show that such manipulations are technically plausible. This in turn means that the trustworthiness of the supply chain is a highly important issue. This also raises new research questions, i.e. what are the means to reliably detect manipulations as well as what are the means to prevent manipulations in the first place.

References

[1] European Chips Act. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en

[2] Robertson, Jordan. Riley, Michael. 2018. *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*. In Bloomberg Businessweek, Feature. URL: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[3] Robertson, Jordan. Riley, Michael. 2021. *The Long Hack: How China Exploited a U.S. Tech Supplier*. Bloomberg. URL: https://www.bloomberg.com/features/2021-supermicro/

[4] BSI veröffentlicht Studie zu Manipulationsmöglichkeiten von Hardware in verteilten Fertigungsprozessen. URL: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/PANDA_240604.html

[5] James, Dick (sdavis). 2015. *Apple Watch and ASE Start New Era in SiP*. URL: https://chipworksrealchips.blogspot.com/2015/08/apple-watch-and-ase-start-new-era-in-sip.html

[6] River Loop Security. A TALE OF TWO SUPPLY CHAINS. URL: https://riverloopsecurity.com/blog/2018/12/supermicro-validation-1/

[7] Trammell, Hudson. 2018. *Modchips of the state: On the technical feasibility of the BMC implant*. Bloomberg. Annotated transcript. URL: https://trmm.net/Modchips/,
Video. URL: https://ftp.fau.de/cdn.media.ccc.de/congress/2018/h264-hd/35c3-9597-eng-deu-fra-Modchips_of_the_State_hd.mp4

[8] J. Harrison, N. Asadizanjani, and M. Tehranipoor, "On malicious implants in PCBs throughout the supply chain," Integration, vol. 79, pp. 12-22, 2021.

[9] S. Kaji, D. Fujimoto, and Y. Hayashi, "Simulation-Based Approach to Generating Golden Data for PCB-Level Hardware Trojan Detection Using Capacitive Sensor," in 2023 IEEE Physical Assurance and Inspection of Electronics (PAINE), Oct. 2023, pp. 1–7. doi: 10.1109/PAINE58317.2023.10317949.

[10] J. Huan, S. D. Paul, S. Mandal, and S. Bhunia, "PRISTINE: An Emulation Platform for PCB-Level Hardware Trojans," IEEE Access, vol. 12, pp. 49291–49305, 2024, doi: 10.1109/ACCESS.2024.3383834.

[11] Y. Xu, T. Ke, W. Cao, Y. Fu, and Z. He, "Reliable and Efficient Chip-PCB Hybrid PUF and Lightweight Key Generator," IEICE Trans. Electron., vol. E106.C, no. 8, pp. 432–441, Aug. 2023, doi: 10.1587/transele.2022ECP5050.

[12] NXP A1006. Secure Authenticator IC. Rev. 1. Product short data sheet. URL: https://www.mouser.de/datasheet/2/302/PHGL_S_A0007960927_1-2522290.pdf

[13] OPTIGA™ Trust Product Authenication Family. SLE95250 OPTIGA™ Trust B Authentication IC. Brief Databook. Rev. 2.01. URL: https://www.infineon.com/dgdl/Infineon-OPTIGA%20TRUST%20B%20SLE%2095250-DataSheet-v02_01-EN.pdf?fileId=5546d4625b10283a015b18f045a3476e

[14] IHP GmbH. SiGe BiCMOS and Silicon Photonics Technologies. URL: https://www.ihp-microelectronics.com/services/research-and-prototyping-service/mpw-prototyping-service/sigec-bicmos-technologies

APPENDIX

Fig. 13-*(b)*, zoomed in:

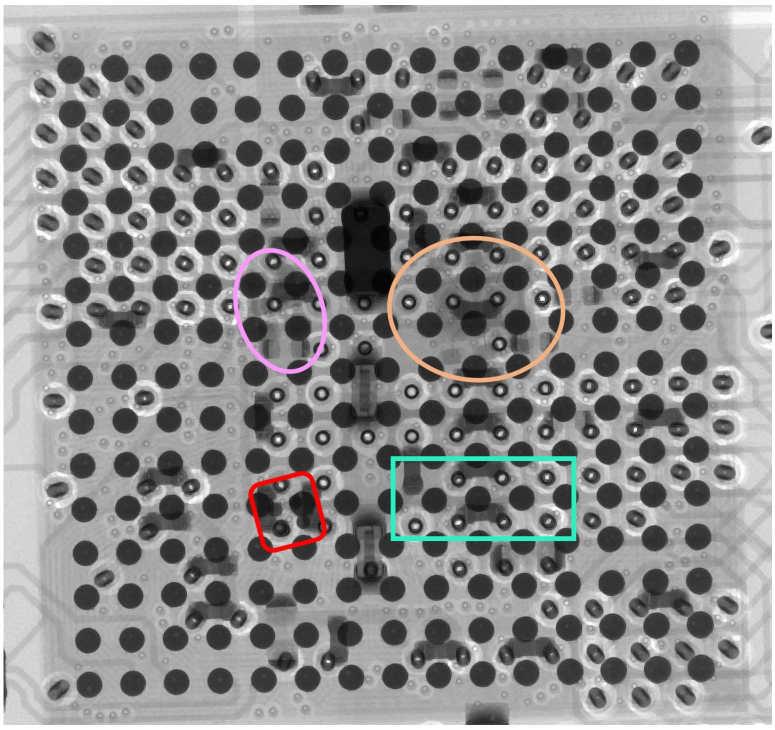


Fig. 14-*(b)*, zoomed in: