O *HARDWARE* COMPROMETIDO: UMA IMPORTANTE AMEAÇA A SER CONSIDERADA PELA ATIVIDADE DE INTELIGÊNCIA

Gustavo Andrade Bruzzeguez *
Clóvis Neumann **
João Carlos Félix Souza ***

Resumo

As questões ligadas à segurança cibernética são complexas e sofisticadas, e estão em constante transformação. Nos últimos anos, pesquisadores vêm demonstrando a possibilidade de implementação de códigos maliciosos em circuitos integrados (*chips*) durante a fabricação destes dispositivos. A ameaça, que ficou conhecida como hardware Trojan, vem atraindo a atenção dos governos e da indústria, dado que potencialmente envolve questões de espionagem e guerra cibernética. O problema vem se agravando com a globalização da cadeia de fabricação de circuitos integrados, considerando que são comumente manufaturados fora dos limites dos territórios nacionais, o que implica em perda de controle sobre as etapas do processo. O presente artigo objetiva alertar para a existência da ameaça do hardware Trojan, e discorrer sobre a relevância do tema para a área de inteligência, a partir de breve revisão da literatura relativa ao assunto, na qual utilizou-se, do ponto de vista metodológico, o enfoque meta-analítico. Observa-se que o potencial lesivo do hardware Trojan é preocupante, com ações que incluem vazamento de dados, espionagem, ataques de indisponibilidade, disrupção de sistemas, sabotagem, dentre outras. Trata-se, portanto, de uma questão que precisa ser abordada e gerenciada no âmbito dos governos e, em particular, nos serviços de inteligência.

Palavras-chaves: hardware Trojan; Atividade de Inteligência; segurança da informação e comunicação; segurança cibernética.

COMPROMISED HARDWARE: AN IMPORTANT THREAT TO BE ADDRESSED BY INTELLIGENCE SERVICES

Abstract

Issues related to cybersecurity are complex and sophisticated, and are constantly changing. In recent years, researchers have been demonstrating the possibility of malicious codes being inserted into integrated circuits (chips) during the fabrication of these devices. The threat, known as hardware Trojan, has been drawing the attention of governments and industry since it potentially involves espionage and cyber warfare issues. The problem is getting worse with the supply chain globalization, since the chips are often manufactured in factories outside the boundaries of the national territories, which implies a loss of

* Servidor público federal, mestre em Computação Aplicada e especialista em Governança de Tecnologia da Informação. É pesquisador na área de segurança cibernética, tendo participado da elaboração da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal, no âmbito do Gabinete de Segurança Institucional da Presidência da República.

** Doutor em Engenharia, professor e pesquisador da Universidade de Brasília - UnB.

*** Doutor em Economia, professor do Departamento de Engenharia de Produção - UnB e pesquisador no Programa de Pós-graduação em Ciência da Computação Aplicada - UnB.

Artigo recebido em julho/2018
Aprovado em outubro/2018

control over the process steps. This article aims at warning about the existence of the threat of hardware Trojan and to discuss the relevance of the topic to the intelligence service, starting from a brief review of literature on the subject, in which it was used, from the methodological point of view, the meta-analytic approach. The potential of hardware Trojan is a concern, with actions that include data leakage, espionage, denial of service attacks, system disruption, sabotage, and so on. It is, therefore, an issue that needs to be addressed and managed within the government, and in particular the intelligence services.

Keywords: *hardware Trojan; Intelligence Service; information and communications security; cybersecurity.*

Introdução

Imaginemos uma situação hipotética: um alto executivo do governo, supostamente utilizando um *smartphone* seguro, percebe que seu equipamento está travando sem motivo aparente. Nada parece funcionar, nem mensagens, nem ligações, nem qualquer aplicativo. Ele reinicia o dispositivo e os problemas permanecem. Então retira e reinsere a bateria, além de reiniciar o equipamento várias vezes - tudo em vão. Pareceria um simples problema de hardware se, mais tarde, não se descobrisse que o caso não é isolado. Centenas de milhares de *smartphones* também apresentam o mesmo comportamento mundo afora.

A situação hipotética descrita, adaptada de Villasenor (2010), na verdade ilustra um possível e sofisticado ataque cibernético em larga escala. Em tese, qualquer dispositivo que contenha um circuito integrado no hardware está sujeito a esse tipo de ataque, que será abordado em detalhes nesse artigo.

Na atualidade, os circuitos integrados (CIs), também referidos como "*chips*" de computador, estão presentes em uma infinidade de equipamentos, tais como computadores, celulares, equipamentos de redes computacionais e outros dispositivos eletrônicos, que por sua vez são empregados nas mais diversas áreas, muitas delas estratégicas para um país, a exemplo das Atividades de Inteligência, das comunicações, das infraestruturas energéticas, dos meios de transporte, dos mercados financeiros, em sistemas de defesa, em sistemas de controle de tráfego aéreo, dentre outros.

Os CIs concentram boa parte da "Inteligência" dos equipamentos, o que faz com que qualquer mal funcionamento nesses pequenos dispositivos afete de forma relevante a confiabilidade da máquina ou do sistema no qual ele opera. No entanto, tradicionalmente os ataques cibernéticos não exploravam vulnerabilidades do hardware. A Figura 1 exemplifica ataques em diferentes camadas, como aqueles que exploram o usuário (engenharia social[1]) e os ataques implementados por meio do software (*malwares* e macros em softwares de aplicação; e vírus e cavalos de Tróia[2] em sistemas operacionais).

O hardware, "*the root of trust*" (raiz de confiança), como mencionaram Becker *et al.* (2013) e Bhunia *et al.* (2014), é geralmente considerado a parte do sistema cuja confiança é uma premissa. Até recentemente, essa era uma assunção razoável (VILLASENOR, 2011), mas o cenário vem se alterando. A possibilidade de implementação de códigos maliciosos no nível do hardware – os chamados "hardware Trojans" (HT) – vem sendo estudada e discutida há alguns anos. A globalização da cadeia de fabricação de CIs, principalmente em países asiáticos (BEAUMONT, HOPKINS e NEWBY; 2011), e o aumento da complexidade na fabricação desses dispositivos têm incentivado os debates acerca dos problemas

1 Técnica por meio da qual um agente malicioso procura persuadir um usuário a executar determinadas ações, com o fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes (CERT.BR, 2017).

2 Tipo de código malicioso que, além de executar as funções para as quais foi aparentemente projetado, também executa funções maliciosas e sem o conhecimento do usuário (Cert.BR, 2017).

de se garantir a confiança no nível do hardware e os riscos decorrentes da perda de controle sobre os processos envolvidos na cadeia de fabricação de *chips*.

Figura 1- Visão esquemática de ataques cibernéticos em diferentes camadas. Adaptada de Iqbal (2011).

O fenômeno vem chamando a atenção dos governos de diversos países, como mencionaram Yoshikawa, Takeuchir e Kumaki (2014), a exemplo dos Estados Unidos, que estruturou, em 2004, o chamado *Trusted Foundry Program* (MCCORMACK, 2006), objetivando assegurar a confiabilidade de sistemas críticos para a defesa nacional. Em 2011, a Austrália liberou ao público seus estudos sobre o tema (BEAUMONT, HOPKINS e NEWBY; 2011), abordando formas de implementação do HT, técnicas de detecção e contramedidas.

Estudos revelam a possibilidade de CIs serem "intencionalmente comprometidos durante o processo de *design*, antes mesmo de serem manufaturados" (VILLASENOR, 2013). Ou ainda, a alteração pode se dar durante o processo de manufatura, como alertaram Becker *et al.* (2013). As possibilidades são diversas e potencialmente envolvem comprometimentos na disponibilidade, na integridade e na confidencialidade de dados que trafegam no hardware.

Não obstante os riscos e danos em potencial, a detecção do HT não é uma tarefa simples, e as técnicas existentes atualmente não são efetivas o bastante para detectá-lo (XIAO et al., 2016). O ex-chefe da Agência Central de Inteligência (CIA) e Agência de Segurança Nacional (NSA), General Michael Hayden, chegou a declarar que a questão de hardware comprometido é um problema que não pode ser resolvido, mas uma situação que deve ser gerenciada (RAWNSLEY, 2011).

Portanto, entender a ameaça e criar capacidade de reação é uma necessidade, e estudos futuros terão que focar na combinação das melhores técnicas de prevenção e detecção para prover equipamentos livres da ameaça do HT (BEAUMONT, HOPKINS e NEWBY; 2011).

O presente artigo aborda breve revisão da literatura a respeito do hardware Trojan, demonstrando a relevância do tema para as atividades de inteligência. Para tal, ilustra as características fundamentais do HT, seu potencial lesivo, possíveis pontos de inserção na fabricação de CIs e aborda ainda algumas formas de implementação. Analisa um tipo de implementação específica, de característica furtiva e dissimulada e de difícil detecção. Na sequência, discute implicações do fenômeno nas atividades de inteligência e introduz visão geral sobre possibilidades de detecção e prevenção da ameaça e os desafios da Contrainteligência. Por fim, ideias conclusivas são apresentadas.

No levantamento das fontes de pesquisa bibliográfica, utilizou-se o enfoque meta-analítico, metodologia que surgiu com o objetivo de dotar as revisões de pesquisa com o rigor, a objetividade e a sistematização necessárias para que se constitua o verdadeiro saber científico (SANCHEZ, 1999). As bases de dados consultadas foram ISI Web of Science[3] e Scopus[4], no período de 2007 a 2017.

Circuitos Integrados

Os CIs são constituídos por uma matriz microscópica de circuitos eletrônicos e outros componentes, tais como resistores, capacitores, diodos e transistores, implantados na superfície de um material semicondutor – como o silício, por exemplo (GOERTZEL, 2013). Dessa forma, o circuito resultante é um *chip* monolítico (inteiriço), que pode ser tão pequeno a ponto de ocupar poucos centímetros ou mesmo milímetros quadrados de área (Figura 2).

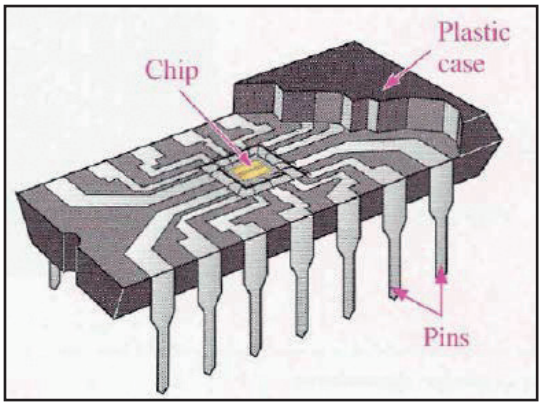

Figura 2 - Visão em corte de um Circuito Integrado típico. Fonte: Floyd (2014)

A fabricação de um CI é um processo complexo que chega a envolver, em alguns casos, mais de quatrocentas etapas (GOERTZEL, 2013). No entanto, visto de uma forma simplificada, pode-se enumerar cinco macroprocessos genéricos, conforme demonstrado na Figura 3.

Conforme Villasenor (2013), o processo de fabricação de um CI se inicia na especificação, que consiste na definição das funcionalidades do CI, incluindo características como velocidade, capacidade de processamento, dentre outras. Na fase do *design*, as especificações são então traduzidas na forma de operações lógicas e, posteriormente, nos circuitos elétricos correspondentes. Uma vez finalizado, o projeto de *design* é então enviado para uma fábrica de semicondutores, onde de fato ocorre a manufatura física do CI. Após essa etapa, testes de qualidade são feitos em amostras do circuito integrado e só então ele estará pronto para ser comercializado e inserido em algum equipamento.

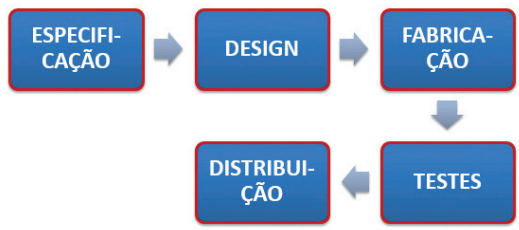

Figura 3 - Etapas da fabricação de um circuito integrado. Adaptado de Villasenor (2013).

3 Disponível em: <www.webofknowledge.com>. Acesso em: 10 set. 2018

4 Disponível em: <www.scopus.com>. Acesso em: 10 set. 2018

O Potencial Lesivo do Hardware Trojan

O hardware Trojan (HT) representa qualquer alteração maliciosa e deliberada no CI (RAJENDRAN *et al.*, 2010). É uma modificação maliciosa, intencional e indesejada no CI, resultando em um comportamento incorreto de um dispositivo eletrônico quando em operação (BEAUMONT, HOPKINS e NEWBY; 2011). São modificações no circuito original inseridas por adversários com o objetivo de expor o hardware ou acessar dados ou software rodando nos sistemas que utilizam o *chip* (TEHRANIPOOR e KOUSHANFAR, 2010).

As consequências de um circuito infectado podem envolver desde modificações na funcionalidade ou na especificação do hardware, conforme apontaram Beaumont, Hopkins e Newby (2011) e Swierczynski *et al.* (2015), passando pelo vazamento de informações sensíveis, efeito citado por diversos autores, a exemplo de Beaumont, Hopkins e Newby (2011); Becker *et al.* (2013); Baumgarten *et al.* (2011), Agrawal *et al.* (2007), Karri *et al.* (2010); e Li, Liu e Zhang (2016); ou mesmo ataques de negação de serviço (Denial of Service – DoS), conforme mencionaram Baumgarten *et al.* (2011); Beaumont, Hopkins e Newby (2011); Chakraborty, Narasimhan e Bhunia (2009); e Tehranipoor e Koushanfar (2010). O hardware Trojan pode ser capaz de derrotar qualquer mecanismo de segurança, seja baseado em software ou hardware, subvertendo ou alterando a operação normal de um dispositivo infectado (BEAUMONT, HOPKINS e NEWBY; 2011). O que pode ser feito em milhões de linhas de código (programação de software), em tese, também pode ser feito com milhões de circuitos impressos em CIs (CLARKE e KNAKE, 2015).

Os HTs não são necessariamente implementados objetivando-se um ataque específico e imediato, mas podem apenas "suportar ataques" (KING et al., 2008), a serem ativados por meio de um gatilho (*trigger*) implementado *a posteriori*. Essa possibilidade permitiria uma espécie de infiltração silenciosa na cadeia de fabricação de CIs, dando ao agente a oportunidade de lançar, em momento oportuno, um "ataque de hardware em larga escala" (VILLASENOR, 2010).

Pontos de Inserção do HT

Dentre as fases envolvidas em um típico esquema de fabricação de circuitos integrados, as mais suscetíveis à inserção do HT são o *design* e a manufatura (CHAKRABORTY, NARASIMHAN e BHUNIA, 2009). As possíveis ações maliciosas nessas fases são descritas a seguir (BHUNIA *et al.*, 2014): no *design*, um agente não confiável que esteja envolvido no processo de escrita do bloco IP (*Intellectual Property* ou Propriedade Intelectual, que constitui o desenho lógico de partes ou blocos funcionais do circuito integrado) pode alterar maliciosamente a lógica, inserindo o HT; ainda nesta fase, o uso de softwares do tipo EDA (*Electronic Design Automation*, ferramentas que facilitam o trabalho de *design*) corrompidos também pode resultar na inserção do código malicioso; e, finalmente, na fase de manufatura, é possível comprometer o CI a partir da ação de um agente mal intencionado, utilizando técnicas

de engenharia reversa.

Implementações do HT

Compreendendo que a ameaça existe e é explorada em diversos momentos na fabricação do circuito integrado, é importante entender como ela é criada e se há meios de detectá-la.

Conforme Becker *et al.* (2013), os esforços de pesquisa concentram-se basicamente em duas áreas: uma relativa ao *design* e implementação do HT; e outra lidando com o desafio de detectar a ameaça.

A seguir, serão apresentados casos de implementação do HT. Em seção posterior, detalhes e possibilidades de detecção e prevenção serão abordadas.

King *et al.* (2008) apresentaram uma forma combinada de ataque envolvendo hardware e software. Neste ataque, um hardware Trojan implementado no CI dá suporte para um ataque por meio do software, ao permitir que o agente malicioso tenha acesso privilegiado (*root*) ao sistema operacional (KRIEG *et al.*, 2013). Tal implementação permite ataques poderosos e de propósito geral, embora utilize pequena quantidade de hardware adicional no circuito (KING *et al.*, 2008). Shiyanovskii *et al.* (2009) apresentaram um HT que implementa um ataque de negação de serviço (Denial of Service - DoS) ao degradar a performance do *chip* de forma gradual. As modificações podem manter os parâmetros iniciais de performance dentro dos padrões aceitáveis de variação, dessa forma permanecendo indetectável pelos testes tradicionais.

A viabilidade de inserção de hardware malicioso em circuitos mapeados em *Field-Programmable Gate Array* (FPGAs[5]) foi discutida por Chakraborty *et al.* (2013). Em particular, os pesquisadores se utilizaram de um HT baseado em um anel-oscilador[6] capaz de reduzir o tempo de vida do *chip* através do aumento da temperatura de operação do circuito.

Em Subramani *et al.* (2017), estudou-se a possibilidade de um ataque de HT em redes *wireless* a partir da infecção de um transmissor 802.11a/g, permitindo ao agente malicioso o vazamento de informações sensíveis na conexão.

Neste artigo, uma implementação específica será abordada com mais detalhes, de forma a demonstrar potencialidades e complexidades da ameaça: o chamado "*Stealthy Dopant-Level Hardware Trojan*" (hardware Trojan furtivo implementado no nível do dopante), proposto por Becker *et al.* (2013).

Trata-se de um HT com duas características peculiares: ele é furtivo ou dissimulado, o que significa que sua detecção não é possível pelos meios convencionais; e ele é implementado no nível do "dopante", ou

5 *Field-Programmable Gate Array*, ou Matriz de Portas Programáveis em Campo, é uma espécie de CI projetado para ser programado após a manufatura. Dessa forma, ele possui blocos lógicos reprogramáveis passíveis de configuração em campo, ou seja, pelo consumidor ou projetista após a fabricação (KRIEG *et al*., 2013).

6 Um anel-oscilador é um circuito serial com número ímpar de portas lógicas e com retorno na entrada. A frequência resultante é uma função do número de portas, da temperatura, dentre outros (KRIEG *et al.*, 2013).

seja, utiliza-se do processo de dopagem do semicondutor.

Conforme Pikma (2013), o processo de dopagem envolve a adição de impurezas no material semicondutor, modificando suas propriedades elétricas. Por exemplo, a adição de átomos de Fósforo ao silício puro atribui-lhe polaridade negativa, enquanto que a adição de átomos de Boro cria polaridade positiva. Esse processo de dopagem é um recurso comumente utilizado na fabricação de transistores que compõem o circuito integrado.

A questão aqui é que o agente malicioso se utiliza desse mesmo procedimento para a implementação do HT, ou seja, ao manipular as polaridades dos transistores presentes no circuito integrado, é possível criar uma lógica maliciosa no funcionamento do CI.

Utilizando-se dessa técnica, Becker *et al.* (2013) provaram que é possível reduzir a segurança dos números aleatórios gerados pelo *Random Number Generator* - RNG (Gerador de Números Randômicos) dos processadores *Ivy Bridge* da Intel (linha de processadores de 22 nanômetros da marca americana), a partir da implementação de códigos maliciosos por meio de dopantes. O RNG do *chip* Intel é uma implementação embarcada no hardware que produz números randômicos de 128 *bits* a partir de ruídos termais. Os números são usados em processos criptográficos.

Com a ação do hardware Trojan, ou seja, com a implementação da lógica maliciosa na fabricação do CI, foi possível reduzir a complexidade da saída do RNG de 128 *bits* para "n" *bits*, no qual "n" pode ser definido pelo atacante, a depender do número de transistores modificados. Essa possibilidade constitui uma importante quebra de segurança na funcionalidade do CI.

Observa-se, ainda, que a ação é possível a partir de modificações em poucos transistores. Em uma das implementações, os autores modificaram apenas 896 transistores (dentre os milhões existentes no *chip*).

Tal tipo de implementação, como mencionado, é extremamente difícil de ser detectada. Conforme se concluiu no estudo conduzido por Pikma (2013), uma vez que o *layout* e a fiação do circuito permanecem exatamente os mesmos quando comparados a um CI não infectado, e considerando que a única diferença está no nível atômico do substrato do semicondutor, esse tipo de HT escapa às formas tradicionais de detecção, como a inspeção ótica, os testes funcionais, ou mesmo a inspeção por uso de *golden chips* (CIs não infectados usados como modelos para comparações).

Caso Síria – Uma Implementação Real?

Em 6 de setembro de 2007, aviões israelenses F-15 Eagle e F-16 Falcon entraram no espaço aéreo Sírio, vindos da Turquia, e bombardearam o que seriam instalações nucleares projetadas pela Coreia do Norte. A imprensa chegou a divulgar ainda suposto envolvimento dos EUA no ataque (CLARKE e KNAKE, 2015).

Não obstante as complexas implicações políticas do episódio, o que chamou a atenção foi o fato de que o sistema de defesa

antiaérea da Síria permaneceu inoperante na ocasião, o que permitiu que os aviões de ataque entrassem e saíssem sem serem alvejados. A Síria havia investido milhões de dólares nos sistemas de defesa antiaérea comprados da Rússia.

Pesquisadores vem trabalhando a hipótese de que o sistema antiaéreo sírio estaria infectado com alguma espécie de *backdoor*[7] inserido nos chips do sistema (QAMARINA, 2017). Cogita-se ainda a hipótese de ter sido, de fato, um hardware Trojan implementado nos sistemas sírios (LI, LIU e ZHANG; 2016). Em outro artigo, Moein *et al.* (2016) destacam a possibilidade de microprocessadores comerciais *off-the-shelf*[8] terem sido adquiridos com um *backdoor* utilizado para desativá-los no momento oportuno. Ou seja, a falha teria sido intencionalmente ativada por meio de um gatilho (*trigger*), em momento definido pelo atacante, conforme defenderam XIAO *et al.* (2016).

A Relevância do Tema para as Atividades de Inteligência

A Política Nacional de Inteligência - PNI (BRASIL, 2016), documento de mais alto nível de orientação da Atividade de Inteligência no Brasil, estabelece, dentre outros, pressupostos, objetivos, instrumentos e diretrizes no âmbito do Sistema Brasileiro de Inteligência (SISBIN).

Neste contexto, declara as principais ameaças às quais o país se sujeita, dentre elas: a espionagem; a sabotagem, sobretudo às infraestruturas críticas do país; e os ataques cibernéticos.

O documento ainda acrescenta que o desenvolvimento das tecnologias da informação e das comunicações impõe a atualização permanente de meios e métodos, obrigando os órgãos de Inteligência a resguardar o patrimônio nacional de ataques cibernéticos.

De fato, conforme demonstrado ao longo do artigo, são inúmeras as possibilidades de ação por meio do uso de HT. Pode-se direcionar um ataque para o vazamento de informações de redes de comunicação na área de defesa ou Inteligência, o que traria graves consequências para a segurança nacional, conforme pontuou Villasenor (2013). Ações de sabotagem ou disrupção de operações militares são possíveis, conforme analisaram Anderson, North e Yiu (2008). A proteção das infraestruturas críticas é estratégica e fundamental para o funcionamento do país (CARUZZO, ZAWADZKI e BELDERRAIN; 2015), e a ação de HTs pode ameaçar todo o sistema de infraestruturas críticas, tais como sistemas financeiros e militares (ALIYU *et al.*, 2014). Enfim, tais inclusões maliciosas de fato agem como "espiões ou terroristas" no CI, e podem ser extremamente poderosas, com consequências catastróficas em diversas aplicações (BHUNIA *et al.*, 2014).

7 O *backdoor* é uma espécie de *malware* que, após incluído em um sistema, é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado (CERT.BR, 2017).

8 Componentes eletrônicos prontos, de prateleira, com acesso direto para aquisições (KRIEG *et al.*, 2013).

Assim, estamos diante de um instrumento poderoso e potencialmente utilizado em ações de espionagem, sabotagem e ataques cibernéticos, ações essas cujo enfrentamento encontra-se devidamente declarado nas diretrizes da PNI (BRASIL, 2016).

Além disso, a natureza furtiva do HT permite uma infiltração silenciosa, cuja detecção, conforme veremos a seguir, é extremamente complexa, o que o torna um instrumento importante em ações de inteligência.

Detecção e Prevenção do HT e os Desafios da Contrainteligência

As Atividades de Contrainteligência objetivam prevenir, detectar, obstruir e neutralizar a inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado (BRASIL, 2016).

Dessa forma, no contexto do hardware Trojan, as ações de Contrainteligência podem, em tese, atuar antes da inserção do circuito malicioso – na prevenção; e após a ameaça ter se instalado, através da detecção. Neste tópico, serão analisadas as possibilidades e os desafios envolvidos na detecção e na prevenção da ameaça.

Conforme visto, a inserção do HT é possível em diversas fases da criação do CI. Segundo Abramovici e Bradley (2009), não há métodos confiáveis que garantam a detecção de HT antes da utilização efetiva do *chip*. Não há uma solução mágica para detectar todos os tipos de HT (BEAUMONT, HOPKINS e NEWBY; 2011). Assumindo que o atacante pode maliciosamente alterar o *design* antes e após a manufatura, tem-se que a detecção de tais alterações é extremamente difícil, por diversas razões (TEHRANIPOOR e KOUSHANFAR, 2010).

Primeiro, dada a quantidade e a complexidade dos IP cores utilizados nos CIs, detectar pequenas modificações no circuito é extremamente complexo.

Segundo, as características nanométricas dos CIs fazem com que detecções por meio de inspeção física ou engenharia reversa (destrutiva) sejam muito difíceis e caras. Ainda, a engenharia reversa destrutiva (feita em uma amostra) não garante que os demais CIs estejam livres do HT, em especial quando os Trojans são inseridos seletivamente em determinada porção da população de *chips*.

Terceiro, circuitos de HT são geralmente ativados sob condições muito específicas (WANG, TEHRANIPOOR e PLUSQUELLIC; 2008), por exemplo, detectando um sinal específico, como temperatura ou potência, o que os fazem improváveis de serem ativados ou detectados por meio de estímulos funcionais ou randômicos (TEHRANIPOOR e KOUSHANFAR, 2010).

Quarto, testes utilizados para detectar falhas de manufatura, como falhas de atraso (*delay*) não garantem a detecção dos Trojans. Tais testes operam no nível do *netlist* [9] de circuitos livres do Trojan e, consequentemente, não

9 Descrição da conectividade de um circuito eletrônico, conforme Krieg *et al*. (2013).

são capazes de ativar ou detectar os HTs.

Finalmente, uma vez que o tamanho das características físicas de CIs vem se reduzindo em virtude de aprimoramentos na técnica de litografia (processo que imprime a imagem do circuito), variações no processo e no ambiente tem um impacto cada vez maior na integridade da parametria dos circuitos. Assim, a detecção de HT utilizando simples análise desses sinais paramétricos seria inefetiva (TEHRANIPOOR e KOUSHANFAR, 2010).

Assim, há variadas técnicas para a detecção do HT, mas são apenas capazes de detectar classes específicas de Trojan. É de se esperar, como ocorre com os *malwares* de software, que os agentes que projetam HT tentarão escapar de técnicas já conhecidas de detecção, de forma a ter sucesso em seus objetivos (BEAUMONT, HOPKINS e NEWBY; 2011).

Por outro lado, as ações de prevenção buscam impedir que a inserção do HT ocorra. Xiao *et al.* (2016) mencionam três tipos de técnicas de prevenção: ofuscação lógica, que consiste em esconder a funcionalidade genuína de um circuito inserindo mecanismos de bloqueio no *design* original, impedindo portanto que o atacante conheça a lógica (genuína) do circuito, condição necessária para que se projete a lógica maliciosa; camuflagem, um tipo de estratégia de ofuscação no nível do *layout* físico, que consiste na adição de contatos e conexões falsas, dessa forma "enganando" o atacante e impedindo que se extraia a *netlist* correta; e abordagens de preenchimento total de células no circuito, de forma a não deixar espaços vagos no *design*, que poderiam ser utilizados para a inserção do HT.

De fato, não existe uma solução única, que possa garantir proteção segura contra todos os tipos de HT (BHUNIA *et al.*, 2014). No entanto, estratégias que combinem prevenção e detecção podem ser interessantes em cenários que envolvam sistemas críticos e informações sensíveis.

Conclusões

O potencial lesivo do hardware Trojan é preocupante, com ações que incluem vazamento de dados, espionagem, ataques de indisponibilidade, disrupção de sistemas, sabotagem, dentre outros.

O fenômeno envolve uma quebra importante de paradigma na área cibernética, dado que comumente as ameaças são baseadas em software, e não em hardware, em que geralmente a confiabilidade é uma premissa.

Constata-se que o fenômeno hardware Trojan vem preocupando os governos de diversos países, notadamente por envolver, no contexto da guerra cibernética, delicadas questões de espionagem e soberania. De forma geral, países vêm tentando lidar com a ameaça e mitigar os riscos associados, uma vez que o problema não pode ser totalmente eliminado.

O fenômeno traz ainda importantes implicações no contexto das Atividades de Inteligência e da segurança cibernética. A perda de controle na cadeia de fabricação de circuitos integrados, consequência de um modelo forçosamente globalizado por questões de viabilidade econômica, aliada ao crescimento da complexidade dos *chips*, trouxeram relevantes desafios não só para a prevenção da ameaça, como para a sua

detecção.

Como a grande maioria dos sistemas críticos de um país é baseada em arquiteturas que utilizam a Inteligência de circuitos integrados, a ameaça pode trazer relevantes prejuízos para a segurança nacional, devendo ser considerada no âmbito das ações e objetivos das Atividades de Inteligência.

Referências

ABRAMOVICI, Miron; BRADLEY, Paul. *Integrated circuit security: new threats and solutions.* Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies (CSIIRW 09), p. 0–2, 2009.

AGRAWAL, Dakshi; BAKTIR, Selcuk; KARAKOYUNLU, Deniz; ROHATGI, Pankaj; SUNAR, Berk. *Trojan detection using IC fingerprinting.* Proceedings - IEEE Symposium on Security and Privacy, p. 296–310, 2007.

ALIYU, A.; BELLO, A.; MOHAMMED, J.; ALHASSAN, I. H. Hardware Trojan Model For Attack And Detection Techniques. In: *International Journal of Scientific & Technology Research,* 2014.

ANDERSON, M. S.; NORTH, C. J. G.; YIU, K. K. *Towards Countering the Rise of the Silicon Trojan.* Command, Control, Communications and Intelligence Divison. Australian government, 2008.

BAUMGARTEN, Alex; STEFFEN, Michael; CLAUSMAN, Matthew; ZAMBRENO, Joseph. A case study in hardware Trojan design and implementation. In: *International Journal of Information Security,* 10(1):1–14, 2011.

BEAUMONT, Mark; HOPKINS, Bradley; NEWBY, Tristan. *Hardware Trojans - Prevention, Detection, Countermeasures (A Literature Review).* Command, Control, Communications and Intelligence Division. Australian government, 2011.

BECKER, Georg T.; REGAZZONI, F.; PAAR, C.; BURLESON, Wayne P. *Stealthy dopant-level hardware Trojans:* Cryptographic hardware and embedded systems, CHES 2013, p. 197–214, 2013.

BHUNIA, S.; HSIAO, Michael S.; BANGA, M.; NARASIMHAN, S. Hardware trojan attacks: threat analysis and countermeasures. In: *Proceedings of the IEEE,* v.102, p. 197–214, 2014.

BRASIL. *Política Nacional de Inteligência (PNI)*. Decreto n° 8.793/2016, Brasília-DF, 2016.

CARUZZO, A.; ZAWADZKI, M.; BELDERRAIN, M. *Proteção de Infraestruturas Críticas: desafios da previsão meteorológica como ferramenta de apoio aos Serviços de Inteligência. Revista* Brasileira de Inteligência, Brasília, ABIN, v.9, 2015.

CERT.BR. *Cartilha de Segurança para Internet:* Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <cartilha.cert.br>. Acesso em: 01 out. 2017.

CHAKRABORTY, R. S.; SASHA, I.; PALCHAUDHURI, A.; NAIK, G. K.: *Hardware trojan insertion by direct modification of FPGA configuration bitstream*. IEEE Design and Test, 30(2), 2013.

CHAKRABORTY, R. S.; NARASIMHAN, S.; BHUNIA, S. *Hardware trojan: Threats and emerging solutions*. IEEE, 2009.

CLARKE, Richard A.; KNAKE, Robert K. *Guerra Cibernética:* A Próxima Ameaça à Segurança e o que Fazer a Respeito. São Paulo: Brasport, 2015.

FLOYD, Thomas L. *Digital Fundamentals*. 11 ed. England: Pearson, 2014.

GOERTZEL, K. M.: Integrated circuit security threats and hardware assurance countermeasures. In: *The Journal of Defense Software Engineering,* p. 33–38, 2013.

IQBAL, Asif: *Understanding Integrated Circuit Security Threats*. Disponível em: <sdm.mit.edu/news/news_articles/webinar_021014/iqbal_021014.pdf>. Acesso em:09 set. 2017.

KARRI, Ramesh; RAJENDRAN, Jeyavijayan; ROSENFELD, Kurt. *Trustworthy hardware: Identifying and Classifying hardware Trojans*. IEEE Computer Society, p. 39–46, 2010.

KING, S. T.; TUCEK, J.; COZZIE, A.; GRIER, C.; JIANG, W.; ZHOU, Y. Designing and implementing malicious hardware. In: *Proceedings of the 1st Usenix workshop on large-scale exploits and emergent threats,* 2008.

KRIEG, Christian; DABROWSKI, Adrian; HOBEL, Heidelinde; KROMBHOLZ, Katharina; WEIPPL, Edgar. *Hardware Malware*. Synthesis Lectures on Information Security, Privacy, and Trust. Williston, USA: Morgan & Claypool Publishers, 2013.

LI, He; LIU, Qiang; ZHANG, Jiliang. *A survey of hardware trojan threat and defense*. Integration, the VLSI journal, 2016.

MCCORMACK, Richard. *$600 Million Over 10 Years For IBM's 'Trusted Foundry' Chip Industry's Shift Overseas Elicits National Security Agency, Defense Department Response.* Manufacturing & Technology News, v. 11, n. 3 (Feb. 3, 2004). Disponível em: <www.manufacturingnews.com/news/04/0203/art1.html>. Acesso em: 16/10/2018.

MOEIN, Samer; GULLIVER, Thomas A.; GEBALI, Fayez; ALKANDARI, Abdulrahman. *A New Characterization of Hardware Trojans.* IEEE Access, 4:2721–2731, 2016.

PIKMA, T.: *Stealthy dopant-level hardware trojans.* In: Research Seminar in Cryptography, 2013.

QAMARINA, Nur; NOOR, Mohd; NUR, Nilam; SJARIF, Amir; HUDA, Nurul; MOHD, Firdaus; DAUD, Salwani M. Hardware Trojan Identification Using Machine Learning-based Classification. *Journal of Telecommunication, Electronic and Computer Engineering Result.* 9(3):23–27, 2017.

RAJENDRAN, J.; GAVAS, E.; JIMENEZ, J.; PADMAN, V.; KARRI, R. Towards a comprehensive and systematic classification of hardware trojans. In: *Proceedings of 2010 IEEE International Symposium,* p. 1871–1874. New York, USA, 2010.

RAWNSLEY, Adam. *Can DARPA Fix the Cybersecurity Problem From Hell?*. Disponível em: <www.wired.com/2011/08/problem-from-hell/>, 2011. Acesso em: 2017-11-22.

SANCHEZ, Julio: *Metodología para la Investigación en Marketing y Dirección de Empresas.* Ed. Pirámide: Madrid, 1999.

SHIYANOVSKII, Y; WOLFF, F; PAPACHRISTOU, C; WEYER, D; CLAY, W. *Exploiting Semiconductor Properties for Hardware Trojans.* ACM CoRR, p. 6, 2009.

SUBRAMANI, Kiruba S.; ANTONOPOULOS, Angelos; ABOTABL, Ahmed A.; NOSRATINIA, Aria; MAKRIS, Yiorgos. INFECT: INconspicuous FEC-based Trojan: A hardware attack on an 802.11a/g wireless network. In: Proceedings of the 2017 *IEEE International Symposium on Hardware Oriented Security and Trust,* HOST 2017, p. 90–94, 2017.

SWIERCZYNSKI, Pawel; FYRBIAK, Marc; KOPPE, Philipp; PAAR, Christof. FPGA Trojans Through Detecting and Weakening of Cryptographic Primitives. In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 2015.

TEHRANIPOOR, Mohammad; KOUSHANFAR, Farinaz. A survey of hardware trojan taxonomy and detection. In: *IEEE Design and Test of Computers,* 27(1):10–25, 2010.

USA: *Discussion draft of the preliminary cybersecurity framework [report],* 2013.

VILLASENOR, J. *Compromised by design:* Securing the defense electronics supply chain. USA: Brookings Institute, 2013.

VILLASENOR, J: *Ensuring Hardware Cybersecurity.* Electrical Engineering, 2011.

VILLASENOR, J: *The hacker in your hardware.* Scientific American, 303(2):82–87, 2010.

WANG, Xiaoxiao; TEHRANIPOOR, Mohammad; PLUSQUELLIC, Jim. Detecting malicious inclusions in secure hardware: Challenges and solutions. In: *2008 IEEE International Workshop on Hardware-Oriented Security and Trust,* HOST, 1(July):15–19, 2008.

XIAO, K; FORTE, D.; JIN, Y.; KARRI, R.; BHUNIA, S.; TEHRANIPOOR, M. Hardware Trojans: lessons learned after one decade of research. In: *ACM Transactions on Design Automation of Electronic Systems,* 22(1):1–23, 2016.

YOSHIKAWA, M.; TAKEUCHIR, D.; KUMAKI, T. Reset Signal Aware Hardware Trojan Trigger. In: *ICAET,* 2014 (pp. 528–531).