STRATEGIC BUSINESS INSIGHTS

scan™

2021 年 4 月

SoC1225

The Impossible Challenge of Hardware Verification

By Katerie Whitman（Send us feedback）

ハードウェアの検証という難題

国や企業はもはや、自分たちが使っているコンピューター・ハードウェアに、セキュリティや機能を損なう隠れた回路が入ることなどないとは思っていない。この信頼の欠如から、中国の電子機器メーカーでは、技術の輸出入制限や投資の禁止、またはその両方を行う貿易制裁により、莫大な収益減となっている。アメリカやイギリスなど、危険なハードウェアが入っているとして中国のエレクトロニクス製品を禁止・制限している国と中国との溝は、この信頼の欠如によって深まる一方だ。それはまた、危険なハードウェアの問題を技術的に解決しようという新たな産業の誕生にも一役買っている。しかし残念ながら、そうした解決策がこの問題との闘いに効力を発揮することはなさそうだ。

国や企業はもはや、自分たちが使っているコンピューター・ハードウェアに、セキュリティや機能を損なう隠れた回路が入ることなどないとは思っていない。

ハードウェア「トロイの木馬」（HT）とは、コンピューターチップや電子機器に密かに入り込み、その機器のセキュリティを損なう回路部品を指す専門用語である。いったん機器に組み込まれると、コンピューターウィルスといったソフトウェア・ベースの同等物と同じように機能し始める。こうなると、感染した機器が接続している（グローバルインターネットなどの）ネットワークにアクセス可能な悪意の行為者は、遠隔アクセスによるコマンドで機密データを送らせたり、財産や生命を危うくするように機器の機能を変更したりできてしまう。ネットワークに接続していない機器でも、隠れた回路に設定済みのトリガーによって誤作動を起こす可能がある。

コンピューターウィルスやソフトウェア・ベースの「トロイの木馬」では、コード解析で「トロイの木馬」の有無を判断したり、「トロイの木馬」によるデータへのアクセスや重要な機能への影響を制限したりといった、さまざまな防御策が考えられる。しかし、相手が HT となるとうまく機能しないか、まったく用をなさない。HT はソフトウェアの動作に影響を及ぼすため、組み込まれたデバイス上で動くどのソフトウェアからも、容易にその存在が隠せるからである。同様に、HT は自らが構成するハードウェアからも電子的に隠れることができるので、ハードウェア・ベースの手段で HT の存在を簡単に検出することもできない。

HT の検出方法は存在するものの、実施が非常に難しく、特別な装置も必要とされる。コンピューター・ハードウェアにさまざまな入力信号を与えて出力信号を記録し、両方の信号を基準装置に照らし合わせて異常がないか確認する方法もある。しかし、コンピューター・ハードウェアは現在きわめて複雑化し、この方法ではあまり効果が期待できない。より確実な方法では、コンピューターチップの外側のコーティングを物理的に剥がして回路を露出させ、それを電子顕微鏡で観察して基準設計と比較し、異常を確認する。とはいえ、こうした方法にも問題がある。昨今のコンピューターチップはきわめて複雑化し、製造過程でどうしても各チップ間に不整合が生じてしまうのである。

こうした課題に対処するため、東芝はチップの回路トレースに HT が存在しているかの検査過程を自動化するソフトウェアを開発した。これまでに HT の一部と判明している 9 種類の回路設計をスキャンし、機械学習で新たな HT がチップに含まれているかを予測

するものだ。しかし残念ながら、このソフトウェアでは物理的にチップの回路トレースを検査しなければならず、チップを破壊しないと実施できないらしい。ソフトウェアの効果を得るにはチップを東芝に送って検査してもらう必要があり、2 週間と 2 万ドル近くかかるという難点がある。

東芝の新サービスは HT の存在を検査する数少ない例のひとつで、そうした検査に特化した新たな産業の先駆けになるかもしれない。こうしたサービスは通常、チップを検査して偽造品かを判断する研究所で行われており、専門のサービスとして広く提供されてきたわけではない。東芝が用いた技術を開発したのは早稲田大学で、同大学では(破壊検査ではなく)信号解析による HT 検出法にも取り組んでいる。この他にも HT の問題に取り組んでいる研究者は少なくない。

検出方法がそれだけ優れたものになっても、HT の検査には「一度に複数のチップを検査できない」という致命的な欠陥がある。たとえあるチップが陰性だと判定されても、世界中で既にデバイスに組み込まれているそのチップの数百万のコピーのどれか 1 つが感染するかもしれないのだ。チップの HT を検出しても、せいぜい特定の生産工程やサプライヤーが危険にさらされると分かるだけで、そのチップの例がすべて安全だという保証にはならない。

こうした理由から、コンピューター・ハードウェア業界では、チップのサプライチェーンを非常に厳格に管理することが最善慣行となっている。こうした慣行は軍事業界では古くから行われてきたのだが、商用ハードウェアで一般化したのはごく最近のことだ。Bloomberg Businessweek 誌が 2018 年、大手ハイテク企業のサプライチェーンに、中国の工作員が HT を忍ばせたデバイスが入り込んでいたと報じて物議を醸して以来、欧米諸国は一気に中国メーカーの電子機器を禁止し出したが、その動きはここ数か月でさらに強まっている。こうした禁止措置は、半導体や安全保障の関連業界の専門家のあいだでは、HT 問題への過剰反応だと言われている。その是非はともかく、禁止措置は今後も継続されると思われ、すでに世界の電子機器サプライチェーンに多大な影響を与えている。

SoC1225

本トピックスに関連する Signals of Change		関連する Patterns	
SoC1215	フィンランドにおけるイノベーションの探求	P1525	イーグルとパンダの綱引き
SoC1054	オンチップのAI	P1512	サプライチェーンのレジリエンス？
SoC1041	消費者のテクノロジーに対する不安への対処	P1311	中国によるエレクトロニクスの支配を危・・・