先端技術キーワード解説

知っておきたい最新の動き

[CET（Control-Flow Enforcement Technology）]

このところ、マルウェアが猛威をふるっています。特に、最恐のマルウェアと言われる「Emotet」は、巧妙に感染を広げています。

そんな中、期待のできそうな技術があります。Intel が、2020 年 6 月、チップレベルの新たなセキュリティ機能である「CET（Control-Flow Enforcement Technology）」を、次世代プロセッサである「Tiger Lake」に搭載すると発表しました。どのようなものなのでしょうか。

１．CET（Control-Flow Enforcement Technology）とは

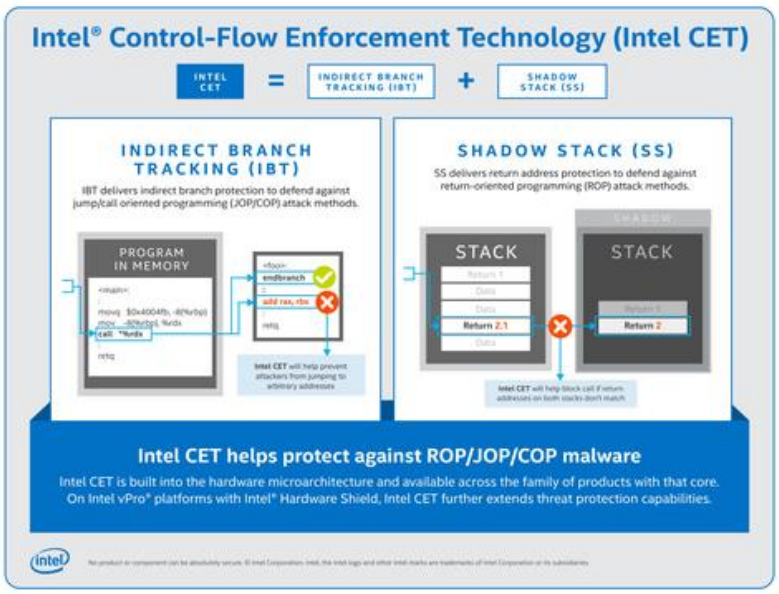
CET はチップレベルのセキュリティ機能です。従来のセキュリティ機能は、ソフトウェアのみで防御していました。CET は、ハードウェア、つまり、チップレベルで防御するため、従来。困難だったマルウェア攻撃からデバイスを保護できるとのことです。

２．CET の防御機能

マルウェアは、そのデバイスに搭載されているアプリケーションソフトの脆弱性を利用して CPU の制御フローを乗っ取ります。そして、悪意のあるコードを実行します。

このとき、実行が許可されている正規のコードを改変することで、プログラムの挙動を変えてしまいます。このため、ソフトウェアによる検出や予防が困難でした。

この攻撃を防ぐために CET は、二つの基本的機能を備えています。



（１）　indirect branch tracking

分岐命令（ジャンプ命令）を悪用したジャンプ指向／呼び出し指向プログラミングジャンプ（JOP/COP : jump/call-oriented programming）攻撃を防ぎます。CPU のジャンプテーブルを使用するソフトの機能を

制限する保護機能です。

（２） shadow stack

リターン（RET）命令を悪用したリターン指向プログラミング（ROP：Return-Oriented Programming）攻撃を防ぎます。アプリケーションソフトが目的とする制御フローのコピーを作り、CPU の安全な領域である shadow stack に格納し、ソフトの実行順序で不正が行われないようにする仕組みです。

３．Microsoft の対応

Intel は Microsoft と緊密に協力しており、「Hardware-enforced Stack Protection（ハードウェア強制型スタック保護）」と呼ぶ CET に対応した機能を Windows 10 に取り込むとしています。

［参考文献］

1）Intel CET Answers Call to Protect Against Common Malware Threats
https://newsroom.intel.com/editorials/intel-cet-answers-call-protect-common-malware-threats/#gs.glpkef

（注）

本解説は、執筆当時の状況に基づいて解説をしております。ご覧になる時には、状況が変わっている可能性がありますので、ご注意をお願いします。

技術・経営の戦略研究・トータルサポータ
ティー・エム研究所
工学博士
中小企業診断士
社会保険労務士（登録予定）
代表　芳賀　知
E-Mail：info_tm-lab@mbn.nifty.com　URL：http://tm-lab@a.la9.jp/