Host Identity Protocol (HIP) とは何か?

IPコミュニケーションのゲームチェンジャー

Dr. Andrei Gurtov, Aalto University, Finland

Andrei Gurtov 氏は、フィンランドヘルシンキ大学でコンピュータサイエンスの学士号 (2000)、博士号 (2004) を取得しました。現在は Helsinki Institute for Information Technology (HIIT) の Principal Scientist であり、IEEE と ACME のシニアメンバーでもあります。

彼はまた、Aalto University、University of Helsinki 及び University of Oulu の非常勤教授でもあり、2010 年から 12 年まで University of Oulu でワイヤレスインターネットの教授も務めていました。最近では、TeliaSonera、Ericsson Nomadic Lab そして University of Helsinki で働き、2003 年、2005 年及び 2013 年にはバークレーの International Computer Science Institute (ICSI) で客員学者も務めました。

Dr. Gurtov は 150 以上の出版物の共著者で、それには 3 冊の本、研究トン分、特許、5 つの IETF RFC が含まれます。彼は IETF で HIP の標準化に貢献し、Internet Research Task Force (IRTF) で HIP Research Group を率い、初期の HIP の実装と配備に関する経験をまとめて RFC 6538 を共同で執筆しました。HIP に関する著作は Communications and Information Systems Security (CIS) の分野で IEEE の「Best Readings」に挙げられています。

I E T F

IEEE

acm

歴史

Host Identity Protocol (HIP) は、(2015年末現在) インターネット標準化過程にあるネットワークセキュリティプロトコルで、2015 年にインターネットの主導的な標準化機関である Internet Engineering Task Force で承認されました。これは、Ericsson、Nokia、Verizon、TeliaSoneraなどの大企業や Trusted Computing Group、IEEE 802 などの標準化団体と共に進めてきた 15 年に及ぶ HIP 開発における最高の瞬間でした。

Internet Engineering Task Force (IETF) は、HIP を IP アーキテクチャの次の大規模な変更と考えています。HIP は、勢いを増すサイバーセキュリティ上の脅威に対抗するための費用対効果の高いスケーラブルなソリューションとして、最初に防衛航空産業での利用が始まりました。このプロトコルは、国家レベルのサイバー攻撃が日常的に行われ、システムが 1 時間ダウンすると 100 万ドルの損失が出るような環境において、10 年以上の実績を誇っています。

技術

HIP は IPsec プロトコルに代わる鍵交換機能を提供するため、TCP/IP アプリケーションは透過的で従来の環境との互換性を保ちながら、高度なセキュリティを実現できます。HIP は識別子とロケーターの分離 (IP アドレスの役割をホスト識別機能とインターネット上のトポロジー的なロケーションに分ける) をコンセプトとし、2048bit の RSA 公開鍵を使って強力に暗号化した識別子を使って、ホストを識別します。ロケーターは IPv4 または IPv6 アドレスですが、ID はホストに紐付けされません。ホストは IP アドレスを変えることができますが、識別子は暗号化されたままです。

HIP は IPv4 及び IPv6 アプリケーションと互換性があり、ネットワークアプリケーションの機密性、認証、完全性のためにカスタマイズされた IPsecトンネルモードを用意しています。

長年にわたって、プロトコルの各ステップを表したステートマシンの厳格な検証を行ってきたため、HIP は強力なセキュリティ属性を持っています。ホストとネットワークデバイスが、一時的な IP アドレスに代わってなりすまし不可能な暗号化された ID を使うことにより、ホストとネットワークのモビリティ、シングルサインオン、マルチホーミングなどを簡単に実装することができます。

TCP と比べ、HIP は最初から DoS 攻撃やマンインザミドル攻撃に強力に対抗できるよう設計されています。暗号化を使った巧みなメカニズムと、鍵生成と認証におけるステートレスなアプローチによって、インターネットを悩ます問題に対処できるのです。

Tempered Networks はどのように HIP を使っているのか

現代のインターネットは、様々なハッカー (アマチュアからサイバー戦争に関与する政府機関のプロフェッショナルまで) が活動する余地を残しています。責任や信頼の所在が不明な上に、IP 及び MAC アドレスを偽装することは簡単です。さらに、パッチの当たっていないコンシューマ PC が放置されており、脅威は確実に高まっています。

外部から隔離した接続 (クローキング) と強力な認証が利用できないと、企業や公共のインフラへの侵入を許してしまい、ユーザーデータや営業秘密が漏洩してしまう恐れがあります。これに対し、多くの企業では、従来型のツール (IDS やファイアウォールなど) を使ってこれを防ごうとしていますが、これはトラフィックを解析するアプローチで、TCP ポートや IP/MAC アドレスは簡単に偽装できるため、効果に

疑問が残ります。これでは流砂の上に家を建てるようなもので、ハッカーが従来型の TCP/IP スタックに新たなエクスプロイトを見つけることを防ぐことはできません。

Tempered Networks は、まったく違うアプローチをとっています。現在のインターネット攻撃の根幹である、ホスト識別子の不在と侵害可能なシステムの放置に注目するのです。暗号化されたホスト ID は、ホストアクセス制御とネットワークトラフィックフィルタリングにおける第一のオペレーショナルユニットとなります。プリンターや工業製品などのような、レガシーなインターネットデバイスにパッチをあてるのは困難なため、Tempered Networks では HIPswitch と呼ばれるゲートキーパーを用意し、IP 接続されるデバイスの前に設置します。ネットワークへの変更は必要ありません。

静的なフィルタリングルールを使う従来型のファイアウォールや、全てのトラフィックをトンネル化する IPsec ゲートウェイと違い、HIPswitch はもっと強力なアプローチをとります。HIPswitch はパブリックインターネット上にセキュアなトンネルを作って、脆弱なユーザートラフィックを安全に送信することができます。そしてその際に、暗号化された識別子を使ってホストをホワイトリスト化して、そのトンネルの利用を管理します。そのため、認証されていない、悪意のあるトラフィックを排除できるのです。

ネットワークを信頼関係に基づく小さなセグメントに分離することにより、Tempered Networks は脆弱なインフラを外部から完全に隠蔽します。その際、各々のデバイスをアップデートするなどの作業は必要ありません。隠蔽されるデバイスは、他のネットワークからは見えず、検知もできません。強力でスケーラブルなマネジメントインターフェースにより、インターネットコミュニケーションを簡単かつ効率的に保護できるのです。現在、様々な企業が HIP を採用した製品を出荷していますが、Tempered Networks の製品が最も成功しています。

サイバーセキュリティへの影響

HIP を使うことにより、現代の既知の脅威に対するネットワークセキュリティのレベルを上げることができます。事実、ボーイング社のアーキテクトで OpenGroup に所属するセキュリティエキスパートの Richard Paine は、HIP の導入について書籍を著しています。

“Beyond HIP: The End to Hacking as We Know It.” (HIP を超えて: ハッキングの終焉)

強力な暗号を使ったホスト ID により、HIPswitch は非認証トラフィックを完全にフィルタでき、DoS 攻撃やなりすまし攻撃の危険を無くすことができます。ミリタリーグレードの AES-256 暗号化と、データパケットの SHA-256 認証を組み合わせることにより、インターネット上の最も有能な攻撃者であっても、HIP トラフィックをクラックすることはできません。

レイヤー 4 セキュリティ (SSL) を使った VPN とは違い、HIP はネットワークのプロトコルスタックレベルでのセキュリティを実現しており、既知のアプリケーションレベルの攻撃によるリスクを軽減します。SSL は TCP トランスポートプロトコルの上で動作するため、SYN flood 攻撃や TCP リセット攻撃に対して脆弱で、非常に危険です。悪意のあるユーザーが、TCP レベルの弱点を使って安全なセッション割り込むことができるのです。さらに、SSL は証明書の認証を公的な組織に頼っているため、ルート CA が侵害された場合に信頼性を失う可能性があります。攻撃者は SSL/TLS プロトコルを侵害することで、通信の信頼性と完全性を侵害することができるだけでなく、DDoS 攻撃をも可能にします。

新たなサイバーセキュリティ環境

HIP は最高レベルのネットワークセキュリティを可能にしますが、かつては導入に困難が伴いました。大きな問題の一つは、HIP ミドルボックスデバイスのルール設定が難しかったことです。XML ファイルを手作業で編集し、それを複数のデバイス間で同期させなければならなかったのです。

Tempered Networks は、この問題を解決しました。集中化した使いやすい GUI を使ってユーザーデバイスを信頼リストに簡単に追加したり、削除したりできます。使い勝手はセキュリティソリューションにとって常にアキレス腱です。簡単な管理機能を持ったオールインワンプラットフォームにより、Tempered Networks がこの問題を解決したのです。

Tempered Networks のソリューションは、航空機製造、社会インフラ、石油・ガス、発電などのミッションクリティカルな産業分野で活用されており、一般企業での導入も進んでいます。例えば、サポート切れの Windows XP を使ったチケット発行機を分離する用途などに使われます。Tempered Networks のプラットフォームがユニークなのは、それが安全な接続を提供する目的で設計されており、活用分野はお客様によって日々広がっていると言うことです。

今後、このセキュアなアーキテクチャは、様々な分野で活用されて行くでしょう:

- スマートグリッドによる電力の自家発電と共有
- データセンター同士の接続とソフトウェアデファインドネットワーク (SDN) による集中管理
- 工業機械のセンサーからの大量のデータをクラウドベースでデータマイニングと学習し、製造業を革新

多くの専門家が、産業機械の接続性にとって、サイバーフィジカルシステムのセキュリティが普及の障害になっていると言っています。そのため、Tempered Networks のソリューションには大きなチャンスがあります。

この他にも、小さなセンサーのセットで安全性を確保するという Tempered Networks の方向が IoT の分野でどう受け入れられるか、大規模な導入でのブリッジングのスケーラビリティとオーバーヘッドがどのようなものか、ブリッジの管理に階層構造をとるのかなど、研究者としての興味は尽きません。

TEMPERED NETWORKS®

http://temperednetworks.jp

info_Japan@temperednetworks.com