2015 年 2 月 26 日
株式会社日立製作所

サイバー攻撃の侵入経路を考慮したセキュリティリスク評価技術を開発

リスク評価の容易化によりセキュリティ対策の迅速化とコスト低減を実現

株式会社日立製作所(執行役社長兼 COO:東原 敏昭/以下、日立)は、このたび、ソフトウェアの脆弱性に対する攻撃リスクを自動的に算出し、対策優先度を提示することで、情報システム管理者による迅速な対処を支援するセキュリティリスク評価技術を開発しました。本技術により、サイバー攻撃の進入経路の推定や脆弱性対策の優先度付け等の処理を自動化することで、高度な情報セキュリティスキルを持たないシステム管理者でも容易かつ迅速に対策を行えるようになるほか、脆弱性対策に関わるコスト低減を実現します。典型的な WEB システム[*1]の場合、一般的な方法と比較して対策すべき脆弱性の数を約 1/3 まで絞り込む[*2]ことが可能となります。

近年、ソフトウェアの脆弱性を狙ったサイバー攻撃の脅威が高まっています。セキュリティ情報公開機関(米国 NIST[*3]や IPA[*4]など)は、昨年約 8,000 件の脆弱性情報を公開しています。その中でも、「Heartbleed」[*5]や「ShellShock」[*6]と呼ばれる脆弱性は影響範囲の大きさから、高い関心を集め、特に「Heartbleed」の場合、脆弱性情報を公開した直後から、同脆弱性を狙った攻撃が急増したため、迅速な対処が求められました。このような場合、脆弱性の性質や保護対象となるシステムの構成などに基づき、サイバー攻撃の侵入経路を想定して、優先的に対処すべき脆弱性を特定する必要があり、高度な情報セキュリティスキルが必要となります。しかし、個々の組織でそのような専門家の確保や育成は困難な状況でした。

そこで、日立は、公開された脆弱性情報と保護対象とするシステム構成情報(ソフトウェア情報、ネットワーク構成情報)から、自動的にシステムの各機器が持つ脆弱性を特定した上で、そのシステムに想定される侵入経路を推定し、脆弱性対策の優先度付けを行う技術を開発しました。

今回開発した技術の特徴は以下の通りです。

(1)脆弱性情報とシステム構成情報に基づく脆弱性の有無を特定する技術

公開されている脆弱性情報には、脆弱性の内容とともに対象となるソフトウェアの識別子[*7]が記載されています。このソフトウェア識別子と、既存の構成管理ツール等により機器から取得できるソフトウェア名称は一致しないことがあったため、機器に内在する脆弱性を機械的に特定することが困難でした。そこで、日立は、機器から取得したソフトウェア名称とソフトウェア識別子の類似度を算出することで、公開脆弱性情報との突き合わせを可能とし、脆弱性の有無を自動的に特定する技術を開発しました。本技術により、大量に公開される脆弱性情報から、大規模なシステムを構成する多数の機器に内在する脆弱性を迅速に特定することが可能となります。

(2)サイバー攻撃の侵入経路を考慮したリスク定量化技術

組織を狙ったサイバー攻撃では、システムに内在する脆弱性を次々に狙うことにより侵入範囲の拡大を図ります。通常は、外部から直接アクセスできない機器の脆弱性も、一度システムに侵入されてしまうことで危険に晒されることがあります。そのため、脆弱性がもたらすリスクは、その機器への侵入経路の有無やその経路の侵入確率によって変動します。そこで、日立は、システムのネットワーク構成情報からサイバー攻撃の到達可能性を自動解析し、各システムにおいて侵入可能な経路を網羅的に抽出する技術を開発しました。さらに、これらの侵入経路をベイジアンネットワーク*8 で解析可能な有向非巡回グラフ*9 化する方式を考案しました。この方式により、各経路における侵入確率と、各脆弱性の影響度を算出します。機器ごとの脆弱性の有無だけでなく、各脆弱性のリスクを定量的に評価することで、その脆弱性対策の優先度付けを的確かつ一律に行うことが可能となります。これにより、情報システムの管理者によるセキュリティリスク評価の容易化と脆弱性対策の迅速化を支援します。

なお、開発した本技術は、2015 年 3 月 5 日～6 日に法政大学にて開催される第 68 回コンピュータセキュリティ研究会(CSEC)で、詳細を発表する予定です。今後は、セキュリティ運用の支援サービスとして、提供できるように開発を進めていきます。

また、ソフトウェアの脆弱性対策の重要性は、情報システムに留まらず、制御システムのコンポーネントでも拡大しており、日立は、本技術を社会インフラシステムに活用し、安全・安心な社会の実現に貢献していきます。

*1 Web3 階層システムの典型的な構成における評価。
*2 2014 年に公開された脆弱性情報を対象とした標準的な脆弱性特定方法との比較。
*3 NIST: National Institute of Standards and Technology. 米国商務省配下の国立標準技術研究所。
*4 IPA: Information-technology Promotion Agency. 経済産業省所管の独立行政法人。情報処理推進機構とも呼ばれる。
*5 Heartbleed: 暗号化ソフトウェア「OpenSSL」に潜んでいた脆弱性の一つ。2014 年 4 月に公開され、暗号鍵やパスワード等の情報漏洩の脅威が顕在化した。
*6 ShellShock: UNIX 系 OS におけるコマンド実行環境「GNU Bash」に潜んでいた脆弱性の一つ。2014 年 9 月に公開され、リモートから悪意のあるコードが実行される脅威が顕在化した。
*7 ソフトウェア固有の識別子: ソフトウェアを曖昧さなく区別するための名前や番号。公開された脆弱性情報では、NIST が管理する標準化されたソフトウェア識別子が利用されている。
*8 ベイジアンネットワーク: 様々な原因と結果の関係性を記述したグラフから、発生し得る現象を確率的に推論するモデル。
*9 有向非巡回グラフ: 方向性のある矢印を用いて、様々なモノの関係性を抽象化したグラフ。ベイジアンネットワークを用いた確率推論では、関係性がループしない、“非巡回“のグラフである必要がある。

■お客様お問い合わせ先
株式会社日立製作所 横浜研究所 企画室 [担当:吉田]
〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地
電話:050-3135-3409 (直通)

以上