



TOPIC VoIP の脆弱性を理解する

あなたの VoIP の実装がどれくらい脆弱か

長い間、テレコミュニケーションネットワークと電話サービスは、クリティカルな情報インフラの一部でした。そこには常に、可用性と Quality of Service (QoS) に対する高い要求がありました。

VoIP (Voice over Internet Protocol)、もしくは IPTel (IP Telephony) の出現は、新しいネットワークに電話サービスをもたらしました。VoIP は、異なるトランスポートプロトコル上で、同じサービスを提供します。信頼性の観点からは、VoIP は従来の電話インフラと違いはありません。

VoIP では、電話サービスは IP プロトコルファミリー上で提供されます。VoIP そのものは、トランスポートネットワークに、パブリックでオープンなインターネットを使うということの意味するわけではありません。IP ネットワークを使うということが、すなわちインターネットを使うという意味ではありません。

最も一般的な企業向け VoIP の実装はプライベートの専用線を使用するもので、コールのやり取りにパブリックなインターネットは使用しません。これは、オープンで敵意のあるインターネットに関連したリスクが理由です。

データと電話 — 脅威が倍に

VoIP の脅威、攻撃、脆弱性を考えるとき、我々は電話サービスと IP データサービスの両方として考慮する必要があります。この二つの領域には、それぞれの脅威、攻撃、脆弱性があります。

VoIP のサービスは、VoIP プロトコルの観点からのアプローチによって停止させられることがあります。それだけでなく、IP ネットワークとしても攻撃を受ける可能性もあります。攻撃の方法は、大量のトラフィックをシステムやネットワークに送りつけるものから、ターゲットのシステムをダウンさせるような悪意のあるパケットを作成するものまで様々です。

脅威の解析と、関連した脆弱性の解析は、VoIP に関連した真のビジネスリスクを明らかにします。もし、脆弱性が存在しなければ、それが暴かれる脅威のリスクはゼロになります。もし脆弱性が存在するとすれば、攻撃スクリプトやウィルス、ワーム等によって、システムが攻撃される可能性があります。

現実の世界においては、全てのソフトウェアはバグや脆弱性を含んでいます。バグの数は、厳しい試験や検証によって、大幅に削減できます。多くの場合これが、VoIP に関連したビジネスリスクをトータルにコントロールする唯一の方法です。

ほとんどの脆弱性は実装の誤りによるもの

RFC3027 によれば、脆弱性 (vulnerability) とは以下のように定義されています。“システムのデザインや実装、あるいは運用や管理における不具合や欠点で、システムのセキュリティポリシーを破るために利用され得るもの (A flaw or weakness in a system's design, implementation or operation and management that could be exploited to violate the system's security policy.)”。

脆弱性は、ソフトウェアのライフサイクルにおける様々な局面において取り込まれます。要件の定義やデザイン、実装、設定等です。

NIST (National Institute of Standards and Technology) の統計によれば、明らかになった脆弱性の 70%以上が実装の誤りによるもの、すなわち、プログラム作成中に取り込まれたバグであるとされています。誤ったデザインの選択や、安全ではないデフォルトの設定は、報告された脆弱性の 20-25%に過ぎません。

Vulnerability Type Input validation error

Year	2006	2005	2004	2003	2002	2001
# of Vulns	1586	3183	1374	681	977	815
% of Total	68%	66%	58%	54%	50%	49%

Source NIST, an Agency of the U.S. Commerce Department
<http://nvd.nist.gov/statistics.cfm>

オープンなネットワーク、敵意のあるトラフィック

従来の電話網と、全てが Internet Protocol (IP) 上に構築された Next Generation Networks (NGN) との最も大きな違いは、システムがオープンであることです。

従来のシステムでは、'five nines' こと 99.999%の稼働率は、長期間にわたってトラフィックをシミュレーションすることによって測定されました。この試験に使用されたトラフィックは、ほとんどが正常なものです。異常な、あるいは悪意のあるトラフィックは、ほとんどもしくは全く使用されませんでした。

インターネットにおいては、実際の環境が“正常な”トラフィックだけを含んでいることを誰も保証できません。実際、サービスを停止させることを目的として、敵意のあるトラフィックフローや破損したパケットを送る悪意のある攻撃者がいるのは確実です。オープンでパブリックなインターネットを使用する Next Generation Networks (NGN) の安全を確保するためには、全てのソフトウェアコンポーネントにおける全ての信頼性の不具合を発見し改修する必要があります。全体のサービスを停止させるために、攻撃者はたった一つの信頼性あるいはセキュリティの不具合を見つければよいのです。

サービスの停止は損失である

あらゆるサービスが停止、妨害、改ざんされることにより、通常のサービスが利用できなくなることが起こり得ます。脅威と脆弱性におけるサービス停止のカテゴリは、ダウンタイムやメンテナンスのコストによる利益損失の最大の原因の一つです。

脅威にさらされる可能性のあるサービスは、新たなサービスが IP テレフォニーに導入されるに従い増えていきます。今日の電話サービスは次のようなものを含んでいます。コールの発信と受信、ボイスメール、コーラ ID、国際通話、テレフォンナビリング、コールウェーティング、転送、ロケーションサービス、暗号化、合法的傍受、緊急サービス等。これらは全て、シンプルな Denial of Service (DoS) 攻撃によって停止させられる可能性があります。

攻撃 - 総当たりか標的を定めているか？

DoS の状況は、パフォーマンスの問題と、ソフトウェアの品質の問題に起因します。DoS 攻撃の主な二つのカテゴリは、

1. 負荷、ストレス、パフォーマンスをベースとした攻撃
2. ロバストネス、耐久テスト (Torture Test)、ファジング (fuzzing)、プロトコルをベースとした攻撃

最初のカテゴリでは、DoS 攻撃は大量のネットワークトラフィックをターゲットのシステムに送ることで実行されます。ネットワークに開かれたインタフェースに攻撃をかけることで特定のネットワークの要素を利用不能の状態にすることが目的です。

2 番目のカテゴリでは、トラフィックが通常期待されるものとは合致しない、異常なメッセージが使用されます。この種の攻撃では、巧妙に作られたたった一つのパケットでサービスを停止できることがあります。バッファオーバーフロー攻撃は、最もよく知られたプロトコルベースの DoS 攻撃の種類です。

異常なプロトコルパケットによる攻撃は、システム全体の侵害につながる可能性があります。全体が侵害された場合、攻撃者はシステムを“所有”し、本来のユーザに代わって全てのサービスとプロセスを制御、モニタ、再設定することができます。全体的な侵害の例はワーム攻撃で、ワームが被害者のコンピュータの内部で動作し、その被害者のふりをしながら新たなコミュニケーションセッションを作成します。

能動的で目標を定めた試験による VoIP の防御

負荷ベースの DoS 攻撃は容易に検出することができ、サービスプロバイダや当局と協力して悪意のあるパーティからのトラフィックを拒絶することにより、攻撃を軽減することができます。より広い帯域を用意する、ロードバランシングによってトラフィックを分散する、リソースを慎重に割り当てる等の対策によって、これらの攻撃によるリスクを削減することもできます。

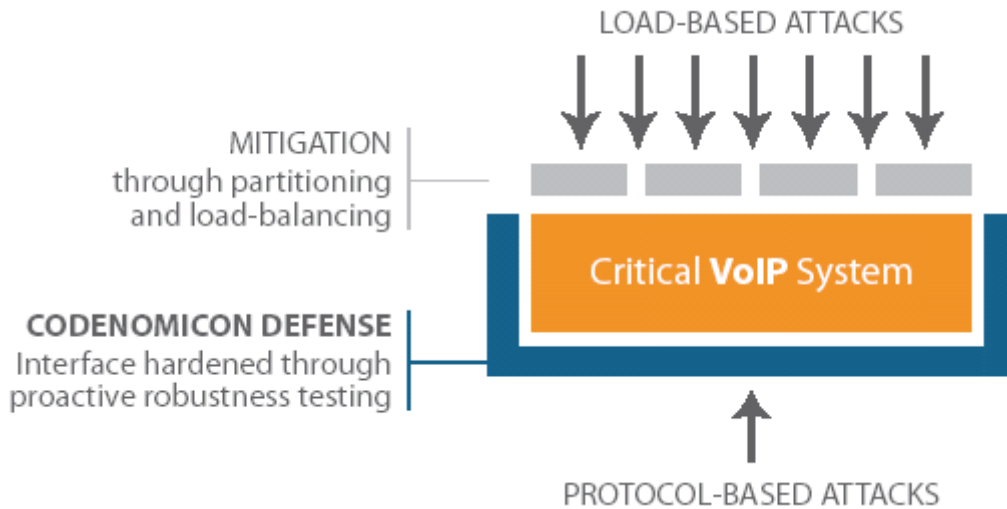
異常なプロトコルメッセージによる攻撃は、防いだり軽減したりすることがより困難です。この種の攻撃が起きたときには、ソフトウェアのバグを修正するには手遅れです。被害者ができることは、被害をコントロールし、損失を最小化することだけです。

プロトコルベースの攻撃を防ぐ唯一の方法は、攻撃者がソフトウェアにアプローチする前に、使用されるソフトウェアを幅広いネガティブテストにかけることです。悪意のある攻撃を擬似するような数万種類のプロトコルメッセージによって攻撃を行ってみることで、実装のロバストネス（堅牢性）、セキュリティ、全体的な品質を調べることができます。

システムチェック、自動的、再現可能なロバストネステストによって、ソフトウェアベンダ、通信事業者、エンタープライズ、及びエンドユーザは、導入段階にある VoIP の実装のセキュリティや品質を評価することができます。

市場にある多くのファジングツールは、擬似的なランダムトラフィックを送信しますが、再現性が低く、テストの範囲も限られています。入念にデザインされ、パッケージとして組み込まれたロバストネステストによって、問題点をより効果的にかつ確実に見つけることができます。この種の試験は、既存の自動的なテストシステムに容易に組み込むことも可能です。

DoS 攻撃に対する防御



VoIP インタフェースの解析

ロバストネスの観点から試験すべき VoIP システムのインタフェースの例：

- シグナリング：H. 323、SIP、SS7、SigComp、SCCP
- メディア制御：MGCP、H. 248、Megaco
- メディア：RTP、Codec、MPEG4 ストリーム
- プラットフォーム/トランスポート：IPv4/IPv6、TCP、UDP、SCTP、TLS
- デバイス管理：SNMP、HTTP、SSH、Telnet、TFTP、NTP、DHCP

PROTOCOL STACK

RTP	audio/video	MPEG4 streams		MEDIA PLANE
SIP	H.323	H.248	MGCP	SIGNALLING/MEDIA CONTROL
TLS				OPTIONAL ENCRYPTION
TCP	UDP	SCTP		TRANSPORT
IPv4	IPv6			IP LAYER
IPsec				OPTIONAL ENCRYPTION

MANAGEMENT PROTOCOLS etc.

SNMP	HTTP	SSH	Telnet	TFTP	DHCP
------	------	-----	--------	------	------

VoIP のロバストネスとセキュリティ用 Codenomicon Test Tool

Codenomicon SIP UAS Test Tool

Codenomicon SIP UAC Test Tool

Codenomicon H.323 Test Tool

Codenomicon H.248 Test Tool

Codenomicon MGCP Test Tool

Codenomicon RTP Test Tool

Codenomicon Audio Test Tool

Codenomicon Video Test Tool

Codenomicon MPEG4 Test Tool

Codenomicon TLS/SSL Test Tools

Codenomicon IPv4 Test Tools Suite (IPv4, TCP, UDP, ICMP, IGMP, ARP)

Codenomicon IPv6 Test Tools Suite (IPv6, TCP, UDP, ICMPv6)

Codenomicon IPsec Test Tool

Codenomicon SNMP Test Tool

Codenomicon HTTP Server Test Tool

Codenomicon SSH1 and SSH2 Test Tools

Codenomicon Telnet Test Tool

Codenomicon TFTP Test Tool

Codenomicon DHCP/BOOTP Test Tool

まとめ

VoIP ネットワークは、可用性について、従来の電話ネットワークと同等の厳しい要求を満たさなければなりません。オープンな環境であることから、VoIP システムはプロトコルベースの攻撃を受けやすく、セキュリティ、信頼性、ロバストネスを保証するためには、能動的な事前の評価が必要不可欠です。

新しい攻撃の技術は絶え間なく作られています。すなわち、攻撃を途中で止めることがますます難しくなっています。ファイアウォールや IDS システム、その他一時的なソリューションでは、全ての攻撃を止めることはできません。最も費用効果の高いソリューションは、自動的なネガティブテストによって、実装そのものを強固にすることです。VoIP の脆弱性に対する最大の防御は、優れた能動的な攻撃です。別の人間が行う前に、ソフトウェアを試験しなければなりません。



株式会社 東陽テクニカ 情報通信システム営業部

〒103-8284 東京都中央区八重洲 1-1-6 電話：(03)3245-1250 Fax：(03)3246-0645

E-mail：codenomicon@toyo.co.jp

<http://www.toyo.co.jp/it/codenomicon/>