シンプルな防御は究極の洗練です。  
21.1はじめに  
ネットワークセキュリティの多くは実用的なエンジニアリングであるため、これは簡単ではありません。コンピュータサイエンスの純粋主義者は、この分野を1つの小屋を別の小屋の上に積み上げたものと見なすかもしれません。  
しかし、多くの組織はネットワークセキュリティに注意を払う必要があり、目に見える戦略的傾向がいくつかあります。  
そして、いくつかの産業には実行可能な代替手段がありません。  
1990年代の終わりまでに、制御システムエンジニアは安価なセンサーとアクチュエーターをIPネットワークに接続していた–そして、センサーのIPアドレスを知っている人なら誰でもそれを読み取れ、アクチュエーターのIPアドレスを知っている人なら誰でもアクティベートできることに気付いたそれ。  
典型的な変電所には、パフォーマンスが重要なLAN上に多数のベンダーの200台のデバイスがあるため、暗号化を改良することは現実的ではありません。しかし、外界とのつながりが1つあるため、ここで保護を行う必要があります。  
内部CANBUSを保護できない車両でも同じアプローチがとられるため、外界との無線インターフェースを保護する必要があります。  
考えられるリーダーの1人はGoogleであり、ファイアウォールなしのアーキテクチャを推進しています。これは、ゼロトラストセキュリティモデルと呼ばれています。従来のVPNを必要とせずに、事実上あらゆる場所から安全に保護できます。」 Googleの経験では、モバイルおよびクラウドテクノロジーへの移行により、ネットワークの境界を定義することがさらに難しくなり、警察もそうです。企業の規模が大きく、内部の侵害が避けられない場合、境界はプライマリを配置するのに不適切な場所になっています。保護[1984]。  
これは、建物ごとのファイアウォールではなく、サービスごとのファイアウォールであると考えるかもしれませんが、感度の階層、デバイスインベントリサービス、およびアクセス制御エンジン[1479]を使用すると、はるかに多くのことができます。  
大部分のデータセンターを運営している他の企業でも、ほとんど同じアーキテクチャが採用されており、ゼロトラストセキュリティは、NISTによる標準草案の主題となっている[1618]。  
他の組織は、ハイブリッドなアプローチを取るかもしれません。  
オプションと制約を調べるために、まず、BGP、DNS、SMTPなどのネットワークプロトコルと、それらの悪用から発生する可能性があるサービス拒否攻撃について説明します。  
次に、TLS、SSH、IPsecなどの広く使用されている暗号プロトコルの制限と、認証局の特にトリッキーな役割について調査します。  
多くの問題は複雑で相互に関連しており、かなりのトレードオフがあります。  
この章では、固定ネットワークについて扱います。次の章では、モバイルネットワークの違いについて説明します。  
21.2ネットワークプロトコルとサービス拒否  
電信概要は以下のとおりです。  
 あるマシンから別のマシンにパケットデータを転送するステートレスプロトコルです。 IPバージョン4は、32ビットIPアドレスを使用します。多くの場合、172.16.8.93のように、0〜255の範囲の4つの10進数として記述されます。  
現在、トラフィックの10〜15％がIPv6です。多くの国では、新しいブロードバンドサブスクリプションにより、すべての通常の消費者の目的で機能するIPv6アドレスを取得できます。  
 アドレス解決プロトコル（ARP）を使用してIPv4アドレスにマップされる  
動的ホスト構成プロトコル（DHCP）  
ネットワークアドレス変換（NAT）  
したがって、悪意のある処理を行ったマシンを追跡したい場合は、多くの場合、デバイスのMACアドレスをIPアドレスにマッピングするログを取得する必要があります。  
最も基本的な懸念の1つは、サービス拒否（DoS）の防止と軽減です。  
これらにはいくつかの風味があります。  
対戦相手は、多くの侵害されたマシンのボットネットから大量のトラフィックを送信できます。分散型サービス拒否（DDoS）  
DNSなどのさまざまなオンラインサービスを悪用して、大量のパケットトラフィックを送信する可能性があります。  
  
インターネットは相互接続されたネットワークのネットワークです。そのコンポーネントは自律システム（AS）です。  
それらをまとめる接着剤、インターネットのコアルーティングプロトコルは、ボーダーゲートウェイプロトコル（BGP）です。ルーター（ネットワークでパケットを交換する専用のコンピューター）は、BGPを使用して、IPアドレスの特定のブロックに到達するために利用できるルートに関する情報を交換し、使用する効率的なルートを選択できるようにルーティングテーブルを維持します。  
、そのうちほとんどの国には少なくとも1つがあり、大きな国にはいくつかある場合があります。  
そのオープンで分散化された組織は、インターネットの成功と回復力に不可欠でした。これは、ハリケーンカトリーナなどの自然災害と9/11などのテロ攻撃の影響が時間と空間で制限されていることを意味します。さまざまな技術的な障害。  
 破壊的な攻撃と同様に。  
事故や事故という形ですでにいくつかの警告が出されています。  
一部の人々は事故を原因と考えたが、他の人々は中国が「サイバー核」をテストしていたと示唆し、その一部は放射性降下物を脱出した。  
中国と（最近）  
中国で情報収集のためにBGPハイジャックが使用されているという報告があります。たとえば、カナダから韓国政府のWebサイトへのトラフィックは、2016年2月から6か月の間中国を経由していました[533]。  
最後に、2019年から20年にかけて、Huaweiがルーターを大規模に（またはまったく）販売することを許可すべきかどうかについて、政治的混乱が高まっています。  
一歩後退して、インターネットの回復力を定義し、測定することは困難です。それは効率と緊張状態にあり、少数の非常に大規模なネットワークが支配的になるにつれて減少する可能性があります。  
 Google、Akamai、Cloud ﬂ areなどが運営しています。  
BGPを介して配信されるルーティング情報の有効性を確認するメカニズムはありません。  
システムがどのように機能するかについての適切な情報の欠如は、合理的な議論も困難にします。  
2011年、同僚と私は、これらの問題を詳細に調査する欧州ネットワーク情報セキュリティ局の主要なレポートを書きました[1906]。  
 これにより、レジストリは「自律システムXがIPアドレス範囲Yをアナウンスする」ことを証明できます。  
すでに脆弱なBGPシステムをより堅牢にして、そこに多くの証明書を残すことができるかどうか。 RIPEの証明書が2020年2月に期限切れになったとき、修正されるまで短時間の停止がありました。  
  
ドメインネームシステム（DNS）  
いずれかの種類のIPアドレスにマップされるcom。これを行うDNSサーバーの階層があり、パフォーマンスと信頼性のためにDNSレコードをキャッシュするISPやローカルネットワーク上のマシンを経由して、数百のトップレベルサーバーにまで至っています。  
しかし、DNSは非常に高速なマシンが非常に大容量のネットワークに接続された大規模分散システムになっているため、DNSに対するサービス拒否攻撃はまれです。  
一部の州では、検閲の手段としてDNSクエリを傍受してリダイレクトしています。一部のISPは、Webページ内の広告をカット元の広告に置き換える手段としてそうしています。 ISPのDNSサーバーがハッキングされて、クライアントを邪悪なWebサイトに誘導する可能性があります。  
次にwww.citibank.comにアクセスしようとすると、それをエミュレートするフィッシングサイトに誘導される可能性があります。  
DNSハイジャックを防ぐために、DNSSECはDNS名レコードにデジタル署名を追加します。  
取り込みは不安定です。.gov内のすべての米国政府ドメインは署名されることになっています。また、登録機関が署名済みドメインを安価にしたため、スウェーデンのほとんどのドメインが署名されています。  
他の企業は、競合他社に「ゾーンを歩き」、すべてのサブドメインを列挙させたくないため、DNSSECを避けています。 NSEC3拡張により、企業はハッシュを使用してこれを回避できますが、多くの企業（またはそのサービスプロバイダー）  
DNSSECのもう1つの問題は、サービス拒否攻撃で悪用されることです。  
 あなた、ボブ！」署名されたDNSレコードははるかに大きいため、DDoS-for-hireサービスはDNSSECを増幅器として使用でき、AliceはBobのIPアドレスからのパケットを多くのDNSサーバーに送信し、ターゲットに返信を送信できます。  
 2020年に物議を醸している問題はDNS-over-https（DoH）です  
メインブラウザーのメンテナーであるChromeとMozillaは、DNSトラフィックを平文で送信するのではなく、httpsを介してDoHリゾルバーに暗号化することを提案しています。  
。  
マルウェアがマシン内のマシンを危険にさらした場合、それがコマンドアンドコントロールサーバーに接続しようとするときにそれを発見する可能性があるため、企業は脅威インテリジェンスフィードを購入し、ドメイン名（およびIPアドレス）を監視しますシステム管理者は、DNSハイジャックを監視し、特定のドメインを不適切な作業としてブロックすることも好みます。  
商業面では、DoHが広告市場でのGoogleの地位を確立する一方で、AkamaiやCloud ﬂなどのコンテンツ配信ネットワークにルーティングや負荷分散などの問題を引き起こしている可能性があります。  
専門家は代わりにDNS over TLSを実行することを好んだでしょう。  
21.2.3 UDP、TCP、SYNフローおよびSYN反射  
 コネクションレス、または伝送制御プロトコル（TCP）  
AliceがBobへのTCP接続を開始し、後続のパケットトラフィックのシーケンス番号を設定するために使用する3ウェイハンドシェイクから始めましょう。  
 図21.1 – TCP / IPハンドシェイクこのプロトコルはさまざまな方法で利用されています。  
アリスは単純に多数のSYNパケットを送信し、どの応答も確認しません。  
これは、1996年にニューヨークのISPであるPanixを数日間ダウンさせた最初の分散型サービス拒否攻撃の1つで使用されました。  
そうすれば、ボブはハーフオープンセッションについて多くの状態を保持する必要がなくなります。  
一般的な原則は、誰でも呼び出すことができるプロトコルを設計するときは、悪意のあるユーザーが正直なユーザーに強制的に機能させないようにすることです。  
アリスはチャーリーから来たと主張するパケットをボブに送ります。  
  
DNSやTCP以外の多くのプロトコルがサービス拒否攻撃で使用されています[1503]。  
、これにより、ユーザーはエコーパケットをリモートホストに送信して、生存しているかどうかを確認できます。  
ブロードキャストアドレスが応答しないようにプロトコルが変更されました。  
パケット増幅に基づく攻撃に対するより徹底的な修正が続くことになっていました。  
Microsoftはまた、ネットワークスタックを変更して、感染したマシンがIPアドレスが偽装されたパケットを送信することをはるかに困難にしました。古いアプリケーションだけでなく、オペレーティングシステムをハックする必要があります。  
2010年代後半、そのよ​​うな攻撃は、DDoS for-hireオペレーターの保護をますます強めており、その攻撃に対して最も効果的な対策は、彼らを襲撃して逮捕することでした。  
21.2.5その他のサービス拒否攻撃  
最初の分散型サービス拒否（DDoS）  
現在、ボットネットはあらゆる種類の脆弱性を使用して組み立てられており、アンダーグラウンドマーケットでは、マシンをハッキングし、さまざまな方法で価値を引き出す他のユーザーに販売することに特化しています。  
Miraiボットネットはこの機会を利用するために2016年10月に登場し、それ以来、1000を超える亜種が存在しています（そのソースコードはHackforumsに投稿されています）。  
サービス拒否攻撃にはさまざまな動機があります。  
DDoSの貸し出しには、数年前から闇市場があり、米国などの当局は閉鎖を試みてきました。  
オンラインブックメーカーの）  
第2章では、州による紛争での使用について説明しました。  
10万人がホワイトハウスに電子メールを送信して何らかのポリシーなどに抗議した場合、これはDDoS攻撃ですか？  
  
電子メールのSMTP標準には、大量の傍受の防止、および不要な大量のメールの防止に関する特定の問題があります。  
PGP / GPGなどのプログラムを使用してメールを暗号化することは可能でしたが、これは小さなコミュニティの外では決して行われませんでした。  
さらに、少人数のグループだけが暗号化を使用している場合、これは当局に注意を向けさせるだけかもしれません。セクション20.4で説明したように、破壊的なグループやスパイなどには、機密性だけでなく匿名性が本当に必要です。  
一括傍受に対する主な対策は2つあります。  
暗号化された交換は中間者攻撃によってブロックされる可能性があり、これらは非民主主義の国で報告されています。  
、Microsoft、Google、Yahoo [1220]でサポートされています。メールサービスプロバイダーは、ウェブサイトからダウンロードした適切な証明書で認証されたTLSセッション経由でのみメールを配信するように指定できます。  
MTA-STSは一般に、以前の標準であるDNSベースの名前付きエンティティの認証（DANE）に取って代わりました。  
2番目の対策は、今日の個人用メールアカウントの95％が大手5つのウェブメールプロバイダーにあり、多くの企業がそれらを使用していることです。  
ただし、一括アクセスはブロックされる場合がありますが、ウェブメールは、企業が外部委託する他のサービスと同様に、正当なアクセスの対象となります。1つ目は完全に合法ですが、望ましくないマーケティングコミュニケーションです。  
21.3。  
2つ目は、大部分がボットネットによって送信された、通常は望ましくないトラフィックのフラッドで構成されており、多くの場合、明確な犯罪目的で送信されます。  
これは、4つの主要なメカニズムを備えた大手プロバイダーによって対処されています。  
ドメインキー識別メール（DKIM）  
署名された素材は、転送中に発生するヘッダーへの追加にもかかわらずメッセージを明確に識別するために選択されますが、悪意のある人物が余分な「From：PayPal」ヘッダーを追加するのを防ぎます。  
スパマーがGmailを介してスパムを送信し、それに署名してから転送するというリプレイ攻撃があります。そのため、メールサーバーはDKIM署名をキャッシュし、すでに数回見られている署名を含むメールを破棄します。  
送信者ポリシーフレームワーク（SPF）  
繰り返しますが、これはドメインDNSレコードのキーに対して検証可能です。  
 転送するメールに再度署名する。  
ドメインのDNSには、ドメインベースのメッセージ認証、報告、適合（DMARC）も含めることができます  
4。  
これは、ユーザーごとに、また時間とともに変化するマーケティング資料のユーザー設定によって、さらに複雑になります。  
その統計は2000年代半ばから「こぶ」であり、これはより顕著になっています。  
  
悪意のあるコードの最初の例はトロイの木馬でした。ギリシャ人がトロイの木馬のために残した馬にちなんで名付けられました。おそらく贈り物として、21.3が含まれていました。  
長年にわたって命名法をめぐる宗教戦争があったため、多くの人がマルウェアという用語を単に使用することを好みます。  
 疑いを持たないユーザーによって実行された場合。  
リモートアクセストロイの木馬（RAT）  
望ましくない可能性のあるソフトウェア（PUS）  
。  
たとえば、ストーカーウェア（ある人が別の人の携帯電話の位置を追跡して使用できるようにするソフトウェア）は、それが密かにインストールされているか、支配者がパートナーをいじめているか、または裁判所がそれを条件として注文したかによって、異なるカテゴリに分類されます寄託。  
マルウェアは一般的にステルス技術を使用して非表示にしますが、最終的には特定され、それを削除するツールが作成されます。  
（マルウェアを販売している企業さえあります–特に政府機関に。）  
  
1960年代初頭、マシンは低速で、CPUサイクルは割り当てられていました。学生がキューの最後にいることがよくありました。  
1970年代までに、大学のタイムシェアリングシステムは、トロイの木馬を巻き込むいたずらの標的になりました。  
1978年、ゼロックスPARCのジョンショークとジョンハップは、ワームと呼ばれるプログラムを作成しました。これは、タスクを割り当てることができるように、ネットワーク全体に自分自身を複製してアイドルプロセッサを探していました[1724]。  
彼は、システムのソースコードを注意深く検査し、脆弱性がないことがわかっていても、トラップドアを挿入できることを示しました[1883]。  
2これが範囲外であると認識した場合、一部のウイルス対策製品は、「無料試用」後に削除するのが非常に困難であったり、不安を招いたりするなど、さまざまな点でマルウェアのように動作します。  
21.3。  
もちろん、誰かがコンパイラのソースコードを調べて、それを最初から再コンパイルするかもしれません。  
したがって、検証可能な安全なハードウェア、オペレーティングシステム、アプリケーションを備えたシステムを購入できたとしても、コンパイラバイナリにはトロイの木馬が含まれている可能性があります。  
ツールチェーンやハードウェアも含め、すべてを作成する必要があります。  
1981年に9年生によってApple II向けに開発された最初のコンピュータウイルス[1216]。  
約3年以内に、ユーザーがフロッピーディスクや掲示板を介してプログラムを共有したときに広がるPCウイルスである、最初の実際のウイルスが実際に見られるようになりました4。  
これはメインフレームコマンド言語REXXで記述されたプログラムで、ヘッダーに「私を読まないで、EXECミー」と書かれていて、実行すると画面上にクリスマスツリーが描かれ、ユーザーの連絡先の全員に送信されます。ファイル。  
 普及し、ユーザーにそれを実行するように勧めることは、時代を先取りするものでした。  
21.3.2インターネットワーム  
これは、1988年11月に1つのマシンから別のマシンに拡散するために多数の脆弱性を悪用したRobert Morris Jrによって書かれたプログラムでした[617]。  
。  
。  
しかし、バグがありました。その結果、膨大な量のトラフィックが発生し、インターネット（より正確には、前身のArpanet）が完全に詰まっていました。  
1つのレッスン3Thisは、1974年のMultics評価でPaul KargerとRobert Schellによって最初に浮上したアイデアを開発しました[1019]。  
21.3。  
  
1990年代初頭までに、PCウイルスは、ウイルス対策ソフトウェアの業界全体を生み出すような問題になりました。  
21世紀の初めまでに、主要なベクトルはWordなどの製品のマクロ言語であり、主要な送信メカニズムはインターネットになりました[298]。  
2000年の「Love Bug」は、被害者のアドレス帳の全員に自分自身を送信するワームで、「I love you」という件名で人々に開かせるように設計されています5。  
同社は各従業員に各自のアドレス帳にある社内ディレクトリのコピーを渡しており、85,000のメールクライアントがそれぞれ85,000のアドレスそれぞれに「愛しています」と発言しようとしたため、結果はメルトダウンでした。  
次の開発はフラッシュワームで、インターネット全体をスキャンしてエクスプロイトやその他の脆弱性のあるマシンを探し、それらを乗っ取る。 Code RedやSlammerなどの例は、すべての脆弱なマシンを数時間または数分で感染させ、どのような自動防御が時間内に反応するかを調査しました[1821]。  
スパイウェアはあなたのコンピュータ（そして今はあなたの電話）から情報を収集して転送します  
また、親やパートナーなどの他の誰かによってインストールされる場合もあります。スパイウェアは、親密なパートナーの虐待にますます関与しています。  
このような製品のベンダーは、自社の製品をブラックリストに登録したウイルス対策企業をも訴えています。  
境界は困難であり、人によって意見が異なる場合があります。  
それまで、ほとんどのマルウェア作成者は楽しみのために、または友達に印象づけるためにそうしました。基本的に、彼らはアマチュアでした。  
21.3。  
マルウェアの作成者は、ボットネットの遊牧民への現金やその他の悪用に販売できるマシンを募集するためのソフトウェアにお金を払うようになりました。  
コードの感染力が不十分な場合、コードは拡散しませんが、コードの感染力が高すぎる場合、数時間以内に、世界のウイルス対策ベンダーが製品をアップグレードして、コードを検出して削除します。  
（主な例外は、パッチを適用できないIoTデバイスを利用する場合です）。  
さまざまなストーリーが使用され、人々がリンクをクリックして、ルートキットを自分のマシンにドロップするトロイの木馬を実行しました。  
最初に本当に大きなものの1つであるStormは、ポンプアンドダンプのオペレーターと薬局の詐欺師から生計を立てました[1090]。  
結局、それはマイクロソフトによって削除の対象となった。  
フラッシュワームは、Miraiワームとその亜種で2016年10月から復活しています。  
それ以来、さまざまなIoTデバイスを攻撃するMiraiの亜種が1000以上あります。  
21.3.4マルウェアのしくみ  
ワームは、実行されたときに別の場所に自分自身のコピーを作成します。おそらく、パスワードを推測したり、リモートコード実行の脆弱性を使用して別のシステムに侵入したりします（どちらもインターネットワームによって使用されました）。  
ウイルスは他のソフトウェアに拡散し、おそらく文書内のマクロとして拡散しますが、トロイの木馬は通常、被害者によって実行されます。  
これをアクティブにすると、いくつかの悪いことの1つまたは複数が発生する可能性があります。•機密データを抽出します。 •バンキングマルウェアまたはスパイウェアを使用して直接攻撃する。 •データを暗号化し、身代金を要求します。 •GCHQの運用社会主義者がセクション21.3で説明した場合など、他者を攻撃する。  
Belgacomの場合のように、標的が個人ではなく会社である場合、攻撃には数週間から数か月の作業が含まれる可能性があります。  
多くの可能性があります。  
昔は、攻撃者はパケットスニファソフトウェアをインストールしてパスワードを収集し、最終的にはシステム管理者を含む他のアカウントを侵害していました。  
2。  
たとえば、Linuxサーバーはネットワークファイルシステム（NFS）を使用できます。  
Kerberosを使用してクライアントとサーバーを認証する私たちのラボでこれをブロックします。  
3。  
有能な攻撃者が現在利用できるツールの範囲について知るには、エドスノーデンによってリリースされたNSAの文書と、Vault 7の開示で漏洩したCIAツールキットを参照することをお勧めします。  
重要なのは、ネットワークへの侵入者が他のマシンを乗っ取ることができる容易さは、ネットワークがどれだけ緊密にロックされているかに依存し、侵害に続くダメージは、ネットワーク内の他のマシンが信頼する程度に依存するということです。 、または侵害されたマシンに対して脆弱です。21.3。  
21.3.5対策  
これは、ウイルスとアンチウイルスの開発者が互いに裏をかこうとする軍拡競争につながりました。  
スキャナーは実行ファイルを検索して侵害の兆候（IoC）を見つけます  
マルウェア開発者はさまざまな方法で対応し、主要な手法は多態性になりました。  
通常の方法は、コードを暗号化し、復号化コードを含む小さなヘッダーを使用することです。  
最近のマルウェアは、半ダースのパッカーを順番に実行され、実行時に再帰的にアンパックする可能性があります。  
AVファームは、最後のアンパック操作にハッキングできる限り、少なくともアンパックされたコードをIoCとして使用できます。  
マルウェア開発者の主な対策はステルスです。これは、このコンテキストでは、マルウェアがチェックサマーで使用される種類のオペレーティングシステムコールを監視し、チェックが行われるたびに自身を隠すことを意味します。  
DOSベースのファイルウイルスの昔は、すべてのインシデントの中央報告ポイントを提供し、組織のマシンにロードされたすべてのソフトウェアを制御することを学びました。  
、および他の組織からのファイル。  
しかし、企業は以前よりも調整された対応を必要としています。  
ボットネットとマシンの悪用の商業化は、マルウェアの作成者が企業のように機能し、研究部門とテスト部門を持つことを意味します。  
 そして、それらの多くは、ウイルス対策業界の注意を引くことなく、目標数のマシンを採用しています。  
つまり、最新の脅威インテリジェンスに照らして、優れたツールサポート、ネットワークトラフィックのログ記録、分析を行う必要があります。  
そして今日、多くの攻撃者、特に有能な攻撃者は、マルウェアファイルを横に置いたままにせず、「土地から離れて」います。サーバーの1つにある承認済みキーのリストにsshキーを追加するだけで、希望するときにポップインして、レガシーAVが見つけるものは何もありません。  
21.4ネットワーク攻撃に対する防御  
原則は2020年まで変わりませんが、タスクの規模と複雑さにより自動化がほぼ必須となったため、現実は今でははるかに複雑になっています。  
各エンドポイントで実行されるエージェント。クラウドサービスにレポートして、どこで実行されているソフトウェアかを完全に可視化し、更新をプッシュできるようにします。 2。  
ファイアウォール、スタッフがアクセスするWebサイトのすべてのURLをフィルタリングするプロキシサーバー、重要なアプリケーションのプロキシなど、さまざまな境界制御デバイス。 4。  
自分のデバイスを持参（BYOD）  
データ漏洩防止（DLP）  
複数のプロバイダーからのフィードを統合する脅威インテリジェンスプラットフォーム。不正なDNS名やIPアドレスなど、侵害のさまざまなインジケーターを警告します。 8。  
セキュリティオーケストレーションとレスポンス（SOAR）  
これらすべてを連携させるにはシステム統合が必要です。それ以外の場合は、ネットワークセキュリティセンターに何十人ものスタッフがいて、不正なドメイン、不正なIPアドレス、その他の侵害の指標のリストをツール間でコピーします。  
ITセキュリティに真剣に取り組んでいる組織–彼らは国家関係者（大手サービス会社など）の標的であるため  
、または（軍のように）失うものがたくさんある  
これは、すべてのパッチを最新の状態に保つことを意味します。これは、自動化されたパッチ管理を意味します。  
これには、ネットワーク上のすべてのデバイスの正確なインベントリを維持するなど、いくつかの難しいサブ問題が伴います。  
したがって、ネットワークもスキャンして、そこに何があるか、また脆弱かどうかを確認する必要があります。  
これは運用上のセキュリティと相互作用します。  
2000年代半ばまでに、主な攻撃経路はスピアフィッシングでした。つまり、ルートキットをダウンロードしてインストールする電子メールのリンクをクリックするように人々を誘導しました。  
あるいは、なりすまし可能なWebサイト、または中間者プロトコル攻撃を仕掛けられる可能性のあるWebサイトにターゲットを誘導します。  
そして、多くの企業は、顧客やサプライヤがリンクをクリックすることを期待しています。そのリンクをクリックすると、スタッフは作業​​を完了するためにクリックする必要があります。  
多くの企業は、ローカルマシンではなくクラウドサービスですべてのメール添付ファイルを開き、スタッフにChromebooks、iPad、Macなどの非Windowsマシンを提供するか、不審なコンテンツを取り除くファイアウォールまたはメールフィルターを用意することでリスクを軽減します。21.4.1フィルタリング：ファイアウォール、検閲器、盗聴  
これは、乗客を燃料火炎から保護するために、車の客室または軽飛行機をエンジンルームから分離する金属製の隔壁にちなんで名付けられました。  
それ以来、論争は前後に揺れ動いている。  
不正なパケットは破棄されるか、無害になるように変更されます。  
非常に類似したシステムは、インターネットの検閲や法執行機関の盗聴にも使用されます。このセクションで説明するほとんどすべてのことは、これらのアプリケーションにも当てはまります。  
たとえば、多くの企業のファイアウォールやメールフィルターはポルノを排除し、一部は悪意のある言葉をさえ遮断しますが、児童ポルノを検閲したり政治的な意見を反対したりするISPシステムは、加害者を自動的に当局に報告します。  
フィルターは、IPパケットレベルで動作するか、TCPセッションレベルで動作するか、アプリケーションレベルで動作するかに応じて、基本的に3つのフレーバーで提供されます。  
21.4.1.1パケットフィルタリング  
この機能は、ルーター、Linux、およびWindowsで標準で使用できます。  
「既知の不良」IPアドレスとの間のトラフィックを簡単にブロックすることもできます。  
基本的なパケットフィルタリングは、特定のポート番号に到着する以外のすべてのトラフィックをブロックするためによく使用されます。  
ソフトウェア定義ネットワーク（SDN）に移行すると  
ただし、パケットフィルターはいくつかのトリックによって無効にすることができます。  
もう1つの制限は、ブラックリストの維持が難しいことです。特にブロックしたいIPアドレスではなく、特に一時的にIPアドレスに解決される場合です。  
  
次のステップは、各TCPセッションのすべてのパケットを再構成して検査する回線ゲートウェイです。  
 これにより、インターネットを介して渡される企業トラフィックは、ファイアウォールからファイアウォールへと暗号化されます。  
TCPレベルのフィルタリングは、DNSフィルタリングなど、さらにいくつかのことを行うために使用できます。  
したがって、特定のタイプのトラフィックをアプリケーションフィルターに転送するようにプログラムできます。  
21.4.1.3アプリケーションプロキシ  
例としては、スパムを排除しようとするメールフィルターや、望ましくないコンテンツをブロックまたは削除するWebプロキシがあります。  
Webベースのメールサービスへの移行とhttpsの採用により、メールフィルターに必要な作業が大幅に減り、サービス会社はプロキシを防ぐために透明性を証明するなどの技術的手段を採用しているため、フィルタリングはエンドポイントにシフトする必要があります。  
例としては、中国のグレートファイアウォールがあり、2000年代を通じて、禁止された主題を参照するメールおよびWebコンテンツをブロックしようとしました[448]。  
Googleが推進する新しいBeyondCorpモデルでは、プロキシはアプリケーションサーバー自体の前に配置されるため、内部ネットワークを信頼する必要はありません。  
21.4.1.4入力と出力のフィルタリング  
開拓者は軍のメールシステムで、発信トラフィックを監視して、分類されたものが何もクリアされないようにしました。  
このソースアドレスの検証により、UDP反射攻撃を使用するDDoSオペレーターはボットネットを使用できなくなり、データセンターでサーバーをレンタルする必要が生じます。  
。  
ただし、httpsの普及により、DLPシステムは通常、ミドルボックスを使用するのではなく、エンドポイントにソフトウェアをインストールする必要があります。  
21.4.1.5アーキテクチャ  
それがあなたの悩みの種であるならば、単純なフィルタリングルーターはあまりメンテナンスを必要とせず、あまり邪魔になりません。  
には、メール、ウェブ、その他のサービスをフィルタリングするための多数のアプリケーションサーバーまたはプロキシが含まれています。  
。  
インターネットイントラネットの分類Classifiedffiイントラネット図21.2：MLSネットワークの複雑なファイアウォール（外側または下向き）（図21.2）  
もう1つの方法は、より多くのネットワークを用意することですが、ネットワークを小さくすることもできます。  
学生と金融部門が同じネットワーク上にある必要がある理由はなく、コンピュータサイエンス部門は神学部門とはまったく異なる要件を持っています。  
ネットワークセキュリティアーキテクチャの設計における考慮事項には、シンプルさ、使いやすさ、非境界化と再周辺化、アンダーブロッキングとオーバーブロッキング、保守性、インセンティブなどがあります。  
組織のマシンの種類が異なる場合は、少数の単純なボックスにできるだけ多くのセキュリティタスクをロードするのが理にかなっています。これらはおおよそ、上記の概要で説明したエネルギーユーティリティとGoogleのモデルです。  
セクションで話し合いますか？  
 外交官たちは、公式のシステムが使用できなかったときに、プライベートメールを使用することでどのように行き詰まったのか。  
また、慎重なシステム管理者は、単に「ポリシー」に依存するのではなく、実際のネットワーク構成を監視します。  
初期のファイアウォールはメールとWebトラフィックのみを通過させました。そのため、コンピュータゲームから匿名プロキシまでのアプリケーションの作成者は、クライアント/サーバートラフィックを通常のWebトラフィックにできるだけ似せるようにプロトコルを再設計しました。  
次に、非境界化があります。GoogleのBeyondCorpが指摘しているように、以前はデスクトップコンピューターで実行されていた機能に使用されている電話やPDAの急増、および正式に下請け業者に、または非公式に広告サポートされたWebアプリに、機能のより多くのアウトソーシングを含むビジネス方法。  
営業部隊とR＆Dラボ）  
 次に、個別のアーキテクチャが必要になる場合があります。  
コードとデータの違いは、新しいスクリプト言語によって着実に侵食されています。  
今日では、まったく保護できないだけの大量のIoTデバイスをスタッフが接続することを防ぐことができない場合があります[1254]。  
完全な精度を備えたフィルタリングメカニズムはないため、アンダーブロッキングとオーバーブロッキングの間には必然的にトレードオフがあります。  
 セックス、暴力、不適切な言葉によるウェブコンテンツのフィルタリングに使用されるファイアウォールシステムも、フリースピーチサイトをブロックする傾向があるため、事態はさらに悪化します（これらの多くはファイアウォールベンダーを批判しています。ブロッキング。）  
知り合いの100人が使用する部門ネットワークを管理し、侵入や設定エラーによって引き起こされた混乱を個人的に解決しなければならないシステム管理者は、大規模なチームの1人のメンバーである誰かよりもはるかにやる気があります。何千ものマシンの後。  
21.4.2侵入検知  
発生している悪いことを検出するために使用されるシステムは、一般的に侵入検知システム（IDS）と呼ばれます。  
前に説明したウイルス対策ソフトウェア製品はその一例です。ただし、この用語は通常、ネットワーク上に存在し、進行中の攻撃または侵害されたマシンの兆候を探すボックスに適用されます[1636]。  
このような場合、IDSは通常、特定のマシンを調べる必要があることをsysadminに通知します。  
以前の章で見た侵入検知の他の例には、支払いカード詐欺を検出するメカニズムや、価格に敏感な発表の直前の取引量の増加などによるインサイダー取引を探す株式市場システムが含まれます。  
  
最も簡単な侵入検知方法は、しきい値を超えたときにアラームを鳴らすことです。  
より洗練されたシステムは、一般的に2つのカテゴリに分類されます。  
銀行システムは、ユーザーが3日連続で現金自動預け払い機から最大許容額を引き出した場合に警告する場合があります。また、Unix侵入検知システムは、以前にナイーブなユーザーが突然、コンパイラーなどの高度なツールの使用を開始した場合に警告して、ユーザーアカウントの乗っ取りを探す場合があります。  
これは、データで明示的にすることもできます（特定のマルウェアとしてマークする実行可能ファイルの部分文字列など）。  
。  
セクション12.5.4で説明したように、カード詐欺を検出するために使用されるシステムは数十の信号を使用します。なぜなら、現代の支払いシステムの規模を考えると、低い誤警報率が役立つためです。  
以前に認識およびカタログ化されていない攻撃を検出することが期待されています。  
誤用と異常検出の境界線はややぼやけています。  
数字「1」、「2」、...で始まる数字を期待するかもしれません  
しかし、数値がランダムな自然の情報源からのものであり、1桁以上にわたるため、それらの分布がそれらが表現される数体系に依存しない場合、分布は対数的です。10進数の約30％が 'で始まります1 '。  
別の境界線のケースはハニーポットです-注目を集めるために残されたもの。ネットワークコンテキストでは、ハニーポットは多くのタイプのデバイスをエミュレートするため、攻撃者はインターネットをスキャンして（たとえば）探します  
その結果、ハニーポットのオペレーターは誰が何をどのように攻撃しているかを知ることができます。  
21.4.2.2侵入検知の一般的な制限  
活動家がWebサイトを破壊することを心配している場合は、ページを頻繁にフェッチし、変更があったときにアラームを鳴らすマシンをどこかに設置してください。  
ウイルスのパイオニアであるフレッドコーエンは、ウイルスを検出することを証明しました（プログラムが何か悪いことをするかどうかを決定するという意味で）  
定義の問題もあります。  
しかし、これにより侵入検知システムがアクセス制御メカニズムに変わり、サービス拒否攻撃への扉が開かれます。  
次に、誤警報の代償があります。  
しかし、Gmailチームに所属していて、毎日自分自身を認証する10億人のユーザーを扱っている場合、それはやりすぎです。  
最後に、機械学習分類子には3つの一般的な問題があります。それらは、新しい攻撃を検出するのがあまり得意ではないという事実、人々が攻撃すること、そしてトレーニングデータの偏見を吸い込むことです。  
  
次に、ネットワークへの侵入を検出するという特定の問題に目を向けると、支払い詐欺よりも発見するのが困難です。  
実際の侵入を後で検出するのが一般的です。  
•インターネットは非常に騒々しい環境です。コンテンツのレベルだけでなく、パケットレベルでも同様です。  
多くの不良パケットはソフトウェアのバグが原因です。その他は、DNSデータが古くなっている、または破損しているという障害です。いくつかは、脱出し、世界中を旅して戻ってきたローカルパケットです[213]。  
100万セッションあたり10の実際の攻撃がある場合（これはほぼ確実に過大評価です）、システムの誤警報率が0.1％と低い場合でも、誤報と実際の警報の比率は100になります。  
信号がノイズよりずっと下にある場合、警備員は疲れてしまい、本物の警報は見逃されます。  
エラーを検出するソフトウェアを書く方が、少し奇妙な動作を検出するよりも簡単です。  
ただし、多くの企業は保険会社や監査人を満足させるために侵入検知システムを購入しており、製品は常に最新の状態に保たれているとは限りません。  
DNS-over-httpsが標準になると、DNSトラフィックの分析に依存するツールの効果が大幅に低下します。  
パケットレイヤーでフィルタリングできます。これは高速ですが、多くは失敗します。または、アプリケーションをプロキシすることもできます。これは高価であり、新しいアプリケーションや攻撃に対処するために常に更新する必要があります。  
暗号化されたWebセッションのおかげで、ローカルマシンで実行する必要のある処理はますます増えています。しかし、一部の攻撃はステルスです。対戦相手は1日あたり1〜2パケットを、おそらく100,000台のホストのそれぞれに送信します。送信元と宛先のアドレス、およびポートごとにパケットをカウントする中央監視が必要です。  
すでにセクション21.4で説明したように、Windowsを使用する何万人ものスタッフを持つ大企業には、通常、数十の製品があります。  
暗号化：不規則な境界への対応は、CISOの仕事をますます構成しています。  
、セキュリティオーケストレーションおよびレスポンス（SOAR）  
  
ネットワークセキュリティは、さまざまな方法で暗号と相互作用します。  
それらはSSHです。 WiFi、Bluetooth、HomePlugによって提供されるローカルリンク保護。 VPNで使用されるIPSecメカニズム。 TLS;および公開鍵基盤（PKI）  
前の章では、暗号化からより信頼できるコンポーネントを構築しようとする試みが、多くの実際のエンジニアリングおよび経済的制約に直面する方法について説明しました。  
新たなテーマは、ベンダーが気にしないため、問題の最も分散した部分は管理できないということです。特に、「モノのインターネット」の一部として販売されている何千ものデバイスタイプには、ユーザーが利用できるリモート管理機能がなく、ベンダーはソフトウェアをアップグレードしないことが多く、ユーザーインターフェイスがないため、認証は無計画です。ベスト。  
  
ラップトップを使用してデスクトップマシン上のファイルにアクセスするとき、またはそのためにラボの他のマシンで何かをするときは、セキュアシェル（SSH）を使用します。  
そのため、自宅で仕事をするときはトラフィックが保護され、デスクのPCからラボ内の別のマシンにログオンするときに、使用するパスワードが平文でLANを通過することはありません。マシン間で暗号化された接続をセットアップするため、ログオンパスワードがネットワーク上を平文で移動することはなく、急速な採用につながったその他の便利な機能がサポートされます[1617]。  
秘密鍵は、ユーザーがキーボードで入力するパスフレーズによって保護されます。  
サーバーにログオンするときに、パスフレーズの入力を求められます。 2台のマシンはDiffie-Hellmanキーをセットアップします。秘密鍵は一時的な公開鍵に署名し、中間者攻撃を阻止するために使用されます。したがって、後続のトラフィックは暗号化され、認証されます。  
Diffie-Hellmanを使用して設定されたセッションキーを認証するか、21.5を設定するかに関係なく、Kerberosを使用するオプションもあります。  
（後者の場合、SSHは、信頼できるサードパーティのプロトコルになり、警察がKerberosサーバーにトラフィックを復号化させることができるという意味で、Kerberosのバリアントにフォールバックします。）  
ただし、最悪の場合、サーバー間通信に使用されるほとんどのSSHキーは、パスワードで保護されることなく、クリアテキストで保存される可能性があります。  
SSHは、単純なログオンメカニズムとしてよく使用されます。多くのIoTデバイスはLinuxを実行しており、適切なパスワードを知っている人なら誰でもリモートログオンできます。  
ここでの対策はハニーポットです。  
21.5.2周辺の無線ネットワーク  
WiFi、Bluetooth、Homeplugなどのプロトコルはすべて暗号化を提供し、サービスの悪用やおそらく盗聴からの保護を提供します。  
  
WiFiは、自宅で電話やその他のデバイスをホームルーターに接続する場合も、企業が決済端末や在庫管理デバイスやPCを接続する場合も、ワイヤレスローカルエリアネットワークをサポートしています。  
最初に広く使用されたもの、WEP（有線同等のプライバシー用）  
2004年以降、WPA2と呼ばれる改良されたシステムはAES暗号化を使用しています。  
WiFiネットワークは信頼できないものと見なす必要がありますか？  
英国やアメリカの多くの人々は、ゲストが使用できるオープンなネットワークを用意し、あなたとあなたの隣人が互いのネット​​ワークをバックアップとして使用できると便利だと感じています。  
インドなど一部の国では、オープンWiFiアクセスポイントを設置することは法律に違反しています（2008年にボンベイで攻撃を仕掛けたテロリストは、目立たないように自宅に電話をかけました）  
カードにキーを付けることは、使用可能なセキュリティ設計の優れた例です。世帯主は、壁にカードを固定するかロックすることにより、必要に応じてネットワークをオープンまたは安全にすることができます。  
暗号化：不規則な境界WiFiセキュリティは依然としてやや脆弱です。  
 ネットワーク内のすべてのデバイスがルーターのファイアウォールに穴を開けることができます。 DHSは2013年以来、人々がそれをオフにすることを推奨しています。  
WiFi Protected Setup（WPS）とともに使用されます  
PINを設定できますが、メカニズムでいくつかの攻撃が見つかりました。  
2007年3月、小売チェーンのTJ Maxxは、約4570万のクレジットカード番号がシステムから盗まれたと報告しました。 Wall Street Journalは、ミネソタ州セントポールでの安全でないWiFi接続のせいだと報告しました[1509]。  
パッチの適用が問題です。  
おもちゃから家電まで、IoTデバイスの大多数については、パッチが当てられることはありません。  
21.5.2.2 Bluetooth  
また、カメラや電話をラップトップに接続したり、キーボードをPCに接続したりするためにも使用されます。  
バージョン2.1（2007年にリリース）から  
中間者攻撃はより困難です。それらは、数値比較のために6桁の数を生成することによって処理されます。  
、番号をあるデバイスで生成し、別のデバイスでパスキーとして入力することもできます。中間者攻撃から保護されていない「ジャストワークス」モードがあります。  
ここでも、パッチの適用が問題です。  
したがって、パッチが適用されていないBluetoothチップを搭載したデバイスを使用している場合、脆弱性が存在する可能性があります。  
21.5.2.3 HomePlug  
HomePlug AVはWi-Fiエクステンダーで広く使用されています。1つのステーションをルーターまたはケーブルモデムに接続し、別のステーションを家の反対側にあるリモートWi-Fiアクセスポイントに接続します。  
 Bluetoothチームと同じ設計上の制約に直面しました。すべてのデバイスにキーボードまたは画面があるわけではなく、コストを低く抑える必要がありました。  
このモードでは、鍵は暗号化さえされていません。その目的はセキュリティを提供することではなく、デバイスが隣のネットワークと誤って結合する場合などの誤った関連付けを防止することです[1436]。他の人は、キーがすでにインストールされたエクステンダーをペアで販売しています。  
。  
この混乱の結果として、キー管理にほとんど依存することができません。  
21.5.2.4 VPN  
 通常、IPsecと呼ばれるプロトコルスイートを使用して、IP層で暗号化と認証を行います。  
保護されたパケットは、認証されたり、暗号化されたりします。前者の場合、データの整合性を保護する認証ヘッダーが追加されますが、後者の場合、パケットも暗号化され、他のパケットにカプセル化されます。  
 キーを設定し、パラメータをネゴシエートするプロトコル。EdSnowdenの開示から、これの標準のデフォルト設定（1024ビットDiffie-Hellmanを使用）  
VPNはファイアウォールベンダーによって提供されているため、ローカルLANとルーターの間の各ブランチにボックスの1つをインストールすることにより、すべての内部トラフィックをインターネット経由で暗号化して渡すことができます。  
VPNも商用で提供されており、たとえばイランや中国などの国の人々や企業が国のファイアウォールを迂回するために使用しています。  
21.6 CAとPKI  
当初、政府や電話会社がこれを行うと考えられていましたが、遅すぎました。  
 また、MicrosoftやNetscapeなどのソフトウェア会社は、公開鍵をブラウザに埋め込みました。  
その愚かさがなくなると、世界の政府は独自のCAのルート証明書をインテリジェンスと監視の目的でブラウザに取り込むように動きました。  
、これは、ターゲットのブラウザが受け入れるセキュリティ機関の公開鍵の証明書をwww.gmail.comに作成するCAを持つことを意味しました。  
この時点で男が聴衆の中で立ち上がって、「わが国を侮辱するなんて、あえてよ！ツビタクは諜報機関ではありません–それは研究組織です！」Mozillaの男は肩をすくめて肩をすくめながら言いました、「今度はガバナンスの証明がどれほど難しいかわかります。」その年の終わりにDigiNotarスキャンダルが起こりました。  
イランのエージェントは、イランで30万人のGmailユーザーを監視するためにハッキングしました。制裁措置は、トルコとは異なり、主要なブラウザーに政府の証明書をインストールすることはできないことを意味しました。  
これはオランダで本当の混乱を引き起こし、その多くのオンライン政府サービスはDigiNotar証明書を使用し、他のものを得るためにスクランブルをかけなければなりませんでした。  
それ以来、ブラウザのルートストアからCAと監査者への圧力が高まっています。  
’と‘（公開鍵）  
最初に、インフラストラクチャは、新しいアプリケーションが登場するときに使用できます。これをオープンPKIと呼びます。  
政府機関が攻撃する可能性が高いサービスを構築している場合は、自社の敷地内で実行されるCAを使用してPKIを閉じたままにしておくことをお勧めします。これにより、令状を知ることができます。  
PKIには固有の制限がいくつかあり、その多くは分散システムの章で説明しました。  
不要な名前を削除することで、物事を単純化できる場合があります。「Ross AndersonのキーはKRである」という1つの証明書ではなく、「Ross Andersonはx.foo.comを管理する権利がある」という別の証明書ではなく、「KRには管理する権利があるx.foo.com。」これは、「1つのキーまたは多数の」議論の側面です。  
 または、それぞれを別の資格情報に置き換える必要がありますか？  
バンキングと簿記の章で見たように、機器に別のメッセージを表示させることで、簡単にメッセージに署名させることができます。  
 電話帳の電子的な代替品を提供するために開発されたので、オープンPKIアーキテクチャでは誰もが一意の名前と一意のキーを持っていると想定することから始めました。  
•何百ものルート証明書の1つをFirefoxから削除すると、Mozillaがそれをサイレントに置き換えます。 Windowsにはさらに多くのルート証明書が付属していますが、完全に削除することはできません。  
•政府がWindowsで証明書を持っているが他のブラウザーでは持っていないという興味深い効果がありました（2014年の軍事クーデター後のタイなど）。  
•多くの企業は、古くなっている、または間違った会社に対応する証明書を使用します。これは、多くの場合、企業のマーケティング部門が請負業者に何らかのプロモーションを実施してもらうためです。最近のFirefoxなどのブラウザでは、過去の警告をクリックするのが難しくなっています。  
「拡張検証」証明書6を使用すると、状況は少し良くなりますが、完全に保証されているわけではありません。  
•証明書の取り消しは問題です。  
 CAから、彼らが依存しようとしていた証明書を確認します。  
さらに、一部のシステムのユーザー（特に米国政府のシステム）  
2013年頃から、人々はオンライン認定ステータスプロトコル（OCSP）に移行しました  
この混乱の背後には、いつものように安全保障経済学があります。  
 これは、ブラウザで緑色の南京錠を表示するために使用されていましたが、これはChromiumで2020年にv 76から廃止されました。  
コンプライアンスのコストはユーザーに捨てられました–ユーザーはしばしば対処することができません[524]。  
執筆時点での大きな問題は、証明書の寿命です。 LetsEncrypt;透明性を証明します。  
2017年と2019年の投票では13か月に削減することを提案し[1581]、2020年にAppleは9月からそのデバイスが398日より長い有効な証明書を受け入れないことを宣言して問題を強制しました[1446]。  
（また、ソフトウェアのアップグレードが難しいため、年次証明書を使用するシステムと、証明書を何年も保持する必要がある一部の産業用およびIoTシステムとの間のギャップも広がります。）  
ここでの変更メーカーは非営利のインターネットセキュリティリサーチグループ（ISRG）です  
証明書を無料にすることで完全な自動化が可能になり、コストが抑えられます。「LetsEncrypt」CAは、1億のサイトを1億ドルの予算でサポートします。  
このサービスは、スノーデンの啓示から2年後の2015年に始まりました。  
透明性ログがあり、システムには手動の上書きがないため、証明書の発行を強制されたことはありません。  
 2019年11月には、最大のCAとなり、1億8800万のドメインに1億2600万の証明書が発行されました。上位100サイトの5％、上位100サイトの35％でした。  
  
ComodoとDigiNotarへの攻撃に続いて、悪意を持って発行された証明書をブロックするメカニズムの研究が始まりました。  
Googleは2013年に最初の証明書の透明性ログを公開し、Chromeは2015年に拡張検証証明書のためにそのようなログを要求し始めました。  
 ドメイン所有者の知識なしで[1786]、2018年にすべてのCAに証明書の透明性を義務付けました。  
21.7トポロジ  
•公益事業には、信頼できるネットワーク上に数十から数百のデバイスを備えた発電機または変電所を含むアイランドがいくつかあり、専用のファイアウォールとVPNを介してネットワークコントロールセンターに接続されています。  
また、内部ネットワークは信頼できない場合がありますが、ネットワークの場所がアクセス制御の決定に関与しないという意味で、フロントエンドシステムによるDDoS攻撃から保護されている場合があります。  
ノードがユーザーで、エッジが互いのアドレス帳での存在である、より複雑なトポロジが見つかります。  
ソーシャルネットワークは、頂点次数のべき乗分布を持つグラフでモデル化できます。少数の適切に接続されたノードは、ランダムな障害に対するネットワークの回復力を高め、ナビゲートを容易にします。  
適切に接続されたノードを削除すると、ネットワークは簡単に切断されます[36]。  
現在、定量的モデルがあり、革命家が細胞内で組織化する傾向がある理由を説明するのに役立ちます[1373]。少数の適切に接続されたオーガナイザーに対してトラフィック分析を行うことにより、最初の場所でセル構造で組織された反体制派でない限り、警察は反体制派組織の驚くべき数のメンバーを特定できます[510]。  
21.8まとめ  
攻撃の種類とセキュリティテクノロジーの範囲が非常に広いため、困難です。  
多くのことが役立つ場合がありますが、魔法の解決策がある可能性は低いです。  
全体として、問題は非常に複雑で面倒なので、それらを管理するには、自動化によるシステム全体のアプローチが必要です。  
ただし、これらは悪者のエコシステム全体に発展しており、セキュリティエンジニアも調査および理解する必要があります。  
2010年までに、経済学と政策についてより多くの議論がありました。責任規則の変更が物事をどのように改善できるかについてです[97]。運用レベルでは、ゲームは自動化と統合に関するものであり、大企業が大量の脅威インテリジェンスとネットワーク監視情報を処理し、実用的なインテリジェンスに変換し、ネットワークセキュリティチームがどれだけ効果的に仕事をしているかを測定できるようにします。  
ウイルスに関する独創的な研究はFred Cohen [450]によるものであり、JavaセキュリティはLi Gong（設計者）によって議論されています。  
BGPのセキュリティについては、2011年のENISAレポートをご覧ください。Montyは200ページ以上あり、ネットワークセキュリティの博士号を取得する人向けに設計されていますが、エグゼクティブサマリーも短くなっています[1906]。  
認証機関のエコシステムの概要についてはよくわかりません。  
MicrosoftとNetscapeの最初の目標は、世界中のWebで電子商取引を開始することでした。証明書の使用はその後、パスワードやソフトウェアの更新にまで広がり、Javascriptが登場したとき、同じ起源の原則が信頼をWebサイトに移しました。  
技術的なセキュリティ目標と法的目標の間、および監査人と規制当局の間には矛盾があります。  
 およびETSI（最も関連性の高いヨーロッパ標準化団体）  
詳細については、エコシステムの問題[1785]に関するRyan Sleeviのプレゼンテーションは、技術的および運用上の現在の問題とその背景を掘り下げたい人に多くの指針を示しています。