–クリストファーストレイチーそれが確かに安全である場合、おそらく安全ではありません。  
1IntroductionPasswordsは、より一般的な概念であるセキュリティプロトコルの一例にすぎません。  
 プリンシパルが信頼関係を確立するために使用する手順を指定します。  
 チャレンジレスポンス認証やKerberosなど、すでにいくつかのプロトコルを利用しています。  
典型的なセキュリティシステムは、人々、会社、電話、コンピューター、カードリーダーなどのさまざまなプリンシパルで構成され、ファイバー、Wi-Fi、セルラーネットワーク、Bluetooth、赤外線などのさまざまなチャネルを使用して通信します。銀行カードや交通チケットとして。  
それらは、システムが電話での人々の嘘、ラジオを妨害する敵対的な政府、または偽造者が電車のチケットのデータを変更するなどの悪意のある行為に耐えるように設計されています。  
 たとえば、ユーザーにマシンにパスワードを入力してログオンさせる場合、ユーザーが正しいマシンにパスワードを入力できると暗黙的に想定します。  
 したがって、プロトコルの評価には2つの質問があります。1つ目は、脅威モデルが現実的かどうかです。次に、プロトコルはそれを処理しますか？1254。  
 パスワードの盗聴のリスクプロトコルは、バッジをリーダーに通して建物に入るなど、非常にシンプルな場合があります。  
 たとえば、レストランで高級ワインのボトルを注文する場合、標準的なプロトコルでは、ワインウェイターがメニューを提供します（価格は表示されますが、ゲストは表示されません）。彼らはボトルを持って来るので、ラベル、シール、温度を確認できます。彼らはそれを開いて味わうことができます。そしてサービット。  
 Matt Blazeは、チケット検査、航空セキュリティ、投票[260]から、他の非技術的なプロトコルの例を示しています。  
技術的には、プロトコルははるかに複雑になり、常に改善されるとは限りません。  
しかし、キーレスエントリへの移行により、キーが実際よりも車の近くにあるように見えるリレーデバイスを構築する方法を悪者が設定したため、車の犯罪が再び増加しています。  
 ヨーロッパは2000年代後半にこの動きを作りましたが、アメリカは2010年代後半に追いついています。  
 また、盗難犯が暗証番号を知らなくても、盗まれたチップカードを店で使用できるというプロトコルの失敗があり、銀行の修正には数年かかりました。  
4。  
 前の章でそれらの使いやすさについて説明しました。次に、あるマシンと別のマシンの間で動作するプロトコルを設計するときにブロックしなければならない種類の技術的攻撃について考えてみましょう。  
 ガレージを開けたり、1990年代半ばまでに製造された車のロックを解除したりするために使用されるリモートコントロールなどの初期のシステムは、シリアル番号をブロードキャストするだけです。  
 最初のグラバーは台湾からのようでしたが、1995年頃に市場に登場しました。泥棒は駐車場や標的の家の外に潜んでいて、車をロックするために使用された信号を記録し、所有者が行ったらそれを再生します1。  
 一般的なチップはPrinceton PT2262で、これは12個のトライステートピンを使用して312または531,441アドレスコードをエンコードします。  
 他の4つはチップの反対側にあるため、それらの多くは8つの入力のみを使用します。  
3。  
しかし、泥棒はあなたの家の外に潜んでいて、午前中に車で出かける前にロック解除コードを記録し、夜間に戻って自分自身を助けることができます。  
 時々、間違った車のロックを誤って解除したり、所有者が知らない車にアラームを設定したりすることがありました[308]。  
 コードは平均して約215回の試行後、1秒あたり10回で1時間未満かかります。  
次の対策は、パスワードの長さを16ビットから32ビットに2倍にすることでした。  
 しかし、これは彼らが問題を本当に理解していないことを示しただけです。  
シリアル番号をパスワードとして使用すると、さらに脆弱性が生じます。多くの人がシリアル番号にアクセスできます。  
 一部の強盗はシリアル番号をマスターパスワードとして使用していて、さらに悪いことに、銀行が盗難警報を購入すると、シリアル番号が注文書、納品書、請求書に表示されることがあります。  
単純なパスワードが適切な場合もあります。  
 私はまともな偽造品を作ることができると確信していますが、改札口の係員が「常連」を知るようになるので、これ以上高価なものは必要ありません。そして、車のように人々が盗みたいものには、もっと良いものが必要です。  
4。  
 トークンにはボタンが1つあります。ボタンを押すと、最初にそのシリアル番号が送信され、次に同じシリアル番号で構成される認証ブロックが送信され、その後に乱数が続きます。すべて、デバイス固有のキーを使用して暗号化され、送信されますガレージバリア（通常は434MHzの無線によるものですが、赤外線も使用されます）。  
次に、アクセストークンと駐車場の間のプロトコルは、次のように記述できます。 G：T、{T、N} KT組み合わせをすばやく、平均27回の試行後にガレージのドアを開けます。  
 現在は、ホームセキュリティシステムやおもちゃのリモコン用にも販売されています。  
3。  
トークンTは、ガレージGにメッセージを送信します。ガレージGには、その名前TにNを連結した暗号化されたTの値が続きます。Nは、「一度使用された回数」またはナンスを表します。  
 nonceの目的は、メッセージが新鮮であること、つまり古いメッセージの再生ではないことを受信者に保証することです。  
多くの人が混乱する1つの理由は、コロンの左側でプリンシパルの1つ（サブスクライバーを表すトークン）を識別するのに対し、右側ではトークンの名前（つまり、一意のデバイス番号）を意味するためです。  
だからあなたはTを考えるかもしれません！コロンの左側にあるGは、プロトコル設計者が何を考えていたかに関するヒントです。  
 乱数、カウンター、第三者から受け取ったランダムなチャレンジ、またはタイムスタンプです。  
 非常に低コストのシステムでは、一方向のみで通信する方が安価であり、安価なデバイスには通常時計がないため、乱数とカウンターが主流です。  
 典型的なガレージトークン製品では、各トークンのキーは、ガレージに知られているグローバルマスターキーKMで暗号化された一意のデバイス番号にすぎません。KT= {T} KMこれは、キー多様化またはキー派生と呼ばれます。  
 目標は、トークンをドリルダウンしてキーを抽出することでトークンを危険にさらす人物が、他のトークンになりすますことができないことです。彼ができることは、特定の加入者のトークンのコピーを作成することだけです。  
しかし、まだエラーの余地があります。  
 これは暗号化によってマスクできます。  
 どちらの場合も、可能なキーは216のみであり、セキュリティエンジニアリング128ロスアンダーソン4であっても十分ではありません。  
 誰が行くの？ –単純な認証それらはランダムに見える2。  
 例は、前払いユーティリティメーターの世界から来ています。  
 南アフリカで広く使用されていた初期のメーターの1つは、ナンスが前回と異なることのみを確認しました。  
。  
 有効と見なされた[93]。  
 乱数を使用する場合、ロックは多くの過去のコードを記憶する必要があります。  
 さらに、誰かが車を借りて、十分なロック解除コードを記録し、後でレンタルロットに戻ってそれを盗む可能性があります。  
カウンターを選択した場合、問題は同期です。  
したがって、カウンターが数百またはおそらく数千回増加した後に回復する方法が必要です。  
 トークンが他の場所で16回以上使用された（または家族のペットにかじられた）場合に対処するために、有効なコードが入力されてからカウンター値が17から32,767回増加した場合、2回目のプレスでロックが開きます（カウンターは、0が65,535の後継になるようにロールオーバーします。  
 あなたのアプリケーションでは、それについて心配しますか？したがって、単純なトークン認証メカニズムを設計することも、見た目ほど簡単ではありません。  
 多くのプリンタ会社は、認証メカニズムをプリンタに組み込んで、本物のトナーカートリッジが使用されるようにしています。  
 科学機器からゲーム機まで、あらゆる種類の業界がこの動きに加わっています。  
 しかし、裁判官は、LexmarkとSCCのケースで、ベンダーには顧客をロックするために見つけることができる最高の暗号技術者を雇う権利がありましたが、競合他社にも次の権利があることを発見しました2セクション5で詳しく説明します。 。  
1。  
セキュリティエンジニアリング129ロスアンダーソン4。  
 誰が行くの？ –簡単な認証他の場所からアクセサリを自由に購入できるように彼らが見つけた最高の暗号解読者を雇う。ここで、セキュリティは必ずしも良いことではないことを述べておきます。  
 効果は公共政策に反するかもしれない。 1つの例は携帯電話のロックです。その結果、何億ものハンドセットが毎年埋め立て処分になり、有毒な重金属や埋め込まれた炭素コストが発生します。  
3。  
 エンジンイモビライザーは、物理的な手段を使用してバイパスするのが難しく、2パスのチャレンジ/レスポンスプロトコルを使用してエンジンの始動を許可します。  
 車の鍵はチャレンジを暗号化することで応答を計算します。これは多くの場合、着信無線信号によって電力を供給される別のRFIDチップによって行われるため、バッテリーが切れていても動作し続けます。  
エンジンコントローラのE、車のキーのトランスポンダのT、トランスポンダとエンジンコントローラの間で共有される暗号キーのK、ランダムチャレンジのNを書くと、プロトコルは次のようになります。 T：NT�！ E：T、{T、N} Kこれは理論的には健全ですが、セキュリティメカニズムの実装は、多くの場合、最初の2、3回は失敗します。  
 攻撃には、プロトコルエラー、ピアキー管理、脆弱な暗号、輸出管理法で義務付けられている短いキーの組み合わせが含まれていました。  
 Stephen Bonoらは、2005年に、40ビットのキーを持つブロック暗号を使用していることを発見しました。これは、たった2つの応答から力ずくで計算できます[297]。  
2。  
1。  
 DST80は2020年にLennert Woutersと同僚によって破られました.Lennert Woutersと同僚は、チップへのサイドチャネル攻撃と同様に、鍵管理に深刻な実装上の問題があることを発見しました：現代の鍵には24ビットのエントロピーしかないが、トヨタの鍵はセキュリティから派生していますエンジニアリング130ロス・アンダーソン4。  
 誰が行くの？ –単純な認証攻撃者が読み取ることができるデバイスのシリアル番号（Teslaも脆弱でしたが、ソフトウェアのアップグレードで問題を修正できる古い会社とは異なります）[2048]。  
 さらに悪いことに、一部のタイプの車では、プロトコルのバグもあり、鍵の多様化が排他的に使用されている-またはKT = T�KM。  
また、2007年に、誰かがPhilips Hitag 2暗号を公開しました。これにも48ビットの秘密鍵がありました。  
 2016年までに、攻撃は8回の認証試行とラップトップでの1分の計算を要しました。彼らは日産、三菱そしてシボレーと一緒にすべてのフランスとイタリアのメーカーからの自動車に対して働いた[748]。  
 メガモス暗号を含み、バーミンガムとナイメーヘンからの研究者– Roel Verdult、Flavio GarciaおよびBarıBars Ege –がそれを解読した[1952]によってリバースエンジニアリングされた車の鍵鍛造ツールが2008年から市場に登場しました。  
 フォルクスワーゲンは、ロンドンの高等法院で、彼らのUsenix 2013での仕事の発表を停止するよう差し止め命令を出し、彼らの営業秘密が侵害されたと主張した。  
 2年間の議論の後、訴訟はどちらの側にも責任を認めることなく解決した。  
 攻撃者が96ビットキーの各16ビットワードを次々に書き換えて、一度に16ビットのキーを検索できるため、プロトコル攻撃もあります。これにより、攻撃に必要な時間が数日から数分に短縮されます[1953]。  
 多くのフォルクスワーゲンの実装では、車やトランスポンダ間でキーを分散させることはしませんでしたが、一度に数百万台の車に固定グローバルマスターキーを使用しました。  
車が脆弱かどうかは簡単にわかります。スペアキーを購入してみてください。  
 前の所有者が購入した妻の2005年型レクサス用のスペアキーがあります。  
もう1つの例は、衛星TVセットトップボックス内の加入者スマートカードです。これについては、後で説明します。  
 盗難を容易にする方法で、また改ざん防止チップを使用してそれらを保護することなく、ユニバーサルマスターキーを車などの貴重な資産にインストールすることは、重大なエラーでした。  
3。  
第3章で、パスワードシステムの設計の難しい部分は、回復メカニズム自体が脆弱性または迷惑になることなく、侵害から回復することでした。  
チャレンジレスポンスは非常に良さそうだったため、自動車メーカーは、金属製のキーではなく、ダッシュボードのジャスタプッシュボタンを使って車を始動しました。  
 マーケティングピッチでは、キーをポケットやハンドバッグに入れていれば、心配する必要はありません。近づくとロックが解除され、離れるとロックされ、コントロールに触れると自動的に開始します。 。泥棒は、1つのリレーで玄関に忍び寄り、もう1つのリレーを車の隣に置きます。  
車が固定されていても、彼はあなたの敵を盗むことができます。  
重要なメッセージは、1990年ごろから暗号化技術を使用して車を盗むのを難しくする試みは、イモビライザーが車を盗むのを難しくし、保険料が下がったため、最初の成功はありました。  
 政治家は、もし人々が車の盗難を止めたとしても、解読できない暗号を使用することが許されれば、法執行機関にとって悲惨なことになるだろうと述べた。  
私たちは何ができる？まあ、少なくとも2つの自動車メーカーが加速度計をキーフォブに入れているので、キーが動いていないと機能しません。  
地元の警察は、昔ながらの金属製のステアリングホイールロックを使用するようにアドバイスしています。自治会は鍵をビスケット缶に保管することを推奨しています。  
それで我々はその車を取り戻し、適切なプッシュボタンのリモートロック付きの中古車を手に入れました。  
ただし、暗号自体はリレー攻撃を修正できません。適切な修正は、固有のレンジングを備えたウルトラワイドバンド（UWB）に基づく新しい無線プロトコルで、キーフォブから車までの距離を10cmから150mの範囲の精度で測定します。  
15。  
偶然にも、車内のCANバスで使用される認証プロトコルは、いくつかの点で脆弱です[891]。  
セキュリティエンジニアリング132ロスアンダーソン4。  
 誰が行くの？ –シンプルな認証最初のチップが2019年に利用可能になり、2020年から車で出荷されます。  
私が自動車のスタートアップに助言していたら、LRPが私の出発点になります。  
 HTTPDigest認証では、Webサーバーはナンスを送信することにより、パスワードを共有するクライアントまたはプロキシにチャレンジします。  
これにより、パスワードスヌーピングに対して脆弱ではないメカニズムが提供されます。  
 平文でパスワードを送信するよりもはるかに優れていますが、キーレスエントリのように、中間者攻撃から被害を受けます（受益者は偽物です）。  
3。  
 多くの組織では、パスワードジェネレーターを使用して企業のコンピューターシステムにログオンできるようにステータスを発行し、多くの銀行では同様のデバイスを顧客に提供しています。  
 ログインするときは、7桁のランダムなナンスが表示されます。  
 デバイスは、企業のセキュリティサーバーと共有する秘密鍵を使用してこれらの11桁を暗号化し、結果の最初の7桁を表示します。  
 このプロトコルを図4に示します。  
 正しい秘密鍵を持つパスワードジェネレーターがあり、PINの権利を入力し、その結果を正しく入力した場合は、次に進みます。  
 キーボードを持たない単純化されたバージョンがありますが、カウンターまたはクロックを暗号化することによって新しいアクセスコードを生成するだけです。  
これは、詐欺師が銀行の顧客を大規模にフィッシングし始めたちょうどその時だったので、多くの銀行がこの技術を採用しました。  
私の他の銀行では、Chip Authentication Program（CAP）、aSecurity Engineering133Ross Anderson4を使用しています。  
 誰が行くの？ –簡単な認証？  
 。  
 。  
1：–パスワードジェネレーターusecalculatorで、銀行カードを挿入して暗号化を実行できます。  
 この本の第2版では、「あなたの銀行カードをナイフポイントで受け取った人が、あなたが正しいPINを伝えたことを確認できるようになりました」と書きました。  
 そのような攻撃がどのように機能するかを確認するために、軍事的な例を見てみましょう。  
3。  
 1930年代と1940年代の戦闘機の速度の増加により、ジェットエンジン、レーダー、ロケットの発明により、防空部隊が敵の航空機と区別できるようになりました。  
 これらは第二次世界大戦で最初に発見され、レーダーに照らされた飛行機が友好的な意図を伝えるために識別番号を放送することを可能にしました。  
 今日、典型的な防空システムはレーダー信号でランダムなチャレンジを送信し、友好的な航空機は正しい応答で自分自身を識別できます。  
 問題の1つは、南アフリカ空軍（SAAF）の兵士から聞いた次のストーリーに示されています。  
3。  
 いずれにせよ、第二次世界大戦以降、他の電子戦システムで同様のゲームがプレイされています。  
1980年代後半、南アフリカ軍はナミビア北部とアンゴラ南部で戦争をしていた。  
 サウスアフリカ防衛軍は主に小さな白い人口からの徴集兵で構成されていたため、死傷者を制限することが重要でした。N？N？ANGOLANAMIBIASAAFMIGN？N KSAAFN KN K図4。  
 彼らの空軍の優位性が失われたというこの証拠は、プレトリア政府がナミビアをセキュリティエンジニアリング135ロスアンダーソン4に引き渡すことを決定するのを助けました。  
 誰が行くの？ –シンプルな認証インサージェント–それ自体が数年後の南アフリカでの多数決への道への大きな一歩です。  
数年後、SAAFの関係者から、キューバ人がどのようにそれを引き出したのかがわかりました。  
 その後、MIGは鋭く向きを変え、SAAFの防空壕を通過し、IFFに挑戦しました。  
2。  
 黒人の対戦相手に勝っただけでなく、実際には裏をかいていたことは、彼らがそれまで保持していた世界観と一致していませんでした。  
 彼は、彼らのIFF機器はアンゴラ戦争の時点ではまだ暗号化を使用しておらず、常に敵の領土に切り替えられていたと述べました。  
しかし、「ミグインザミドル」のトリックは、韓国、ベトナム、およびさまざまな中東の紛争で顕著だったと言う人もいます。  
 車に対するリレー攻撃は別の例です。  
 銀行はチャレンジを送信します。フィッシャーマンはこれをマークに中継し、マークにデバイスを使用します。フィッシャーマンは応答を銀行に中継し、銀行はフィッシャーマンをマークとして受け入れます。  
 銀行は通常、既知のマシン、パスワード、CAPリーダーからの認証コードなどの2番目の要素、およびトランザクションのリスク評価を探します。  
 ただし、使いやすさのため、最後の4桁のみを認証します。  
 また、悪意のあるユーザーはフォールバックメカニズムを悪用して、おそらく顧客とコールセンターの間で中間者攻撃を実行する電話番号に顧客をスプーフィングする可能性があります。  
このような攻撃は、インターネットセキュリティプロトコルからBluetoothまでのアプリケーションで何度も発生します。  
 数学者のジョンコンウェイがかつて述べたように、郵便チェスでグランドマスターに対して少なくともドローを手に入れるのは簡単です。2人のグランドマスターを同時にプレイし、一方をホワイトとして、もう一方をブラックとしてプレイして、それらの間の動きを中継してください！セキュリティエンジニアリング136ロスアンダーソン4。  
 誰が行くの？ –簡単な認証4。  
4反射攻撃2人のプリンシパルがお互いを識別する必要がある場合、さらに興味深い問題が発生します。  
 ここで、空軍が各航空機にエアガンナーのチャレンジユニットの1つを設置し、それを射撃管制官に接続したと仮定します。  
 上の例では、チャレンジに応答するために友好的な爆撃機が必要になる場合があります。F!! B：次のような応答がある場合：B�！ F：{B、N} KTは、ウィングマンF 0からの反映された応答{F 0、N}を検出できました5。  
 チャレンジNを送信し、20ミリ秒以内に応答{N} Kを受信すると、光は20ミリ秒で3,730マイルを少し下回ることができるため、キーKを持つ人物が2000マイル以内にいることがわかります。 。  
 自分の機器を使用して応答が計算されなかったことを確認できれば、キーKを持っている人が2000マイル以内にいることがわかります。  
 信頼性の仮定とその結果の注意深い分析は、セキュリティプロトコル設計の中心です。  
 しかし、最も重要な問題の1つ、および初期のIFFシステムの設計者が予期していなかった問題の1つは省略しました。  
同盟国はこれを困難な方法で学んだ。 1944年1月に、5の暗号化を解除します。忘れないでください。また、侵入者が自分の攻撃を自分に反映していないことも確認する必要があります。  
4。  
 そのため、より近代的なシステムは、チャレンジと応答を認証します。  
 理論的には敵の領域を切り替える必要はありませんが、実際には有効なチャレンジを記録できる敵は攻撃の一部としてそれらを再生できます。  
その他のIFF設計の問題には、ニュートラルによって引き起こされる困難、高密度の運用環境でのエラー率、機器の障害に対処する方法、キーを管理する方法、および多国籍連合に対処する方法が含まれます。  
 とりあえず、疑似チャレンジの問題は重要なポイントを補強するのに役立ちます。つまり、セキュリティプロトコルの正確さは、要件についての仮定に依存するということです。  
 実際、第二次世界大戦では、疑似チャレンジの問題が非常に深刻になり、何百人もの隊の爆撃機パイロットが命令を無視して敵の領土にいる間にIFFをオンのままにしておくというリスクを負うのではなく、一部の専門家がIFFを完全に放棄することを提唱しました。4メッセージの操作これまでに、参加者の認証に使用される情報を反映または偽装する中間者攻撃が数多く見られました。  
すでに見た1つの例は、最後に見たチケットのみを記憶する前払いメーターです。そのため、2つのチケットAとBのコードを次々とコピーすることにより、無制限に再チャージできます。  
。  
 もう1つのケースは、不正なキャビが、タクシーのギアボックス内のセンサーにタクシーメーターを接続するケーブルにパルス発生器を挿入するときです。  
 海賊装置は余分なパルスを挿入できるため、タクシーはさらに進んだように見えます。  
 そのような攻撃については、セクション14の「MonitoringSystems」の章で説明します。  
監視システムと同様に、制御システムはメッセージ操作攻撃に対して強化する必要があることがよくあります。  
 特定のアプリケーションに関する後の章で、メッセージ操作を伴うプロトコル攻撃の多くの例を見ます。  
5。  
5環境の変更プロトコル障害の一般的な原因は、環境が変化し、設計の前提が失われ、セキュリティプロトコルが新しい脅威に対処できなくなることです。  
 1993年、オランダは「ファントム撤退」の蔓延を抑えました。マスコミで多くの論争があり、銀行は彼らのシステムが安全であると主張し、多くの人々は騙されたと主張して新聞に書いた。  
 これはステーキングされ、スタッフの1人が逮捕されました。  
 2000年代半ばに「チップとPIN」スマートカードに移行した後、英国でもまったく同じ詐欺が起こりました。ギャングはおそらく200の充填ステーションを盗聴し、ワイヤーからカードデータを収集し、CCTVカメラを使用してPINを観察し、ATMがまだ磁気ストリップ技術を使用している国で使用されている磁気ストリップクローンカードの数千の​​砂を作りました。  
システムの設計がひどく悪かったのはなぜですか。また、10年以上にわたって大きなテクノロジーの変化によって設計エラーが長引いたのはなぜですか。まあ、磁気ストライプカードとPINを管理するための標準が1980年代初頭にIBMやVISAなどの組織によって開発されたとき、エンジニアは2つの仮定をしていました。  
 （使用された類推は、磁気ストリップがあなたの名前であり、PINがパスワードであるというものでした。  
 したがって、PINパッドからサーバーに向かう途中で、PINを暗号化することだけが「明らかに」必要でした。磁気ストリップのデータは、カードリーダーからクリアテキストで送信できます。  
 1980年代後半の極東でのカード偽造の蔓延により、銀行は磁気ストリップに認証コードを導入しました。  
 これら2つの環境変化の組み合わせにより、元のシステムアーキテクチャの背後にある仮定が破壊されました。  
 これらの変化は非常にゆっくりと、そして非常に長い期間にわたって行われていたため、業界は問題の発生を認識していませんでした。  
6Chosen Protocol Attacks IDカードのプッシュに熱心な政府は、IDカードを他の多くのトランザクションに使用させようとしました。 ID、バンキング、さらにはセキュリティエンジニアリング139Ross Anderson4に1枚のカードを使用したい人もいます。  
 選択されたプロトコル攻撃  
 これはいくつかの興味深い新しいリスクをもたらしました：aNavyキャプテンが良い夕食後にATMから現金を引き出そうとしてPINを忘れた場合、月曜日の朝、銀行を開いてカードを返却するまで船を海に連れて行くことができませんか？一部の企業は、さまざまなトランザクションで使用できる多機能認証デバイスを推進して、数十種類の異なるカードとキーを持ち歩く必要をなくしています。  
しかし、これも見た目ほど簡単ではないかもしれません。  
 では、マフィアはどのように銀行取引の認証を攻撃するプロトコルを設計するのでしょうか？これが1つのアプローチです。  
 すべてを認証するためにスマートフォンが使用されている場合、ポルノサイトが年齢の証明としてランダムなチャレンジを認証するように顧客に依頼するのは当然です。  
3。  
コインディーラーが認証のためにトランザクションデータを送信すると、ポルノサイトを通じて待機している顧客にデータが中継されます。  
sigK XPicture 143！Mafiaporn�siteCustomerBuy10ゴールドコイン購入年齢を証明「X」に署名して「X」�BANKsigKX図4。  
 それ以来、多くのプロトコルは、それ自体は安全ですが、ユーザーが他のアプリケーションで同じキーを再利用するように仕向けられると、破られる可能性があることが示されています[1032]。それは、アクセス制御に関する次の章の主題になります。  
7。  
 古典的なケースは、銀行が認証コードとして顧客にSMSを送信する際に2要素認証を利用する場合です。  
4。  
4。  
 非常に重要な認証プロトコルのクラスがもう1つあります。暗号化キーの管理に使用されるプロトコルです。  
7。  
車両は初期の例を提供しました。  
 同じ問題が、運転手が運転時間と速度を監視するためにトラックが使用する装置であるタコグラフでも逆に起こりました。  
 しかし、キーはどのように管理できますか？解決策は、工場出荷時のリセット後に新しいタコグラフに電源が投入されるたびに、センサーケーブルを介して受信した最初の暗号キーを信頼することでした。  
3。  
 デフォルトの「ジャストワーク」モードでは、新しいHomeplugデバイスは最初に見たキーを信頼します。新しいWi-Fiエクステンダーが隣のWi-Fiとかみ合う場合は、リセットボタンを押して再試行するだけです。  
TOFUアプローチは、フランクスタハノと私がタコグラフ作業のコンテキストで行った分析の結果、「復活したアヒルの子」としても知られています。  
 そのような誤ったインプリンティングが電子デバイスで起こった場合、それを殺して新生児の状態に復活させる方法が必要です–リセットボタンはそれを行います[1819]。  
7。  
7。  
 基本技術は1970年代後半から分散型コンピュータシステムのキーを管理するために開発され、現金自動支払機が初期のアプリケーションです。  
キー配布プロトコルの背後にある基本的な考え方は、2人のプリンシパルが通信する必要がある場合、信頼できるサードパーティを使用してそれらを紹介する可能性があるということです。  
したがって、通信する2つのプリンシパルを「アリス」と「ボブ」、信頼できるサードパーティを「サム」と呼びます。  
 （たとえば、カーディラーが交換用のキーを車と嵌合させるプロトコルでは、アリスが車、ボブがキー、サムが車のメーカーである場合があります。  
1。  
2。  
 それぞれにキーのコピーが含まれています。最初のキーは暗号化されてアリスのみが読み取ることができ、2番目のキーは暗号化されてボブだけが読み取ることができます。  
 次にアリスはボブに電話し、2番目の証明書を紹介として提示します。  
 これで、アリスはキーを使用して、暗号化されたメッセージをボブに送信し、彼からのメッセージを受信することができます。  
 証明書の有効期限が切れない場合は、特権が取り消されたユーザーを処理するときに深刻な問題が発生する可能性があります。  
サムは、アリスの名前、ボブの名前、使用するセッションキー、およびタイムスタンプで構成されるメッセージを作成します。  
 彼は両方の暗号文をアリスに渡します。  
 彼女は、このセッションキーを使用して暗号化し、送信したいすべてのメッセージを彼に送信します。  
7。  
7。  
多くの既存の鍵配布プロトコルは、1978年に登場したNeedham-Schroederprotocolから派生しています[1426]。  
 次のように実行されます。メッセージ1A！ S：A、B、NAMessage 2S！ A：{NA、B、KAB、{KAB、A} KBS} KASMessage 3A！ B：{KAB、A} KBSメッセージ4B！ A：{NB} KABMessage 5A！ B：{NB�1} KABHereアリスが主導権を握り、サムに次のように伝えます。「私はアリスです。ボブと話したいのですが、私のランダムなナンスはNAです。  
この暗号文にはナンスも含まれているため、リプレイではないことを確認できます。  
 彼女はそれをボブに渡し、ボブは自分がいることを警告応答で確認します。  
 これは必ずしもそうではありません。アリスはステップ2と3の間に1年待っていた可能性があります。  
 しかし、対戦相手（チャーリーなど）がアリスのキーを手にしたことがあれば、それを使用して他の多くのプリンシパルとのセッションキーをセットアップできます。  
 つまり、失効が問題です。サムはこれまでに行ったすべての完全なログを保持する必要がある可能性があり、これらのログは、プリンシパルの名前が将来の一定の時点で期限切れにならない限り、永久にサイズが大きくなります。  
 単純化した見方では、ニーダムとシュローダーはちょうどそれを誤解しました。 SusanPanchoとDieter Gollmann（私は同情します）が主張した見解は、これは仮定を変えることによってもたらされたプロトコルの失敗であるというものです[780、1491]。  
 ニーダム・シュローダーの論文は、すべてのプリンシパルが自分自身で行動し、すべての攻撃は部外者からのものであると想定していました[1426]。  
4。  
4KerberosNeedham-Schroederプロトコルの最も重要で実用的な派生物はKerberosです。これはMITで開発された分散アクセス制御システムで、現在は標準のネットワーク認証ツールの1つです[1826]。  
 Kerberosには、単一の信頼されたサードパーティの代わりに、2つの種類があります。セキュリティエンジニアリングの対象となる認証サーバー143Ross Anderson4。暗号化キーの管理ユーザーはログオンし、チケット許可サーバーはチケットを提供して、ファイルなどのさまざまなリソースへのアクセスを許可します。  
 たとえば、ある大学では、カレッジや学生寮を通じて学生を管理し、部門ごとにファイルサーバーを管理する場合があります。会社では、部門の管理者がサーバーやプリンターなどのリソースを管理している間に、人事担当者が給与計算システムにユーザーを登録する場合があります。  
 彼女のPCのクライアントソフトウェアは、彼女のパスワードで暗号化され、セッションキーKASを含むチケットをこのサーバーからフェッチします。  
 その結果は、タイムスタンプTSとライフタイムLを持つキーKABであり、そのリソースを使用してAliceの後続のトラフィックを認証するために使用されます。 S：A、BS！ A：{TS、L、KAB、B、{TS、L、KAB、A} KBS} KASA！ B：{TS、L、KAB、A} KBS、{A、TA} KABB！ A：{TA + 1} KABこれを英語に翻訳：アリスはチケット認可サーバーにBへのアクセスを要求します。  
 彼女はまた、彼女が読める形式、すなわちKASで暗号化された形式でキーのコピーを取得します。  
Needham-Schroederプロトコルの失効問題は、ランダムなノンスではなくタイムスタンプを導入することで修正されました。  
 これで新しい脆弱性が発生しました。つまり、さまざまなクライアントとサーバーのクロックが同期しなくなる可能性があります。より複雑な攻撃の一部として、意図的に非同期化される場合もあります。  
 この機能を備えたプロトコルは、セクション26で説明するように、1990年代の「暗号戦争」の間に支持されました。  
7。  
Kerberosとかなり類似したプロトコルはOAuthであり、これは安全な委任を可能にするメカニズムです。  
 Doodleは、カレンダーサービスのアクセストークンを提供します[863]。  
4。  
3これは、クロスサイトフィッシングのリスクをもたらすことを示しています。  
 これは委任メカニズムを構築できる複雑なフレームワークであり、短期および長期の両方のアクセストークンを使用します。詳細は、CookieとWebリダイレクトがどのように動作および最適化されるかに関連付けられており、サーバーがステートセキュリティエンジニアリングになることを可能にします144Ross Anderson4。  
 設計保証がないため、最新のWebサービスに合わせて拡張できます。  
 この複雑さのため、OpenID ConnectプロトコルはOAuthの「プロファイル」であり、必要なサービスが認証のみである場合の詳細を拘束します。  
4。  
5実用的なキー管理各ユーザーが1つ以上の長期キーをキー配布センターとして機能するサーバーと共有している場合、Kerberosのようなプロトコルを使用してユーザー間の作業キーを設定および管理できます。  
 これは多くの重要な資料です。  
 座って、どのように多くのキーが必要であるか、どのように生成されるか、どのくらいの期間サービスを維持する必要があるか、そして最終的にどのように破棄されるかについて考える必要があります。  
 そして、アプリケーションが進化するにつれて物事はうまくいきません。来年の機能をサポートするためのヘッドルームを提供することが重要です。  
 それでも、標準的な方法はありません。  
 銀行業務では、通常、ハードウェアセキュリティモジュールと呼ばれる専用の暗号化プロセッサを使用します。これについては、後で詳しく説明します。  
4。  
 この演習の目的は、プロトコルが正しいか間違っているかを最初に決定することでした。プロトコルが正しいことを証明するか、攻撃を示す必要があります。  
プロトコールの正確性を検証するためのいくつかの異なるアプローチがあります。  
 それは、プリンシパルが特定のメッセージ、タイムスタンプなどを見たと合理的に信じているかもしれないことについて推論します。  
形式的な方法を使用して正しいことが証明されたプロトコルで見つかったフローのいくつかの歴史が存在します。第2版​​の第3章で、BANロジックを使用して、stored-Security Engineering145Ross Anderson4に使用される銀行カードを検証する方法の例を説明しました。  
 概要価値の支払い。  
 したがって、私はこの版から悲惨な詳細を削除することにしました。第2版​​はオンラインで無料なので、詳細をダウンロードして読むことができます。  
 しかし、彼らにも限界があります。  
 たとえば、Larry Paulsonは、1998年にhisIsabelle定理証明者を使用してSSL / TLSプロトコルを検証しました。それ以来、毎年約1つのセキュリティバグが発見されています。  
 この場合、正式な方法の失敗はありませんでした。それは単に攻撃者に迷惑をかける必要がないことを伝えました。  
 Justasの構造化プログラミング手法は、ソフトウェアが確実に設計され、重要なものは何も除外されないようにすることを目的としています。複数の方法でデータを解釈することはできません。したがって、メッセージ形式では、名前、住所、タイムスタンプなどを明確にする必要があります。文字列形式は明確でなければならず、プロトコル自体を使用して、それを処理するソフトウェアへの攻撃（たとえば、バッファオーバーフロー）を開始することは不可能であるべきです。  
 プロトコルが公開鍵暗号化またはデジタル署名メカニズムを使用している場合、微妙な攻撃とさらなる堅牢性の問題があります。これらは次の章で取り組み始めます。  
4。  
プロトコルは、プリンシパルがシステムで信頼関係を確立するために使用する手順（IDに対する要求の認証、資格情報の所有権の証明、リソースに対する要求の確立など）を指定します。  
 セキュリティプロトコルは、すべてのSecurity Engineering146Ross Anderson4に実装されています。  
 リモートの車のドアロックから軍用のIFFシステムを介して、分散型コンピュータシステムの認証まで、さまざまなシステム。  
 彼らは、中間者攻撃、修正攻撃、反射攻撃、およびリプレイ攻撃を含む、多くの問題に耐えることができます。  
 数学的手法を使用してプロトコルの正確性を検証することは役立ちますが、すべてのバグをキャッチすることはできません。  
その結果、攻撃は依然として私たちが長年使用してきたプロトコルで頻繁に見られ、時にはセキュリティの証拠があると考えられていたプロトコルでも見つかる場合があります。  
 独自のプロトコルに署名しないでください。専門家に協力を求め、研究コミュニティによる徹底的な査読のために設計が公開されていることを確認します。  
 現金の面でも評判の面でも、プロトコルが実際に展開される前にバグを修正するのはかなり簡単です。  
 それらは、探求されるべき新しいエラーと攻撃の新しい作物を伴う新しいアプリケーションの出現によって繰り返し間違っていることが証明されました。  
2000年以降、セキュリティメカニズムがビジネスモデルをサポートするためにますます使用されるようになったため、プロトコル研究の1つのストランドが経済的傾向を獲得しています。デザイナーの「敵」は、多くの場合、商業的競争相手、または顧客ですらあります。  
多くのプロトコル研究は問題主導型ですが、まだ深い疑問があります。  
 歴史的な背景については、元のニーダムシュローダーの論文[1426]、バロウズアバディニーダム認証ロジック[357]、プロトコルの堅牢性に関する論文[2、112]、およびアンダーソンアンドセキュリティエンジニアリング147ロスアンダーソンによる調査論文4をお読みください。  
 概要ニーダム[113]。  
 車のリモートキー入力やその他のセキュリティ問題については、ジープチェロキーのハッキング方法に関するチャーリーミラーとクリスヴァラセックの技術レポートが良い出発点です[1316]。