– LESLIE LAMPORT [1123]名前は何ですか？我々が他の名前をバラバイと呼ぶものは、甘い香りがするでしょう–ウィリアム・シェイクスピア7。  
いくつかのことは迅速に、または正しい順序で行う必要があり、数台のマシンで対処するのが簡単な問題は、復元力のために複雑な配置のハイパースケールデータセンターがあると大きな問題になります。  
過去50年間、電話システムや決済ネットワークからインターネット自体に至るまでさまざまなものを構築してきたため、同時実行性、障害回復、ネーミングなどの問題について多くを学びました。  
 これらの問題は、堅牢な安全なシステムの設計の中心ですが、多くの場合、かなりひどく処理されます。  
システムをフォールトトレラントにするためにデータを複製すると、データ盗難のリスクが高まる可能性があります。  
人やオブジェクトとアカウント、セッション、ドキュメント、ファイル、ポインタ、キー、その他の命名方法との複雑な相互作用があります。  
 多数の識別子を扱うビッグデータ手段は、多くの識別子があいまいであるか、変更さえあり、多くのことがうまくいかない場合があります。  
2。  
2ConcurrencyProcessesは、同時に実行できる場合は同時実行と呼ばれ、これはパフォーマンスにとって不可欠です。現代のコンピューターは多くのコアを持ち、一度に多くのプログラムを実行します。  
 プロセスは古いデータを使用する場合があります。一貫性のない更新を行う可能性があります。市長の更新の順序は重要ではありません。システムがデッドロックする可能性があります。異なるシステムのデータが一貫した値に収束することはありません。正しい順序で物事を行うことが重要な場合、または正確な時間を知ることさえ重要である場合、これは想像以上に難しい場合があります。  
さまざまな理由により、システムの並行性はますます高まっています。  
 2つ目は、デバイスの複雑さです。高級車は現在、数十から数百の異なるプロセッサーを搭載できます。  
 各CPUの奥深くでは、命令が並行して実行され、この複雑さが、アクセス制御に関する章で説明したSpectre攻撃につながります。  
 次に、相互作用の複雑さがあります。アプリケーション層に行くと、レンタカーの予約などの日常のトランザクションが他のシステムを呼び出して、クレジットカード、信用照会機関のスコア、保険金請求履歴などを確認しますが、これらのシステムは次のシステムに依存する場合があります。他の人に。  
 コンピュータ科学者はアムダールの法則を教えられています。並列化できる比率がpであり、sが追加リソースによるスピードアップである場合、全体のスピードアップは（1�p+ p / s）�1です。  
 しかし、現実世界での同時実行制御もセキュリティの問題です。  
 また、同時実行性の問題は、ハードウェアからビジネスロジックまで、システムの多くのレベルで発生する可能性があります。  
7。  
1古いデータを使用して支払うことと状態を伝播するために支払うことすでに2種類の同時実行性の問題について説明しました。攻撃者が古い資格情報を渡して管理するプロトコルに対するリプレイ攻撃。 andrace条件。2つのプログラムが競合して、セキュリティ状態を更新できます。  
 別の例は、1（1�34 +34。  
25 + 0。  
34375）�1= 2。  
2。  
 ユーザーは、ファイルが[1129]の間に変更されるように、物事を整理することができました。  
ファイルシステムでこのような攻撃を見つける体系的な方法がありますが[251]、攻撃は仮想化環境でのシステムコールなどの低いレベルとビジネスロジックなどの高いレベルの両方で発生します。  
良い事例研究はカード詐欺です。  
 すべての損失レポートを数千万のデバイスに瞬時にブロードキャストする必要があるため、完全なホットカードリストをすべてのマーチャントターミナルに保持することは不可能であり、カードを発行した銀行とのすべてのトランザクションを確認しようとしても、ネットワークのない場所（遠隔地の村や飛行機の中など）ではカードを使用できず、他の場所では許容できないコストと遅延が発生します。  
マーチャント端末は、特定の制限（フロア制限）までのトランザクションを処理できます。大規模な取引では、すべてのローカルホットカードと不正に使用されている外部カードについて知っている、販売者の銀行とのオンライン検証が必要です。別の制限を超えると、トランザクションは、かなり最新の国際リストを持つVISAなどのネットワークを参照する可能性があります。一方、最大の取引にはカード発行銀行への参照が必要です。その後、経験により、集中化されたアプローチの方が悪い端末に対してより効果的に機能することがわかりました。  
 FICOは、犯罪者が盗んだ数枚のカードを現金自動預け払い機に持ち込み、1枚ずつ試すことを観察しました。彼らは最近試みられた詐欺のために最近使用された世界中の40のATMのリストを維持し、そのサービスに加入している銀行はそれらのマシンでのすべてのトランザクションを拒否します-それらはそれらの銀行のカードによっておそらく30分使用できなくなります。  
2010年頃まで、ペイメントカードネットワークにはセキュリティ状態のグローバルな伝播を管理する最大のシステムがあり、その経験から、侵害された資格情報を迅速かつグローバルな規模で取り消すにはコストがかかることがわかりました。  
セキュリティ状態の伝播のコストは、集中化につながる可能性があります。  
セキュリティエンジニアリング238ロスアンダーソン7。  
 並行性認証局などの他の企業もオンライン資格情報を提供します。  
たとえば、2011年には、イランのIPアドレスから操作するハッカーがオランダの認証局Diginotarを侵害しました。  
 Diginotarは19日、証明書が誤って発行されたものの、監査人を呼び出しただけであることに気付きました。  
 これにより会社はすぐに失敗し、オランダの公共サービスは、他のサプライヤーからWebサービスの証明書を取得するために省庁が奪い合い、何日もオンラインで利用できなくなりました[471]。  
2。  
 ロックは、ファイルシステムなどのリソースの競合を管理し、競合する更新の可能性を低くする一般的な方法の1つです。  
クレジットカードは、これがセキュリティにどのように適用されるかを示す例です。  
 これは、承認システムと決済システムを分離することによって実装されます。  
 カードが翌日にキャンセルされた場合、私の銀行は私に電話して、警察に連絡するか、または彼女に現金を支払わせるように頼むことができます2。  
ただし、コールバックメカニズムは、汎用的なソリューションを提供しません。  
別の例としてパスポートを考えてみましょう。  
 実際、ますます多くのトランザクションでAadhar生体認証IDシステムを使用するというインド政府の要件に対する頻繁な異議の1つは、すべての重要なトランザクションで市民の指紋または虹彩コードをチェックすると、ビジネスを行ったすべての場所の監査証跡が作成されることです。ソーシャルメディア、および賄賂を必要とするすべての人が利用できます。  
 カードが複数の大きな購入に使用できるように、詐欺師が店を偽装し、承認を取り消す方法を考え出したときも、しばらくの間攻撃がありました。  
 これらすべての詳細は、それ自体が本の章になります。セキュリティエンジニアリング239ロスアンダーソン7。  
 同時実行性クレジットカードなどの発行者に何らかの義務を生じさせるクレデンシャルとパスポートなどのその他のクレデンシャルの間には、一般的な違いがあります。  
これは、更新が行われる順序が重要かどうかに関連しています。  
2。  
 しかし、彼らが私の銀行口座に到着した場合、注文は結果に大きな影響を与えます。実際、トランザクションが適用される順序を決定する問題には、明確な解決策がありません。  
従来の銀行アルゴリズムでは、トランザクションを一晩でバッチ処理し、すべての借方を適用する前に、各口座にすべてのクレジットを適用していました。  
 返送された支払いは取り消す必要があります。また、ATMやデビット取引の場合、すでにキャッシュがなくなっている場合は、顧客が無許可でお金を借りることになります。  
 近年、次々とリアルタイムグロス決済（RTGS）システムが導入され、到着順にトランザクションが予約されています。  
 まず、多くの教育機関では、小売顧客向けのリアルタイムシステムは、プラットフォームのオーバーレイであり、夜通しの更新でも機能します。  
 クレジットカードはハイブリッド戦略を運用しており、クレジット限度額はリアルタイムで実行されますが、決済は旧式の当座預金口座と同じように実行されます。  
 エネルギーコストは、ほとんどのアプリケーションの作業証明に基づいてブロックチェーンを除外します。しかし、他の種類の追加専用の公開元帳でキラーアプリを見つけることができるでしょうか。私たちは待って見なければならないでしょう。  
 経験から、おそらく技術に非常に優れた少数の非常に大規模な銀行を持つことを除いて、一般的なケースで機能する魔法の解決策はないことが示唆されています。他のシステムでは、トランザクションが到着する順序はそれほど重要ではありません。  
パスポート発行者は、ビザがスタンプされる順序ではなく、作成日と有効期限のみを心配しますセキュリティエンジニアリング240ロスアンダーソン7。  
 それらに同意する3。  
2。  
 Edsger Dijkstraは、この問題とその解決策を食事哲学者の問題を通じて有名に説明しました。  
 したがって、全員が一度に食べようとして、それぞれが右側の箸を手に取ると、動けなくなる[560]。  
 デッドロックはテクノロジーだけの問題ではありません。「キャッチ22」というフレーズは、官僚的プロセスでのデッドロックを表すために一般的になりました。4。  
よく知られているビジネス上の問題（フォームの戦い）では、ある会社が独自の契約条件を添付して注文を発行し、別の会社が独自の条件に従ってそれを受け入れ、それ以上の合意なしに取引を進めます。  
 取引の電子化が進むにつれ、勝者は多くの場合、ウェブサイトを使用してtheloserに取引を強要し、契約条件を受け入れることができる会社になります。  
結果として得られる信頼性ゲームは、セキュリティと安全の両方にかなり悪い結果をもたらす可能性があります。それらについては、経済学の章でさらに説明します。  
2。  
「すべて実行するか、まったく実行しない」場合、トランザクションはアトミックです。これにより、障害後の回復が容易になります。  
 これは銀行システムでは一般的であり、各トランザクションで行われた貸方と借方の合計がゼロであることを主張することで達成されます（これについては、銀行と簿記の章で詳しく説明します）。  
これらのプロパティは、多すぎるか、不十分であるか、またはその両方です。  
4ジョセフヘラーの1961年のその小説は、第二次世界大戦の軍事官僚制度における一貫性のない狂ったルールの複数の事例を説明しています。  
2。  
 これは、トランザクション量が減少した場合、最終的には一貫した状態になることを意味します[1353]。  
実際には、問題が発生して完全に回復できないものを生き残る方法も必要です。  
 たとえば、異なるシステムには、銀行取引レコードのフィールドが必須またはオプションであるという異なるアイデアがあるため、支払いゲートウェイは、物事を機能させるためにデータを推測しなければならないことがよくあります。  
結局、修正係数を追加し、それを一定の年間しきい値未満に維持するための目標を設定することによって、物事はだまされる可能性があります。  
 フィッシング攻撃とキーロギング攻撃の出現により、銀行口座のごく一部がいつでも犯罪者の管理下に置かれるようになりました。お金はそれらからそしてそれらを通して移動されます。  
 フィッシャーマンは当然、取引の逆転を行わない、またはせいぜいゆっくりと不本意ながらそれを行う機関または管轄区を通じて資金を移動しようとします[75]。  
7。  
6セキュリティで保護された時間セキュリティエンジニアが特に関心を寄せる最終的な同時実行性の問題は、正確な時間の提供です。  
 1つの可能性はシンデレラ攻撃です。ファイアウォールなどのセキュリティクリティカルなプログラムにタイムロック付きのライセンスがある場合、攻撃者は時計を進めて「ファイアウォールをカボチャに変える」ことができます。  
 時間は見た目よりもはるかに困難です。原子時計があっても、うるう秒は予測できませんが、どういうわけかブロードキャストする必要があります。一部の分は61秒、さらには62秒です。奇数時間の影響はセキュリティの問題になる可能性があります6;世界の多くはグレゴリオ暦を使用していません。  
 為替手形1882年法律は、たとえ手形が盗まれたとしても、誠実に手形を購入した人々に良い称号を与えました。  
 電子決済の場合、銀行はカルテルとして機能し、カードネットワークルールを通じて、および決済サービス指令を通じてヨーロッパの機関にロビー活動を行うことによって、より迅速に決済を行いました。  
7。  
6一部のATMは、Y2Kの数日後に顧客の残高を確認しなかったため、単語が一巡すると、承認されなかった当座貸越が発生しました。セキュリティエンジニアリング242ロスアンダーソン7  
 フォールトトレランスと障害回復とにかく、安全な時間を提供するためのいくつかの可能なアプローチがあります。  
 絶対時間を放棄して、代わりにランポート時間を使用することができます。この場合、気になるのは、日付ではなくイベントAがイベントBの前に発生したかどうかです[1122]。  
多くのアプリケーションでは、ネットワークタイムプロトコル（NTP）を使用することになります。しかし、あなたはまだ注意する必要があります。  
その後まもなく、D-Linkは同じ間違いを繰り返しました[445]。  
 したがって、企業ネットワークの外部にNTPに依存する多数のデバイスを展開する予定がある場合は、信頼するサーバーを十分に検討し、CERT [1797]からの最新のガイダンスに注意することをお勧めします。  
3フォールトトレランスと障害回復障害回復は、多くの場合、セキュリティエンジニアリングの最も重要な側面ですが、最も無視されているものの1つです。  
 しかし、現代の情報ビジネスの実際の支出（銀行であろうと検索エンジンであろうと）は逆です。  
 この本を読むと、盗難警報から電子戦争、DDoS攻撃から企業を保護することまで、他の多くのアプリケーションが基本的に可用性に関するものであることがわかります。  
従来のフォールトトレランスは通常、冗長性に基づいており、ログやロックなどのメカニズムを使用して強化されており、これらのメカニズムに対する悪意のある攻撃に耐えなければならない場合は非常に複雑です。  
 私は次の定義を使用します。障害はエラーを引き起こす可能性があり、これは誤った状態です。これは、システムの指定された動作からの逸脱である障害につながる可能性があります。  
 セキュリティエンジニアリング243ロスアンダーソン7。  
 故障までの平均許容時間と故障回復故障前の平均時間（MTBF）と修理までの平均時間（MTTR）は明白です。  
3。  
 これの多くは、システム固有の動作環境における脅威の分析からもたらされますが、いくつかの一般的な問題が言及されています。  
3。  
1ビザンチン障害最初に、私たちが関係している障害は通常または悪意のあるものであり、しばしば後者をビザンチンとしてモデル化します。  
ゼネラルは宅配便で口頭メッセージを渡すことができ、宅配便業者は信頼できるので、各将軍は機密および真正な通信を互いの将軍と交換できます（各メッセージのMACを暗号化および計算すると想像できます）。  
 バジルはチャラランポスに「アンソニーは攻撃しよう」と言うことができるようになりましたが、これはチャランポスがアンソニーが裏切り者であると結論づけることはできません。  
この美しい洞察は、n�3t + 1 [1124]の場合にのみ問題が解決することを証明したレスリーランポート、ロバートショスタク、マーシャルピースによるものです。  
 これは、特にデジタル署名と一般的なエンドツーエンドのセキュリティメカニズムの能力を示しています。  
もう1つの教訓は、障害が発生した（または対戦相手に失敗するように誘導された）コンポーネントが、答えを返さないだけでなく間違った答えを返す場合、それを使用して回復力のあるシステムを構築するのがはるかに困難になるということです。  
7。  
1。  
 最も明白な2つの方法は、冗長プロセスとフェイルストッププロセスを使用することです。  
 2つを組み合わせることができます;自動車や航空機の一部の安全上重要な機能で使用されるプロセッサは通常、セキュリティエンジニアリング244ロスアンダーソン7です。  
 フォールトトレランスと障害回復には2つ以上のコアがあります。  
 このような研究は、さまざまな潜水艦や宇宙船で使用されているフォールトトレラントプロセッサ、およびボーイングとエアバスで使用されているアーキテクチャの設計を推進することになった。  
 The Stratusには2つのディスク、2つのバス、さらには2つのCPUがあり、それぞれがエラーを検出すると停止しました。フェイルストップCPUは、同じカードに2つのCPUチップを搭載し、それらの出力を比較することによって構築されました。  
 代わりのカードがポストに到着します。あなたはそれを機械室に持っていき、カード5が点滅する赤信号になっていることに気づき、それを引き出して新しいものと交換します–機械が毎秒数十のトランザクションを処理している間。  
 Googleは関連するソフトウェアスタックの開発のリーダーであり、2000年代初頭に、市販のPCとスマートソフトウェアを備えた大規模なシステムを構築する方が、専門のベンダーからこれまでより大きなサーバーを購入するよりもはるかに安価であることを発見しました。  
 まず、より複雑なソフトウェアスタックとツールチェーンを処理する必要があります。  
 次に、バックアップデータのあるサイトが複数ある場合、それらのいずれかが侵害されると機密性が失われる可能性があります7。また、破壊する義務があるデータがある場合、複数のバックアップテープからデータをパージすることは頭痛の種になる可能性があります。  
不注意のための他のトラップがあります。  
 彼はそのカードが本物であると断固言った。何が起こったのか、それを再構築できるのはこれでした。  
5。  
 前者はエラーを検出するために存在し、後者は偽造を検出するために存在します。  
1GCHQがGoogleにそれを行った方法。  
3。  
 その結果、誤警報が発生し、クライアントの生活に大きな混乱が生じました。  
 たとえば、マルチエンジンの航空機を操縦するためのパイロットの訓練には、最初にシミュレーターで、次にインストラクターのいる実際の航空機で、エンジンの故障手順に関するパイロットの訓練が含まれます。  
 機器の故障についても同様です。ストレス下で壊れたものに依存している場合、コックピットに3つの人工的な地平線があることは役に立ちません。  
複雑な障害もあります。たとえば、単一のセンサーで障害が発生したためにボーイング737 Maxの2機が墜落したとき、飛行機に2つあるがソフトウェアが両方を読み取れなかったとき、パイロットが問題を診断して結果を管理する方法を訓練されていなかったときです。 。  
 他の多くの安全障害は、ユーザビリティの障害であり、第3章で説明したように、セキュリティにも同じことが当てはまります。冗長性は貧弱な設計の正解ではありません。  
3。  
 したがって、回復力がローカルであるか、地理的または組織的な境界を越えているかが重要です。  
 StratusやTandemなどの1980年代のシステムについてはすでに触れました。次に、安価なディスクの冗長アレイ（RAID）など、コンポーネントレベルでの標準ハードウェアのレプリケーションを行いました。  
 これらは現在、クラウドサービスアーキテクチャの標準コンポーネントです。何十万ものサーバーを運用している企業では、非常に多くの障害が発生するため、リカバリを大幅に自動化する必要があります。  
 サービスは、そのクライアントの一部がそれをだまそうとしていると想定する必要があり、いくつかのサービスに依存する必要がある場合もありますが、そのどれも完全に正確ではありません。  
 信頼の決定には複雑なロジックが関係する可能性がありますが、電子戦で使用されているシステムとは異なり、妨害されている入力を試します。  
）セキュリティエンジニアリング246ロスアンダーソン7。  
 フォールトトレランスと障害回復不信の方向はプロトコル設計に影響を与えます。  
 誰もが信頼できず、すべてが相互に疑わしい現実世界向けのシステムを設計することは困難です。  
 ここに明らかな例が銀行カードです。銀行は、マグストリップからチップへ、または安価なチップからより高度なカードへのアップグレードにかかわらず、カードの新しいバージョンを郵送することにより、時々セキュリティをアップグレードできます。そして、影響を受けた顧客にサイクル外のカードを郵送することにより、妥協から回復することができます。  
7。  
3冗長性のレベルはどのくらいですか？システムは、さまざまなレベルでエラー、攻撃、および機器の障害に対して復元力を持たせることができます。  
前述のStratusシステムやRAIDディスクなど、一部のコンピューターはハードウェアレベルで冗長性を備えて構築されています。  
次のレベルでは、プロセスグループの冗長性があります。  
 これにより、機械的な破壊によるものであれ、不正なソフトウェアの挿入によるものであれ、対戦相手がマシンに物理的にアクセスして破壊するような攻撃を阻止できます。  
次のレベルはバックアップで、通常は定期的にシステムのコピー（チェックポイント）を取得します。  
チェックポイント間で適用されたすべてのトランザクションのジャーナルを保持する場合もあります。  
 1980年代の典型的な例は、特定の日に顧客データベースを削除する時限爆弾でした。暗号通貨の登場以来、ファッションはランサムウェアに使用されてきました。  
 メインセンターがダウンした場合、サービスは2番目の施設にフェイルオーバーするという考えです。  
バックアップはフォールバックと同じではありません。  
1つの例は、手動のインプリンティングマシンを使用してクレジットカードを取得することでした。セキュリティエンジニアリング247ロスアンダーソン7。  
 電子端末に障害が発生した場合の、カードのエンボスからのフォールトトレランスと障害回復トランザクション。  
これらは異なるメカニズムであることを理解することが重要です。  
 どちらも、データの機密性への攻撃に対する十分な保護を提供しません。  
 実際の復旧計画とメカニズムには、上記のすべてが混在しています。  
 私が1980年代に銀行で働いていたとき、メインの処理センターが破壊されてから1時間程度でバックアップシステムが動作するようになると考えましたが、テストはビジネス中に処理のリスクを冒したくないという事実によって制限されていました時間：年に1土曜日にバックアップデータセンターの主な運用システムを復旧します。2011年までに、Net ﬂ ixは「カオスモンキー」を開発しました。これは、マシン、ラック、またはデータセンター全体をランダムにノックアウトして、回復力を絶えずテストするシステムです。  
 30か所のデータセンターに300万台のマシンがある場合、絶えずマシンを失い、頻繁にラックに入れられ、データセンター全体が頻繁に失われるため、継続的に物事を設計する必要があります。  
 しかし、AmazonまたはGoogleまたはMicrosoftがどのような障害に対処できるか、そして自分で対処する必要があることを本当に理解する必要があります。  
依存しているサービスのうち、直接のサプライチェーンの外にあるものを検討することは価値があります。  
 政府はガソリン配給を医師と看護師に割り当てていたが、学校の教師には割り当てていなかった。  
これはストライカーがトニーブレア首相を倒すのに役立ちました。彼は着実に増加する燃料義務の彼の署名の環境政策を放棄しました。  
8現在、真剣に取り組んでいるランサムウェアオペレーターは、システムをハッキングし、ファイルの暗号化を不正に行い、攻撃が始まるまで待機します。これにより、現在のデータだけでなく、数週間分のバックアップも人質にとどめることができます。セキュリティエンジニアリング248ロスアンダーソン7。  
 フォールトトレランスと障害回復7。  
4サービス拒否攻撃セキュリティサービスをフォールトトレラントにしたい理由の1つは、サービス拒否攻撃を魅力的でない、効果的でない、またはその両方にすることです。  
 たとえば、セキュリティサーバーを停止して、他のサーバーに資格情報のキャッシュされたコピーを使用させるか、Webサーバーを一時停止して一時的にオフラインにしてから、被害者がダウンロードしようとするページを提供する別のマシンを取得します。  
 プリンシパルが匿名である場合-ロードバランサーの背後にいくつかの同等のサービスがあり、相手が誰を攻撃するかわからない場合-彼は効果がない可能性があります。  
これが不可能で、対戦相手が攻撃する場所を知っている場合、冗長性と復元力のメカニズムによって阻止できるサービス拒否攻撃と、そうでない他のタイプのサービス拒否攻撃があります。  
 この種の攻撃に対する防御には、専門のパケットウォッシングハードウェアを備えたより優れたホスティングサービスにサイトを移動すること、または犯人を追跡して逮捕することが含まれます。  
1990年代後半には、スクリプトキディがダウンチャットサーバーを利用することもありました。  
その後の3年間で、恐喝者はそれらを使い始めました。彼らは、侵害されたPCのネットワークであるボットネットを組み立て、所有者が支払いを拒否するまで、パケットトラフィックでターゲットのWebサーバーに殺到しました。  
攻撃が持続したときの最初の解決策はレプリケーションでした。オペレーターはWebサイトをアカマイなどのサーバーに移動し、サーバーの数が非常に多い（そして顧客に非常に近い）ため、平均的なボットネットで発生するあらゆるものを排除できます。  
2018年までに一周し、約50人の悪意のある人々がサービスとしてDDoS-as-a-a-serviceを運用していました。これは主に、対戦相手のチームスピークサーバーを停止したいゲーマー向けです。  
 また、サービスオペレーターはそれらを、よりユーフェミスティックに「ストレッサー」と呼んでいます。これを使用して、独自のWebサイトの堅牢性をテストできます。  
最後に、より脆弱なフォールバックシステムが存在する場合、一般的な手法は、サービス拒否攻撃を使用して被害者を強制的にフォールバックモードにすることです。  
 スマートカードは通常、Security Engineering249Ross Anderson7よりも偽造が困難です。  
 磁気ストリップカードの名前はNAMINGですが、静電気と接点の摩耗により、毎年1％が故障しています。  
そのため、ほとんどのカード支払いシステムには、磁気ストリップを使用するフォールバックモードがまだあります。  
7。  
 1990年代のdotcom boominの間、SSLが発明され、公開鍵認証局の構築を開始したとき、私たちは証明書にどのような名前を付けるかという問題にぶつかりました。  
 私はかつて私が知っている唯一のロス・アンダーソンでした。しかし、最初の検索エンジンが登場するやいなや、私は何十人も私たちを見つけました。  
 名前はコンテキスト内に存在し、安全なシステムでプリンシパルに名前を付けることがますます重要かつ困難になっています。  
 たとえば、「イギリスのケンブリッジでコンピュータサイエンスを教えているロスアンダーソン」、または「ロスアンダーソンはrossjanderson @ gmail」であると識別できます。  
 しかし、これらは同じ種類のものではなく、それらをリンクすると、あらゆる種類の問題が発生します。「これがマシンXを管理するための鍵です」とだけ書かれている公開鍵証明書は、金属製のドアの鍵のように、無記名トークンです。 rootパスワードが銀行の金庫の封筒にあるかのように、その証明書の秘密鍵を管理するのは誰でも管理者です。  
 mypassportが侵害された場合、その影響は広範囲に及ぶ可能性があるため、政府にその代理人の1人にmynameの偽のパスポートを発行するインセンティブを与えたくありません。  
 たとえば、英国では、チケットを購入したクレジットカードだけを使用して国内線に搭乗することはできません。パスポートの運転免許証を作成する必要があります。これは、支店で銀行振込を1000ポンドを超えて注文したり、アパートを借りたり、弁護士を雇ったり、仕事を得たりするためにも必要です。  
世界がより大きく、よりフラットな名前空間に向かって移動している2つ目の理由は、オンライン認証における大規模サービス会社の支配の高まりです。  
 これらの企業は、セキュリティエンジニアリング250ロスアンダーソン7の章で説明した技術的な外部性から利益を得ただけではありません。  
 NAMING認証、およびビジネスの外部性については、第1章の経済学で説明しますが、ネーミングの問題のいくつかをある程度解決しています。  
 したがって、分散システムでの命名について、世代のコンピュータサイエンス研究者が学んだことを振り返ることは有益です。  
4。  
 名前をアドレスにバインドするために使用される基本的なアルゴリズムは、ランデブーと呼ばれます。名前をエクスポートするプリンシパルはどこかでそれをアドバタイズし、インポートしてそれを使用しようとするプリンシパルはそれを検索します。  
分散システムを構築している人々は、ネーミングがすぐに複雑になることにすぐに気付き、その教訓はニーダムによる古典的な記事[1424]に示されています。  
1。  
 これは引き続き保持されます。先週預金したという情報を、今週引き出しをしようとしている窓口係と共有するために私の銀行口座番号が存在します。  
私が預けたのとまったく同じ金額を引き出したいだけの場合は、無記名預金証書が適切です。  
2。  
 これは復讐で成り立つ。  
 したがって、各システムは相互に依存しており、一方への攻撃は他方に影響を与える可能性があります。  
標準攻撃は、詐欺師が電話会社にあなたであると主張し、電話の紛失を報告することです。  
電話会社はそれを止めることができますが、それが失われる可能性があるのは、限界費用がゼロの一部の通信時間だけなので、認証についてあまり気にしません。  
 Googleは、AndroidプラットフォームをAppleと同じくらい厳しくロックダウンすることでそれを阻止できますが、そうする動機がありません。  
 それほど多くの名前が必要になると想定するのは悪いことです。  
 あまり知られていないのは、これまでクレジットカード業界で行わなければならなかった最も高価なアップグレードが、13桁のクレジットカード番号から16桁への移行であったことです。  
4。  
一部の発行者は何百万もの顧客を抱えているため、9桁の口座番号が標準です。  
4。  
 たとえば、IPv6の128ビットアドレスは、理論的には、ユニバース内のすべてのオブジェクトに一意の名前を付けることができます。  
 途中で一意の名前を呼び出しても、何も購入されない可能性があります。一意のネーミングサービスに時間がかかったり、費用がかかったり、場合によっては失敗したりする場合は、確実に邪魔になることもあります。  
 そのため、この四半期には銀の弾丸は期待できません。  
5。  
 この健全な原則は、英国政府の安全な電子メールのための鍵管理システムの設計では無視されました[115]。  
したがって、頻繁な再編成により、セキュリティインフラストラクチャを毎回再構築する必要があり、古い資料へのアクセス方法などの二次的な問題を解決するために、より多くの費用を費やす必要がありました。  
 名前は、アクセスチケットまたは機能を兼ねている場合があります。  
 一般に、今日の名前が明日のパスワードや機能ではないと想定することは悪い考えです。セクション4で説明したユトレヒトの詐欺を思い出してください。  
 たとえばノルウェーは、市民のID番号が公開されていると見なしていましたが、多くのアプリケーションで一種のパスワードとして使用されており、非公開にする必要がありました。  
 したがって、国防総省は、EDIPIと呼ばれる代理番号を作成しましたが、これは機密ではないとされていました。しかし、確かに、人々はそれをIDとしてではなく、Authenticatorとして使い始めました。しかし、名前とパスワードの役割があいまいな場合があります。  
では、「アンダーソン、123」と言った場合、パスワードはどれですか。実際、それは「アンダーソン」でした。誰もが駐車場を通り抜けて、車のフロントガラスにある駐車許可証から有効なバッジ番号を書き留めることができるからです。  
 間違った名前が明らかな場合、物事ははるかに簡単になります。  
 支払いシステムでは、クレジットカード番号が表示される限り、ターミナルがオフラインである間、クレジットカード番号は受け入れられていました。セキュリティエンジニアリング252ロスアンダーソン7。  
 NAMINGvalid（i。  
、最後の数字は最初の15の適切なチェックディジットであり、ホットカードリストにはありません。  
 まだうまくいかない例として、アイルランドの警察は、「Prawo Jazdy」氏のために50を超えるドックを作成しました。これは、「運転免許証」のポーランド語であることに気づくまで、50を超える交通チケットを支払わなかったためです[192]。  
 一貫性は難しく、しばしば不正確です。  
 ネーミングの一貫性は、いくつかの方法でビジネスに問題を引き起こしますが、おそらく最も気にならないのはバーコードシステムです。  
 したがって、「ケロッグ」で製品を検索すると、アポストロフィが挿入されているかどうかによってかなり異なる結果がスローされ、サプライチェーンに混乱が生じる可能性があります。  
上記で説明した収束の問題もあります。理論的にも、データはシステム全体で一貫していない場合があります。  
9。  
 電話番号はコンピュータアドレスよりもはるかに堅牢です。  
 SignalやWhatsAppなどのより近代的なシステムでは、代わりに携帯電話番号を使用します。  
 （セクション21で、公開鍵インフラストラクチャのさらに具体的な問題について説明します。  
）10。  
 賢明なプログラマは通常、絶対アドレスまたはファイル名をコーディングすることを避けます。これは、マシンのアップグレードまたは置き換えを困難にするためです。  
 まだ安全なsystemsoftenは、ぎりぎりの解決に使用されるサードパーティのサービスが攻撃のポイントになる可能性があるため、安定した説明可能な名前を求めています。  
2。  
7。  
2他の問題点Needhamの原則は、システム所有者の都合に応じてネーミングシステムを課すことができる1990年代初頭の世界のために作成されました。  
4。  
2000年代初頭までに、グローバルに一意で、分散化され、人間にとって意味のあるネーミングシステムはあり得ないことを学びました。  
 これまでエンジニアは、PGPの公開鍵やAndroidのアプリ名として機能する自己署名証明書など、URLのように一意で意味のある、または分散型の命名システムを採用していました。  
 前述のとおり、最初の検索エンジンが登場するとすぐに、ロスアンダーソンと呼ばれる他の何十もの人々をすぐに見つけることができましたが、それよりもさらに悪いことです。半ダースは、ソフトウェアエンジニアリングや配電などの分野でも働いていました。  
 ソーシャルコンテキストを使用して、分散型で意味のあるシステムを構築できます。これは、私たちの脳が対処するために進化したものです。  
これをすべて理解して、人々をつまずかせるのに使わないようにするにはどうすればよいでしょうか？名前のプロパティを詳細に分析すると役立つ場合があります。  
4。  
1名前とアイデンティティ最初に、セキュリティプロトコルのプリンシパルは通常、銀行口座番号、会社の登録番号、個人の名前と生年月日または住所、電話番号、パスポート番号、医療サービスの患者番号、またはコンピューターシステムのユーザーID。  
同一性とは、2つの異なる名前（または同じ名前のインスタンス）が同じプリンシパルに対応する場合です（これは、コンピューター科学者には間接名またはシンボリックリンクとして知られています）。  
家を売ろうとする人は、購入したときとは異なる名前を使用することがよくあります。結婚や性転換の際に名前を変更したり、代わりにミドルネームを使用したりした可能性があります。  
侵害につながるIDの失敗には、2つのタイプがあります。私が誰かになりすまして喜んでいる場合と、特定の個人になりすましたい場合です。  
 銀行（または電話会社）が公共料金の請求書など、住所の証明を2つ要求するだけの場合、それは簡単です。  
これは、銀行とパスポートオフィスの2つの別個のシステム間のシンボリックリンクと見なすことができます。  
4。  
アーロンがジムとして一般に知られている場合、それでもなお厄介です。たとえば、パスポート詐欺の多くは発行前の詐欺です。悪人は、パスポートをまだ申請しておらず、出生証明書のコピーを簡単に入手できる本物の市民の名前でパスポートを申請します。  
 セカンドライフのオペレーターであるリンデンラボは、運転免許証番号または誰かの社会保障番号を提供して、18歳以上であることを証明するスキームを導入しました。  
制度的な失敗もあり得る。  
 同様の問題により、多くの国が生体認証ビザを発行するようになりました。そのため、信頼したくない国のパスポート発行者に依存する必要はありません。  
 出生、結婚、死亡の記録が地元や紙面に保管されている国では、一部が失われ、賢いなりすましがこれらを悪用しています。  
 さまざまな州で、市民登録など、永久に保持する必要がある電子文書に関するパイロットプロジェクトが実施されていますが、信頼できる基準がまだありません。  
 開発が進んでいない国では、フラキー政府ITのScyllaと自然災害のCharybdisの間で舵を取る必要があるかもしれません9。  
4。  
2文化的仮定名前の根底にある仮定は、国によって異なります。  
 しかし、一部の国ではエイリアスの使用を禁止し、他の国ではエイリアスの登録を要求しています。  
 そして、国間の互換性のない規則は、移民、観光客、そして実際に海外の顧客を持つ企業にとって実際の問題を引き起こします。  
4。  
 ソミーの研究室の同僚、故カレンスパークジョーンズ教授は、毎年大学から何も発表しなかった理由を尋ねる手紙を受け取りました（彼女はカレンニーダムとして給与を取得していました）。  
 また、ソフトウェアがすべてを取得し、システムがリンクされると、競合が予期しないリモート影響を与える可能性があります。  
大学が建物、図書館、食堂への統一されたアクセスを提供するために給与名を鍵とするIDカードシステムを導入したとき、そのような問題はさらに摩擦を引き起こしました。  
 以前の性別の名前の使用をやめさせたいトランスの人々;離婚したり離婚したりするときに既婚の名前の使用をやめたく、虐待的なパートナーを雇う場合はおそらく必要な女性。宗教的改宗の後に新しい名前を引き継いだ人々–紛争の源の終わりはありません。  
人間の命名規則も文化によって異なります。  
 南インド、インドネシア、モンゴルの多くの人々は、たった一つの名前-匿名を持っています。  
 したがって、「BK Rajan」は、バンガロールのクマールの息子であるRajanを意味する場合があります。  
 ロシア人は、姓、愛称、姓で知られています。  
 昔、「マリアトロスタッタッティル」が米国移民局に到着し、「トロスタタティア」が姓でも愛称でもないことがわかったとき、彼らの標準的な慣行は、彼女を姓パトロニクスとして採用するように強要しました（彼女の父親がカールと呼ばれた場合、「カールソン」と言います）。  
 そして、子供が生まれた後に名前が変わる文化もあります。  
 あまり知られていないのは、大英帝国がその対象集団の多くに幸運にもIDを課したことです。そのため、実際の格差は、おそらく国が征服されたかどうかです。  
 私は、国が人口登録とIDカードの適切なシステムなしでまったく機能する可能性があると信じることを拒否しているドイツ人を知っていますが、IDカードを要求されることはめったにありません（たとえば、銀行口座の開設や結婚など）。  
4。  
 ただし、アイスランドのIDカード番号は静的です。これは、市民の生年月日とさらに2桁の数字です。  
 これらはおそらく、プライベートとパブリックのID番号付けの両極端です。  
 与党は、領土での出生登録を困難にしたり、IDカードを取得するのを不便にしたりして、他の人々の権利を奪おうとするかもしれません。  
 カードは、営業許可や福祉の支払いに関連付けることができます。遅延を使用して賄賂を引き出すことができます。  
 保護者の国籍のある国の外で生まれた難民の子供や、宗教的またはイデオロギー上の理由で無国籍になったグループなど、除外されたグループはたくさんあります。  
国連の持続可能な開発目標の9つは、「出生登録を含むすべての人に対する法的アイデンティティ」です。また、多くの企業が、開発援助によって資金提供されたIDシステムと投票システムを販売しています。  
 ああ、そしてこれが第三世界の問題だと思うなら、厄介な登録手続きを使って黒人が投票するのを難しくするいくつかの米国の州があります。ウインドラッシュスキャンダルでは、英国政府が外国人出身の英国居住者の多くを強制送還したが、彼らは外国人排斥主義者をますます満足させるために十分な市民権の紙の証跡を維持していなかったため、自動的に市民権を得た。エンジニアは、サービス指向のIDが1つであり、合法的なIDまたは市民権の証明書が別のものであることを常に警戒する必要があります。  
7。  
2。  
 銀行は、口座番号による顧客データの格納から、名前と住所による格納に移行した後に訴訟を起こされました。  
 ある顧客への影響は深刻でした。愛人のために保管していた口座の銀行取引明細書は、彼と離婚した妻に送られました。  
 多くの輸送システムでは、チケットと通行料タグを現金で購入できるため、プライバシーの懸念が解消されますが、銀行口座にリンクする方が便利であり、これらのリンクは時間の経過とともに蓄積されます。  
 実際、私はかつて金物屋のポイントカードであるSecurity Engineering257Ross Anderson7を手に入れました。  
 ランダムなアカウント番号を使用した（信用チェックなしの）NAMING。  
7。  
2。  
 私たちは名前だけで始めましたが、中世後期までに旅行の増加により政府は人々をいじめに姓を採用するようになりました。  
人、企業、行政のインターネットへの大規模な移動は、社会的適応には速すぎました。  
 では、人間が覚えやすい名前を一意にするにはどうすればよいでしょうか？  
 名前は、公開キーまたは名前が付けられているオブジェクトの他の安定した属性のハッシュです。  
 バイオメトリクスのハッシュまたはオブジェクトの表面の微細構造を、適切なエラー修正コードと組み合わせて使用​​することもできます。  
 このようなメカニズムでは、名前を再利用できなくなります。期限切れのドメイン名は悪意のある人々によって購入され、悪用されることが多いため、これは重要な場合があります。  
 ただし、適切な場所に十分な一意性を持たないと、失敗につながる可能性があります。  
 かつて彼らが海外に2000万ポンドを送ろうとしたときに、オペレーターは誤って1000万ポンドを入力しました。  
 したがって、2つの支払いが同じ日付、受取人、金額、およびシーケンス番号でSWIFTに送信され、2番目の支払いは重複として廃棄されました[309]。  
4。  
5名前と住所の安定性多くの名前には、ある種の住所が含まれていますが、住所は変更されます。  
 1990年代後半に、暗号化された電子メールを使用する人々のディレクトリとそのキーを作成しようとしたとき、エントリが変更された主な原因は、セキュリティエンジニアリング258ロスアンダーソン7の変更であることがわかりました。  
 NAMINGemailアドレス[103]。  
）物事はおそらく今より安定しています。  
 GoogleやMicrosoftのような大手サービスプロバイダーは、通常、同じメールアドレスを2回発行することはありませんが、他の企業はまだ発行しています。  
ただし、階層ネーミングシステムには、複数の抽象化レイヤーが含まれ、各レイヤーのアドレス情報の一部が上のレイヤーの名前の一部を形成します。  
多くの場合、部門や組織のレベルで名前が異なります（rja14 @ camなど）。  
英国のアンドロス。  
カム。  
私の場合は英国）。  
承認には、アドレスのプロパティの多く（すべてではない）があります。  
 同様の問題は、名前が複合しているシステムを悩ませます。  
 これは明らかに悪い習慣です。  
仮名を使用するのには十分な理由があります。  
 22歳の大学を卒業するための最初の仕事、または45歳のCEOの仕事に行くとき、あなたはすべての10代の怒りをひっくり返すために検索を求めていません。  
 一方、一部の警察や他の機関では、人々が偽名を使用しないことを望んでいるため、オンラインでのトレーサビリティの問題全体に私たちを連れて行ってくれます。  
4。  
6名前の使用に関する制限命名と社会の相互作用により、さらに問題が発生します。一部の名前は制限された状況でのみ使用される場合があります。  
 時にはそれがマーケティングの問題である：かなりの少数の顧客は、あまりにも多くの情報を要求するウェブサイトを避けている。  
 たとえば、病院が患者番号をMedicalRecordデータベースへのインデックスとして使用することは一般的です。これにより、研究者は、ある目的で偽名のレコードを使用できるようになる可能性があります。  
たとえば、英国の医療サービスでは、どの仮名をどの目的に使用できるかについて、長い間問題がありました。  
 たとえば、警察にセキュリティエンジニアリングを許可する規制259ロスアンダーソン7。  
 NAMING通信データ、つまりだれがいつ誰に電話したかを記録するデータを収集することは、通常、電話の盗聴に関する規制よりもはるかに緩やかです。多くの国では、警察は電話会社に尋ねるだけで通信データを取得できます。明らかに一部の警官は、http：// wwwのようなURLにアクセスした全員のリストを望んでいます。  
com / search？q = cannabis + cultivation;同様に明確に、多くの人々はそのような大規模なトロールをプライバシーの許容できない侵略であると考えます。  
これについては、後で「監視またはプライバシー」の章で詳しく説明します。7。  
3種類の名前技術から組織、政治に至るまで、すべてのレベルで名前の付け方が複雑であるだけでなく、本当に邪悪な問題のいくつかはレベルを超えています。  
 連言はしばしば暗黙のアクセス規則を表現します：「アリスは支店長として行動し、ボバスは支店会計士グループのメンバーです」。  
名前は、サービス（NFS、公開鍵インフラストラクチャなど）やチャネル（ワイヤ、ポート、暗号鍵など）にも適用されます。  
 セキュリティに関する文献で使用されている通常の抽象化は、それらを異なるプリンシパルとして扱うことです。  
 多くの組織は、「アリスの対面」、「アリスの自宅のラップトップ上で実行されるプログラムとしてのアリス」、および「企業のクラウド上のアリスの代わりに実行されるプログラム」を慎重に区別し始めており、アクセスに関する章で可能なメカニズムのいくつかについて説明しましたコントロール。  
 企業は主に給与を受け取りたいが、政府は人々を一意に識別したい。  
 インセンティブに基づく分析は、ネーミングシステムがオープンまたはクローズ、ローカルまたはグローバル、ステートフルまたはステートレスのどちらであるか、およびそれを維持する人々が失敗のコストを支払うのと同じ人々であるかどうかを示すことがあります（経済学は重要な問題の1つです）信頼性のため、そして次の章の主題です。  
 現代の企業ネットワークの内部に飛び込むと、DNSSecurity Engineering260Ross Anderson7が見つかります。  
 単一の名前の背後にある、それぞれが独自のIPアドレスにある複数のマシンにラウンドロビンします。または1つの名前の背後にある、同じIPアドレス上の複数のマシンへのエニーキャスト。または、シスコのHSRPプロトコル。IPアドレスとイーサネットMACアドレスは、あるルーターから別のルーターに移動します。  
）とにかく、システムが拡大するにつれて、単純で、交換可能で、不変な名前に依存することは現実的ではなくなります。  
7。  
 これらの基本のほとんどは、ある世代のコンピュータサイエンスの教科書にあります。  
 timeto orderトランザクションを使用すると役立つ場合がありますが、適切なタイミングを知ることは見かけよりも困難です。  
多くの組織にとって、保護の予算の主な目的は、セキュリティの障害だけでなく、物理的およびソフトウェアのランダムな障害から回復する機能を提供することです。  
 ビザンチンの失敗–欠陥のあるプロセスがランダムに失敗するのではなく共謀する–は問題であり、私たちが選択した暗号化ツールと相互作用します。  
 障害や操作の試みからだけでなく、大規模な攻撃計画の一部である可能性のあるサービスを意図的に拒否する試みからも保護する必要があります。  
 たとえば、他の機能が取り消されたことを理由に訴えられることなく、ユーザー名をキャンセルすることで、ユーザーのシステムへのアクセスを取り消すことができるはずです。  
 しかし、互換性のない命名方式を使用する2つのシステムをマージすると、多くの問題が発生します。  
セキュリティエンジニアリング261ロスアンダーソン7。  
 概要研究の問題私はこの章で、セキュアタイムプロトコルから命名の複雑さまで、多くの技術的な問題に触れました。  
 政府からのIDの発行、ブロックチェーンへのIDの発行まで、あらゆる種類の救済策が過去に押し付けられてきました。  
エンジニアが失敗を研究することは常に良い考えです。落下しない1つの橋よりも、落下しない1つの橋から多くを学びます。  
発展途上国のIDシステムの障害を研究する研究コミュニティーがあります[88]。  
おそらく、私たちは腐敗したセキュリティ状態からきちんと回復できる条件をより注意深く研究する必要があります。  
 しかし、銀行システムは継続します。  
古典的なコンピューターサイエンス理論では、分散システムでの収束は本質的に技術的な問題であり、その解決策は技術的な性質（あるレベルでは、原子性、一貫性、分離、耐久性に依存し、別のレベルでは、デジタル署名、二重制御および監査）に依存していました。堅牢な救済の必要性を排除しようとする純粋に技術的なメカニズムは、実際には事態を悪化させる可能性があります。  
コンピュータサイエンスの学生は、分散システムに関する多くの講義を受けます。キャッチアップするには、Saltzer and Kaashoek [1640]をお勧めします。  
 米国国立研究評議会の2003年の報告書プライバシーのレンズを介した認証」では、認証とプライバシーの間のトレードオフと、それらがどのようにうまくスケーリングしない傾向があるかについて説明します[1039]。  
セキュリティエンジニアリング262ロスアンダーソン