– JCフリードリッヒフォンシラー犬が彼の嘔吐物に戻るので、愚か者は彼の愚かさに戻ります。  
1はじめに世界中の人々がカードや電話での支払いを支持して現金を放棄しているため、キャッシュレス決済業界はコロナウイルスの汎流行の勝者の1つです。  
 株式取引から取引決済まで、すべてに特化したネットワークがあり、その多くは他の企業にも開放されています。  
このようなシステムは、いくつかの理由でセキュリティエンジニアにとって重要です。  
 詐欺のより広い問題に取り組むためにトランザクション処理を理解する必要があります、そしてこの章はあなたに大まかな地図を与えます。  
 CFOと信頼できるようにするには、Gramm-Leach-Bliley、Sarbanes-Oxley、およびPCI DSSについての会話を実行できる必要があります。  
第二に、簿記はコンピュータ産業を動かしました。  
 バンキングは急速にコンピューティングの最も集中的なアプリケーション領域となり、37612を介して他の企業にも広まりました。  
 BOOKKKEEPING SYSTEMS 1960年代からの簿記の自動化。  
 また、機密性がほとんど役割を果たさないが、レコードの整合性（および作成された後の不変性）が最重要である保護の十分に理解されたモデルも提供します。  
 バンキングと簿記は、今日ではマルチパーティ認証としても知られるデュアルコントロールの使用を開拓しました。  
 彼らは、暗号化アルゴリズムとプロトコル、およびスマートカードなどのサポート技術の開発を推進しました。  
最後に、今世紀に構築した世界規模のシステムの多くは、何世紀にもわたってローカルシステムと手動システムで置き換えられてきたチェックとバランスを回避するために設計されました。  
 Uberは、世界中の何千もの町や都市でのタクシー規制を回避することにより、グローバルタクシー会社になることを計画していました。  
この章では、最初に、資産の追跡と破損した状態のリスクの管理に使用される簿記システムについて説明します。このような会計システムは、あらゆる規模の他の企業でも使用されています。  
次に、銀行の公の顔であるATMシステムについて説明します。ATMシステムは、ユーティリティメーターなどのアプリケーションにも採用されています。  
 次に、非接触型決済、電話決済、オープンバンキングなど、より最近の技術進歩に移ります。  
2簿記システム簿記は、農業直後の紀元前8500年頃に中東で発明されたようです[1663]。  
 突然、彼らはどの村人が共同倉庫に何を入れたかを追跡する方法が必要になりました。  
。  
 ）は粘土のトークン、またはブラで表され、それは粘土の封筒の中に置かれ、倉庫のキーパーのパターンでそれを回転させることによって密封され、次に窯で焼かれました。  
 （これは最も古い既知のセキュリティプロトコルである可能性があります。  
 Security Engineering377Ross Anderson12について。  
 急上昇システム同時に、金属インゴットが中間商品として使用されるようになり、しばしば検査員によってブラ内部に密閉されました。  
 アテネのペリクレスによって、多くの裕福な個人が銀行家として働いていた[772]。  
1：–粘土の封筒と7瓶の油を表すトークンの内容。ウルク、現在のイラク、カリフォルニア州。  
 暗い時代が終わりに近づき、貿易が成長し始めたので、一部の企業は単一家族が管理するには大きすぎました。  
しかし、会社がオーナーの家族の能力を超えて直接管理する能力を超えて成長するには、外部からマネージャーを雇わなければなりませんでした。  
 歴史家は、12世紀のカイロ[1691]でユダヤ人の商人によって作成された複式の記録を見つけましたが、この主題に関する最初の本は1494年まで表示されませんでした[522]。  
2。  
 たとえば、企業が顧客に100ドル相当の商品をクレジットで販売する場合、100ドルのクレジットをSalesアカウントに転記し、100ドルの借方をReceivablesアカウントに転記します。  
 （会計学校で教えられている原則は、「受取人から借方記入し、寄付者に貸方記入すること」です。  
 最小の企業を除くすべてにおいて、書籍Security Engineering378Ross Anderson12。  
 BOOKKEEPING SYSTEMSは、異なる店員によって保管されていました。  
 各キャッシャーは、一晩保管庫にロックする前にキャッシュトレイのバランスを調整します。現金元帳の借方は、収集した実際の銀行口座の残高と正確にバランスを取る必要があります。  
 本は年末に監査されるだけでなく、ランダムな監査もあります。検査官は予告なしに枝を降りて、家に帰る前にすべての本のバランスが取れていると主張することができます。リッティは、従業員が彼からお金を盗んだサロン所有者でした。  
 National Cash RegisterCompanyを設立したPattersonは、銀行および簿記機器の主要なサプライヤーになっただけでなく、1990年代にMicrosoftがそれを追い出したまで、コンピューター業界を支配していたIBMをスピンさせました。  
2。  
 1950年代後半から1960年代前半に小切手処理などのアプリケーションを始めて、当時の低速で高価なコンピュータでさえ、店員の軍隊よりはるかに安価であることがわかりました。  
 ATMは1970年代に一斉に到着し、1980年代にはファーストラインの銀行システムでした。 1990年代には、ウェブベースのバンキングが続いた。  
米国、ヨーロッパ、およびほとんどの先進国の法律では、銀行だけでなくすべての公開企業に有効な内部統制を設けることを求めており、幹部にそれらの責任を負わせています。  
 簿記に使用されるコンピューターシステムは、通常、複式記入テーマのバリエーションを実装することを要求しますが、品質は可変です。  
たとえば、元帳がすべて1つのデータベースの単なるビューである場合、物理的なアクセス権を持つユーザーとデータベース編集ツールがコントロールをバイパスする可能性があります。  
 たとえば、ある銀行は住所の変更を監査しませんでした。レジ係が顧客の住所を変更し、追加の銀行カードを発行し、再度変更できることがわかるまでは[54]。  
従来のコアバンキングシステムには、いくつかのデータ構造があります。アカウントマスターファイルには、各顧客の現在の残高が、おそらく90日間の前のトランザクションと一緒に含まれています。システムを通過する途中で現金やその他の資産を追跡する多数の元帳、現金自動預け払い機、窓口、マーチャントターミナルなどから受信されたが、まだ元帳に投稿されていないトランザクションのさまざまなジャーナル、およびその監査証跡誰がいつ何をしたかを記録します。  
2。  
コアバンキングソフトウェアは、ジャーナルからのトランザクションをさまざまな元帳とアカウントマスターファイルに適用します。  
これは伝統的にバッチプロセスで夜通し行われていましたが、リアルタイムのオンライン処理がますます関与するため、事態はさらに早く悪化する可能性があります。  
 銀行（またはその支店の1つ）のバランスが崩れると、アラームが鳴り、一部​​の処理が停止して、検査官が原因を探し始めます。  
 従来のビジネスでは、さまざまな事務員によってさまざまな元帳が管理されていたのと同じように、銀行のデータ処理ショップには、さまざまなサブシステムを担当するさまざまな開発チームがいます。  
 承認されると、開発環境がなく、承認されたオブジェクトコードとデータのみを備えた本番マシンで実行されます。  
）12。  
3クラーク・ウィルソンのセキュリティポリシーモデルこのようなシステムは1960年代から発展してきましたが、そのセキュリティポリシーの正式なモデルは、デイブクラークとデイブウィルソン（前者はコンピューターサイエンティスト、後者は会計士）によって1987年に初めて導入されました[436]。  
より正式には、制約のないデータアイテム（UDI）から制約のあるデータアイテム（CDI）にデータを入力できる特別な手順があります。 CDIの有効性をチェックする整合性検証手順（IVP）（e。  
、本のバランス）;銀行の場合、バランスを保つトランザクションと考えられる変換手順（TP）。  
 また、トランザクションを再構築するために、追加専用のCDI（監査証跡）に十分な情報を書き込みます。  
 [47]の公式では：1。  
これにより、コアシステムの負荷が最小限に抑えられ、システムがダウンしたときの苦情も最小限に抑えられます。  
2。  
 CDIへのTPの適用は、その整合性を維持する必要があります。3。  
 被験者は特定のCDIで特定のTPのみを開始できます; 5。  
 UDI上の特定のTPが出力としてCDIを生成できる7。  
 システムは、TPを開始しようとする対象を認証する必要があります。9。  
e。  
多くの事柄が言われています。  
 監査証跡に加えて、これは通常、デュアルコントロールの場合に必要です。これは、1人のマネージャーだけが承認し、1秒後にサインオンを待つトランザクションなど、部分的に承認されたトランザクションを追跡する必要があるためです。  
 状態遷移はバランスなどの不変条件を保持するべきであるという考えを捉えていますが、状態遷移は正しいべきではありません。第三に、難しい質問が残っています。つまり、不正な状態からのリスクをどのように制御するのですか？ルール5は、「適切な職務分離ポリシー」をサポートする必要があると述べていますが、これが何を意味するかについては何も述べていません。  
実際に起こっていることは、4つの大手会計事務所が監査クライアントにプッシュする統制のリストを持っていることです。一般的な会社は、そのセクターに応じて、維持しなければならない約300の内部統制のチェックリストを持っている場合があります。  
 多くの管理策は実際のリスク低減ではなく正式なコンプライアンスであり、実際には有害なものもあります。  
4。  
3 1990年代に大手4人の監査人がNISTの助言をどのように取得して、人々に毎月パスワードを変更させたか。これを書いている時点（2020年）では、監査クライアントにこれを実行するように要求しています。  
内部統制に対する原則的なアプローチが可能であり、実際に望ましい。  
12。  
4内部統制の設計長年にわたり、会計や専門家、弁護士、銀行の規制であるセキュリティエンジニアリング381ロスアンダーソン12によって、簿記や内部統制に関するさまざまな標準が推進されてきました。  
 BOOKKEEPING SYSTEMStors。  
 しかし、自主規制はドットコム時代の過剰を止めることができず、エンロンテールの崩壊に続いて、2002年のサーベンスオクスリー法（SOX）の形で米国議員からの介入がありました。  
 また、監査人に「重大な弱点」を開示するよう要求します。  
 以前、1999年のグラム・リーチ・ブライリー法（GLBA）は、多くの点で銀行規制を自由化しましたが、セキュリティと完全性の予測可能な脅威から情報を保護するセキュリティメカニズムを銀行に義務付けました。  
5。  
 これらの規制は、BigFour会計事務所が内部統制に関する企業ポリシーに及ぼす影響を統合するのに役立ちました。  
 現代のリスク管理システムでは、通常、企業がリスクを特定して評価し、リスクを軽減するための統制を構築する必要があります。  
2）。  
 ISA315は、エラーによるものか詐欺によるものかを問わず、組織のアカウントに重大な虚偽表示があるリスクに焦点を当てています。  
次に、各アサーションが誤っている可能性があるリスクと、そのリスクが重大であるかどうかを検討します。  
パート3で説明するように、エラーに対する安全性と攻撃に対するセキュリティを確保するには、2つの基本的なアプローチがあります。  
 英国の銀行におけるリスクガバナンスの説明については、セクション12で説明するテスコ銀行に対する2016年の不正行為に関する金融行動監督庁の報告[687]を参照してください。  
3。  
2。  
 監査をサポートする場合、財務諸表が依拠する主張に対するリスクに注意を払う必要があります。  
 内部統制がセキュリティ体制のすべてではありません。  
デュアルコントロールでは、2つ以上のプリンシパルが連携してトランザクションを承認します。  
4）。  
保証は特に詐欺の傾向があります。  
 偽造または不正に取得された保証を持つ詐欺師は、銀行Bのローンアカウントを略奪するのに時間がかかる可能性があります。警報は、銀行がデフォルトになり、銀行Bが銀行Aにお金を要求したときにのみ発生します。  
職務の分離により、2人以上のメンバーがトランザクションに補完的に作用します。  
 Alineマネージャーが購入を決定し、購入部門に伝えます。店員が購入注文を出します。店員は商品の到着を記録します。請求書がアカウントに到着します。会計担当者はそれを発注書および店舗のレシートと関連付け、小切手を発行します。アカウントマネージャーは小切手に署名します。  
 ラインマネージャーは、その内部アカウントの毎月の明細書から借方を取り、上司がアカウントをレビューして、部門の利益目標が達成される可能性が高いことを確認します。内部監査部門は、いつでも降下して部門の帳簿を監査できます。年に一度来て、無作為に選んだ部門のサンプルの本をチェックします。  
モデルは、防止-検出-回復として要約できます。  
 検出が遅れる可能性があり、したがって回復が困難になる可能性がある場合（corruptbank保証の場合など）は、おそらく二重制御を使用して、追加の効果を防​​止に費やします。  
 ここでの典型的な例は、銀行のレジ係が簡単に現金を受け取ることができるので、家に帰る前に毎日お金を数えます。4最近の問題は、2人のマネージャーが共謀するか、どちらか一方が他方を偽装するかどうかだけでなく、マルウェアが両方のアカウントを乗っ取るかどうかです。  
3。  
セキュリティエンジニアリング383ロスアンダーソン12。  
 BOOKKEEPING SYSTEMSコントロールは、役割が既存のビジネスプロセスの補完的な部分であり、いくつかのプロセスがそれらをサポートするために何世紀にもわたって進化してきた場合に最適に機能します。  
 スイスの銀行では、ほとんどすべてに2人のマネージャーの署名があり、アメリカ人ははるかにリラックスしています。  
 これは大学では受け入れられませんが、インカデミアでは盗むことがはるかに少なくなります。  
 財務管理者、人事部門、弁護士、監査人、システム担当者はすべて、異なる方向から問題に直面し、部分的な解決策を講じ、互いの管理目​​標を理解できず、事態は真ん中の穴に落ちます。  
 コントロールを文化に適合させ、人々がそれらを使用するように動機づけることが重要です。より良い経営の銀行は、脅迫や誘拐から銀行を保護するための手段として、管理統制を停滞させます。  
儀式となる統制は、その目的が忘れられた、または無関係になった後、何年もの間行われる場合があります。  
密接な同僚の信頼が限られている文化は、維持するのが特に困難です（事業部門間で機能的統制が分割される別の理由がより効果的である場合があります）。  
 しかし、これは多くの理由で徹底的に行うことは困難です。  
 第2に、責任分担システムの管理は面倒すぎます。  
 第3に、デュアルコントロールは、永続的な状態を必要とすることがよくあります。これは、トランザクションをアトミックにすることによって物事をシンプルに保ちたいというプログラマの要望に緊張しています。  
 第4に、企業が開発と運用をDevOpsとして統合し、セキュリティを追加してDevSecOpsにすることで、企業はより信頼できる状態になる可能性があります。  
 第五に、緊急事態があります。  
 そのようなアクセスをログに記録し、sysadminsの場合と同様に、監査人にログを監視させます。  
したがって、詐欺を犯す可能性のあるエンジニアは常にいます。  
セキュリティエンジニアリング384ロスアンダーソン12。  
 BOOKKEEPING SYSTEMSは、2人のシャドウユーザーを作成し、それらの間で多額の支払いを承認するか、支払いシステムの保守担当者が追加の支払いをキューにポップします。  
これについては、セクション12で詳しく説明します。  
3。  
 ただし、機能分離を機能させるには、メカニズムをアプリケーションに組み込む必要があります。そのため、オペレーティングシステムに付属するメカニズムよりも、独自のものであり、あいまいで、十分にテストされていない場合があります。  
 セキュリティアーキテクトや主任監査人など、一部の人々はそれをすべて理解する必要があります。  
 価値の高い意思決定を迅速に行わなければならず、取引のすべての側面を理解しなければならない人もいます。  
 彼らが誰であるかを知り、彼らの数を最小限に抑え、彼らによく食べて、慎重に彼らを監視することが重要です。  
1つの例は、カリフォルニアの銀行が、新しい処理装置を取り付けた後、小切手に2つの署名があるという要求を突然無視し始めたことです[1621]。  
 そして、紛争解決があります：「私の2人のマネージャーは、送金されたと言います！」「しかし、私の2人は、送金されなかったと言います！」12。  
5何が問題になるか盗難と詐欺は、さまざまな形をとります。  
12。  
5。  
 典型的な職務は、数千ドルの損失を伴う軽微なembez-zlementでした。  
年に数百の窓口を失うことは、ビジネスを行うためのコストにすぎませんでした。  
また、今日では、顧客の個人情報を販売することも難しくなっています。なぜなら、顧客がセキュリティの質問をして顧客の記録にアクセスする必要があるからです。  
2。  
注目に値するインサイダーのケースは次のとおりです。•英国での最近の最大の銀行詐欺は、グラスゴーのイーストエンドのFeezan Hameedのギャングによって引っ張られました。  
 彼は標的企業を発見した2人の従業員を倒した–通常は100万ポンド以上のアカウントを持つ中規模企業。  
 これを行う前に、彼はそれらとしてログオンし、大きな5桁の支払いのバッチを設定していました。  
•HSBCの銀行口座にアクセスするためにAT＆Tが使用するパスワードを変更することが知られていない人と共謀したHSBCのパスワード再設定担当者。  
 店員は、内部検査に不合格だった後、パスワードのリセットに雇われていた弱者でした。裁判所は憐れみを取り、彼は5年の猶予を免れた[1569]。•2010年代に急増した銀行詐欺の1つには、中規模企業でのスピアフィッシングアカウントの停止と、いくつかのアカウントの乗っ取りが含まれています。  
銀行は大規模なトランザクションに特別な注意を払う可能性があるため、会社が気付く前に、ゲームは多くの場合、4桁の支払いをたくさん行うことになります。  
 典型的な攻撃では、50万人を狙う可能性があります。  
2。  
 Barings Bankの崩壊は良い例です。マネージャーは不正なトレーダーであるNick Leesonを制御することに失敗し、見かけの取引利益が獲得したボーナスを貪欲で盲目にしました。  
 6のようなopsecルールにより、コールセンターがCovidの大流行の最中に在宅状態で仕事をすることが困難になっているため、被害者の幹部は非常に過失でした。  
セキュリティエンジニアリング386ロスアンダーソン12。  
 BOOKKEEPING SYSTEMSBareingのケース、または株式ファンディングとマクスウェルのように加害者でした。  
エコノミストや会計学の教授は、代理店の問題などの問題を分析します。プリンシパルAがエージェントBを雇って資産を管理し、Bのパフォーマンスを監視および評価できるかどうかを知りたいと考えています。  
 理論的には、内部統制と内部監査部門は、CEOがよりジュニアのステータスを追跡するために使用するツールですが、外部監査人は、株主がCEOと上級経営者を追跡するために使用するツールです。  
 この慣行は、1996年から2004年の間に引用された米国企業に対する230件の企業詐欺の調査で、Alexander Dyck、AdairMorse、Luigi Zingalesによって分析されました[596]。  
 ほとんどは、他のインセンティブを持つ俳優によって検出されました：従業員による19％、業界の規制当局による16％、金融アナリストによる14％、およびメディアによる14％。  
 Af-ter Sarbanes-Oxleyは、必須の俳優のパフォーマンスをわずかに改善しましたが、全体の半分をわずかに超えました。  
 これは、何が起こっているのかを実際に知っているのは支配的な要因であることを示唆しています。  
理論的には、社外監査人は、社外取締役が委員長を務める取締役会の監査委員会によって任命されます。しかし、誰が外部取締役を任命するのですか？私の経験では、社外取締役はCEOと友好的である傾向があり、監査人はCFO8を変更するために邪魔をしません。  
 大手の監査会社は、クライアントの実際のリスクに関係なく、お気に入りのコントロールの独自のリストをプッシュすることにより、情報セキュリティの世界に悪影響を及ぼす。  
純粋な経済的インセンティブとは別に、上司は上級の同僚が無能であるか不正直であるという証拠に対処するのが難しいと感じています。  
2。  
セキュリティエンジニアリング387ロスアンダーソン12。  
 ブッキングキーピングシステム  
 バリングスの誰も、彼らのスターディーラーであるニックリーソンが詐欺師であるとは考えたくありませんでした。ポップは銀行に行きました。  
12。  
6。  
 彼らが疑っているとしても、批判の下で地位を閉じるための社会的反省があり、弁護士はクライアントにすべてを拒否するように忠告するかもしれません。  
 郵便局は手紙を発送するだけでなく、重要な金融機関でもあります。その支店のほとんどはサブ郵便局長、通常はフランチャイズ化された郵便局カウンターのある店主によって運営されています。  
 何千人もの人々が命を落としました。一部の企業は事業を失い、破産し、一部の従業員は不法に解雇され、何人かの人々は彼らが犯していない詐欺で投獄されました。  
 裁判官はホライゾンが「リモートで堅牢ではなかった」と認めました[185]。  
 多くの法的システムでは、誰かが反対の証拠を提示できない限り、会計システムが適切に機能していると想定していますが、これは難しい場合があります。多くの法的手段は、郵便局にソフトウェアへのアクセス権を与えることを強制し、文書化されているため、専門家が検討できます。  
 ポストオフィスのトーカの給与削減のほとんどの場所は、叙階され​​た大臣であるCEOのポーラ・ヴェネルズがかなりの昇給を得た[354]。  
 ソフトウェアサプライヤーの富士通が和解金を支払うことになるかもしれませんが、さらなる訴訟が必要になる場合があります。  
2。  
2その他の失敗ほとんどの会計システムの失敗はそれほど目立たないが、金融機関や他の企業の運営能力に大きな影響を与える多くの失敗がある。  
1。  
 ソフトウェアエンジニアはこれを技術的負債と呼んでいます。つまり、変更はより遅く、より高価になり、障害からの回復は複雑になる可能性があります[41]。たとえば、2012年6月、6。  
2。  
 人々はお金なしで海外に取り残され、一部の会社は給与計算をすることができませんでした。  
 別の週にサービス障害が起こったとしたら、それは再び破綻し、納税者に数百億ドルのコストをかけ、広範囲にわたる混乱を引き起こしたかもしれません。  
 しかし、粗悪な古い中核銀行システムを新しいものに置き換えることは、何年もかかり、独自の戦略的リスクを伴い、9つのコストがかかる主要なプロジェクトです。  
2。  
 私たちの大学の会計システムは2000年代初頭に置き換えられ、300万ポンドのコストがかかるはずだったプロジェクトは、代わりに1,100万ポンドかかりました。  
3。  
 私たちの大学では、ファイナンスシステムの設計において、1,500人の教授より35人のファイナンスオフィスが発言しています。  
 事務員によって節約された時間は、教授によって浪費された時間よりも少ないですが、集中した関心が通常勝ちます。  
12。  
6。  
 また、それらが外部の現実に対応していることを確認する必要があります。  
 記録された資産と在庫の20％が存在しないことが判明しました。  
監査人は、会社の上司について問い合わせることなくマッケソン口座を受け入れていました。彼らは、在庫の確認、顧客との売掛金の確認、または会社内での職務の分離について考えることに失敗しました[1616]。  
 CEOのTino de Angelisのケネディ。  
2020ドルで80億ドルセキュリティエンジニアリング389ロスアンダーソン12。  
 実際にはほとんどが水であり、これを使用して先物取引を多用したBOOKKEEPING SYSTEM [1442]。  
 （その後、WarrenBu↵ettが会社の5％とマデナフォーチュンを購入しました。  
 2001年に失敗してサーベンスオクスリー法に至ったエンロンについてはすでに触れましたが、2008年には、価値のほとんどない住宅ローンに基づいていることが判明した複雑な金融デリバティブの取引が原因の金融危機がありました。  
 そのため、銀行が住宅ローンを登録するためのブロックチェーンについて話しているときに、スマートコントラクトが金融革新を可能にするという点で、いくらか懐疑的かもしれません。  
7。  
決済サービス会社であり、ポルノサイト、オンラインカジノ、および通常の銀行では触れられない他の商人へのカード決済の処理を開始していました。  
 しかし、2020年6月に、ドイツ銀行（時価総額が約200億ドルのドイツ最大の銀行）を買収しようとしたため、ワイアカードの監査人EYは、主張されている資産の4分の1、一部はe2であることを明らかにしました。  
（EYは3年間銀行員と銀行の明細書を検証することに失敗し、代わりに会社自体が提供する「スクリーンショット」に依存していました[1834]。  
 それを使用して支払いを処理する一連の先端技術のスタートアップは取引を停止し、ドイツの内外の何百万人ものカード所有者が彼らのお金にアクセスできなくなった。  
 さらに悪いことに、Financial Timesが2019年にワイアカードの疑わしい会計慣行の分析を発表したとき-そのドバイ子会社には顧客がいないように見え、フィリピンの子会社とされる1社の住所は小さなバス会社であり、もう1社は引退した船員、およびそのシンガポール子会社の内部告発者は本を調理するように命じられたと報告している[1283] –ドイツの規制当局BaFinは会社を調査するのではなく、ジャーナリストの犯罪捜査を開始し、会社の株式の空売りを禁止することで対応した[ 610]。  
 これは、ヨーロッパの歴史上最大の詐欺の1つであり、見かけ上の株主価値だけでなくe200bnを破壊し、ドイツの金融規制に対する公の信頼も破壊しました。  
 マッケソンとロビンズのレッスンがどれほど注意深く行われていたかを見るのは非常に驚くべきことでした。海外の現金残高をチェックすることは本当に監査101であったはずです。  
セキュリティエンジニアリング390ロスアンダーソン12。  
 急上昇システム12。  
6。  
 理論的には、この背後にいくつかのガバナンスがあります。  
これは、システムが米国の公共部門で使用されているのか、または米国の株式市場で引用されている企業によって使用されているのかを判断する基準の1つです。  
その基本的なプロセスは進化のサイクルです。特定の環境で、リスクを評価し、コントロールを設計し、そのパフォーマンスを監視してから、ループを繰り返します。  
 理論的には、そのコアは、彼らの制御ポリシーが実装されていることを確認し、彼らの目的を達成し、そうでない場合はそれらを修正する上級管理職で構成されています。認定情報システム監査人（CISA）試験を管理する情報システム監査管理協会（ISACA）は、より国際的な情報および関連技術（CobiT）の管理目標として知られるCOSOの定義を持っています[946]。  
 より具体的な基準は、米国の上場企業向けのSarbanes-Oxley、米国の金融機関向けのGramm-Leach-Bliley、米国の医療機関向けのHIPAA、およびGDPRの個人情報など、特定の部門別規制に関する監査人の解釈から明らかになります。 EU加盟国の居住者。  
 セキュリティ管理に関するISO 27001もあります。  
 これらの多くは標準であり、誰もが同意できるため、決して十分ではありません。  
 セクション28でこれに戻ります。  
9。  
2。  
あなたも人々と彼らの外部の関係について考える必要があります。  
2。  
 あなたはそれらのうちどれが重要で、どのようにして見つけ出すかを考え出す必要があります。  
 信頼できる人はあなたを傷つけることができる人であることを忘れないでください。  
学ぶべき教訓は次のとおりです。  
•顧客や従業員からの苦情を利用して詐欺やシステム障害を警告している場合は、顧客から連絡を受けたり、顧客の意見を聞いたりするための良い方法があるとよいでしょう。  
•主な露出は会社の従業員や請負業者にありますので、十分に話をして、「会社を詐欺したいと思ったら、どうしますか？」などの質問をするほうがよいでしょう。•言葉だけで考えないでください。トランザクションとプロセスの、しかし人々、インセンティブ、社会的規範と他のものを操作または威嚇する力について。  
•これらの回避策は当然のことながら脆弱性を生み出すため、人々が遵守できる設計管理を改善する必要があります。  
リスクは常に残ります。  
 特定のシステムが絶対に失敗しないという教義を採用するのは非常に悪い考えです。なぜなら、もし失敗をアプリオリにゼロの確率で割り当てた場合、証拠はそれをシフトせず、最終的に失敗すると事態はひどく悪くなる可能性があるからです。  
 そして経験とは、単なる損失履歴ではなく、邪魔になるコントロールを特定して改善する必要があるということです。  
 たとえば、パスワードリセット機能を修正して、必要なステータスを減らしたり、詐欺エンジンを改善して会社のWebサイトが買い物かごを拒否したりできるようにすると、取締役会はより簡単にお客様の声を聞くようになります。  
 一部の業界では、セキュリティ管理に関する国際標準ISO 27001が使用されています。リスクを体系的に分析し、許容できないリスクをSecurity Engineering392Ross Anderson12に委ねることを要求しています。  
 銀行間決済システム何らかの形のリスク処理（管理、回避、移転）;コントロールが更新されていることを確認するための管理プロセスがあります。  
 そして、対処すべきセクター固有の規制制度が数多くあります。  
4）;バンキングと支払いについては、次に説明します。  
3銀行間決済システム電子詐欺のことを考えると、巧妙なロシアのハッカーが銀行のコードを破り、無数のドルの電信送金をタックスヘイブンに送るハリウッドのシーンを思い描くことがよくあります。  
 まず、銀行間での送金に使用されるシステムについて説明し、次に個人または販売者を問わず、銀行の顧客が使用するシステムについて説明します。  
3。  
しかし、それははるかに遡ります。  
 陸上システムは一連のビーコンタワーに沿ってメッセージを送信し、海軍システムはそれらを船間で中継しました。  
 彼らが1836年に発見されるまでの2年間、2人の銀行家が操作員に賄賂を渡して、安全な距離から観測できるトランスミッションの誤りを作り出すことによって株式市場の動きを密かに知らせました。  
 Bookiesは、結果を待って、それが最初に聞こえることを期待するのではなく、時計で「時間を呼び出す」ことを学びました。  
 彼は1842年に議会を説得し、ワシントンからボルチモアまでの実験線に資金を提供しました。  
これは、1990年代後半のインターネットブームのように、さまざまな意味でありました。  
2。  
 Telegramswereは、国内市場の創出にも使用されました。  
 この期間の歴史は、eコマースの概念と問題のほとんどがビクトリア朝時代によく知られていることを示しています[1818]。  
3。  
1970年代までに、銀行家たちはこの価値ある古いビクトリア朝のシステムが全面的な見直しの必要があることに気づき始めました。2。  
第二に、テストキーシステムはデュアルコントロールをサポートしていませんでした。  
第三に、本当の懸念はコストとエラーでした。  
 エラーは詐欺よりもはるかに問題でした。  
3。  
 これは、組み込みの認証および否認防止サービスとオプションの暗号化を備えた電子メールシステムと考えることができます。  
設計上の制約は興味深いものです。  
 当時、多くの国（フランスなど）が機密性のために暗号を使用することを禁じていたため、au-tenticityメカニズムは機密性メカニズムから独立している必要がありました。  
 最後に、銀行は銀行間取引に対して監査可能な二重統制を実施できなければなりませんでした。  
2。  
 鍵は、二国間鍵交換を使用して管理されていました。銀行が海外で関係を築くときはいつでも、それを交渉した上級管理職は、面談でも会議でも、相手の番号と鍵を交換していました。その後、お互いの自宅の住所に郵送します。  
3。  
2：– SWIFTのアーキテクチャが妥協し、1方向に1つ送信されます（銀行のマネージャーのメールがメールボックスで片方の犯罪者によって読み取られても、両方で発生する可能性は低いです）。  
このように、SWIFTはメッセージ認証に関与しませんでした。使用されている認証アルゴリズムが適切である限り、それらの従業員はトランザクションを偽造できませんでした。  
 かなり早く、攻撃が発見され、[1545]で公開されました。  
SWIFT自体は認証に対して信頼されていませんでしたが、否認防止サービスを提供しました。  
 RGPは通常、さまざまなサービス会社によって運営されていました。  
 また、裁判官にとって暗号化よりもログの方が簡単です。  
 これは、銀行とRGPノードの間、およびこれらのノードとメインのSWIFT処理サイトの間のライン暗号化デバイスによって提供されました。  
守秘義務が違法であった国では、これらのデバイスは、信頼性と否認防止メカニズムを損なうことなく省略できます10。  
 これはライブ回線にのみ表示され、バックアップ回線には表示されず、遅れて表示されました。2つの回線間で機器を交換しても効果がありませんでした。  
セキュリティエンジニアリング395ロスアンダーソン12。  
 銀行間支払いシステム：専用の端末または他の銀行システムと統合できるソフトウェアパッケージによって、デュアルコントロールが提供されました。  
 取引を毎日明細書と照合してチェックすることにより、アカウントを調整する機能的なコントロールがあります。  
12。  
3何が問題なのかSWIFTは、システム自体に対する外部からの詐欺の単一の報告なしに20年間実行しました。  
 鍵管理メカニズムはensconcedas ISO 11166であり、このアーキテクチャのセキュリティについていくつかの議論がありました[112、1631]。  
S  
 双方向の鍵交換は、2009年に暗号化メカニズムが独自仕様の新しいシステムに置き換えられました。  
暗号化が強化され始め、デフォルトで機密性が高まるようになると、政治的な問題が発生しました。  
 これはプライバシーを重視するヨーロッパ人との対立を引き起こしましたが、最終的にオバマ大統領がブッシュ大統領を継承した後、EUは米国財務省がスウィフトで召喚状を提供できる条約に同意しました[341]。  
銀行間システムに対する（政府とは対照的な）犯罪攻撃は、支払いメカニズム自体ではなく、周囲のビジネスプロセスに関係しています。  
 国際電信送金が実際に機能する方法は、銀行が互いに口座を維持することです。したがって、銀行Aが銀行Bの顧客にお金を送るとき、実際に「この顧客に私たちの口座から次の金額を支払ってください」という指示を送ります。  
121なぜ銀行がエンドツーエンドの暗号を使用して新しいシステムを構築するのではなく、銀行規制当局はインサイダー取引に対するルールを実施するために銀行間のすべてのメッセージトラフィックと銀行内のトラフィックへのアクセスを要求するのかと質問するかもしれません。  
3。  
 銀行がマネーロンダリング当局に報告できるように、大規模な取引を探すフィルターもあります[75]。  
スウィフトを介して行われた最も有名な攻撃は、2016年2月4〜5日で、北朝鮮のエージェントがバングラデシュ銀行から6300万ドルを盗みました。  
 合計8億5,100万ドルの追加の30件の取引がFRBによる手動審査のためにフラグが立てられ、送信されませんでした。もう1千万ドルがスリランカに送られ、支払い銀行がつづりの間違いに気付いて支払いを停止した後に回収されました。しかし、あなたの人生の目標が銀行詐欺から金持ちになることである場合、コンピューターをいじるのではなく、法律の学位を取得し、銀行のマネージャーとして働く方が良いでしょう。  
•おそらく最初の有名な電信詐欺は、コンピューターコンサルタントのスタンリーリフキンがSecurity Pa-cific National Bankから1,000万ドル以上を横領した1979年のことでしょう。  
彼は、電信送金部門に転送を指示するときに内部で使用される認証コードを観察し、それを電話で使用しました。これは、システムインターフェイスでの二重制御の故障の典型的な例です。  
 彼が失敗したのは、彼が石を集めた後に何をすべきかを計画していなかったからです。  
•わずかに異なるタイプの詐欺が1986年にロンドンとヨハネスブルグの間で発生しました。  
 彼らは7ランドとポンドの為替レートでヨハネスブルグに送金し、翌日の4時に再び戻ってきました。  
 彼がディーリングルームでそれらを見たとき、マネージャーはコレクティヴジャケットに止まることなくﬂし、国境を越えてスワジランドに行き、そしてナイロビを経由してロンドンに向かった。  
 英国には為替管理がなかったため、取引管理詐欺は無罪ではなかったため、彼を引き渡すことはできませんでした。  
セキュリティエンジニアリング397ロスアンダーソン12。  
 自動預け払い機•悪意のある人物が保証書を使って詐欺を逃れるのを見ました。  
 これは、2つの銀行間のSWIFTメッセージまたは紙の手紙として設定できます。  
 偽造された保証が本物であると認められた場合、「受益者」は彼の時間を受け入れ銀行から借金し、それをロンダリングし、消えます。  
 その後、2つの銀行がだれの誤りであるかについて論じるときに、コンピュータフォレンジック事件に終わる可能性があります。  
 しかし、これをより広い文脈で見る必要があります。  
 そして、非常に頻繁に、重要なトランザクションはカジュアルな検査ではそのようには見えません。  
12。  
 このストーリーには少なくとも4つのコンポーネントがあります。最初の現金自動預け払い機（ATM）。第二に、クレジットカード。第三に、2000年代半ば以降、デビットカードとクレジットカードの両方を引き継いだチップカード。第4に、電話バンキングを含む非接触型決済。  
 それらは、1938年に発明者のルーサー・シミアンによって考案されました。ルーザー・シミアンも、テレプロンプターと自動焦点カメラを考案しました。  
 その復帰は1967年、ロンドンのエンフィールドにあるバークレイズ銀行によって設置されたDe La Ruewas製の機械でした。  
400万台、つまり10万人あたり41台[2041]。  
 つまり、ATMは、現代の商用暗号技術と小売決済技術を地面に取り入れた「キラーアプリ」でした。  
4。  
 カードの磁気ストリップには、Security Engineering398Ross Anderson12が含まれています。  
 AUTOMATIC TELLER MACHINESPAN：8807012345691715PINキーKP：FEFEFEFEFEFEFEFEDESの結果{PAN} KP：A2CE126C69AEC82D {N} KP decimalized：0224126269042823Natural PIN：0224O↵set：6565Customer PIN：6789図12。  
 「PINキー」と呼ばれる秘密キーは、PANを暗号化し、それを10進数化して切り捨てるために使用されます。  
 このセットには暗号化機能がありません。顧客が自分のPINを選択できるようにするだけです。  
3。  
 Soeach ATMはすべての顧客PINを検証できます。  
1990年代半ばから、ネットワークの信頼性が高まり、ATMはオンラインでのみ動作する傾向があり、設計が簡素化されました。  
ただし、基本原則は変わりません。PINは暗号化を使用して生成および保護されます。  
1。  
 SCDには、銀行サーバールーム13のHSMと、ATMおよびその他のPINエントリデバイスの暗号モジュールが含まれます。  
 したがって、たとえば、カードは、カードをエンボス加工し、磁気ストリップをエンコードしてチップを初期化するマシンを備えた施設でパーソナライズされ、PINメーラーは、HSMに接続されたプリンターを含む別の施設で印刷されます。  
3。  
同様の儀式（ただし、3人で）は、VISAなどのネットワークスイッチとバンクの間でマスターキーを設定するために使用されます。  
4。  
 ATMがPIN検証をローカルで実行する場合、PINキーは端末マスターキーで暗号化され、ATMに送信されます。  
5。  
 このPIN変換機能は、完全にHSM内で実行されます。  
ATMネットワークは急速にSwiftよりも桁違いに大きくなりました。  
 20,000の銀行間で鍵交換または金融決済を双方向で行うことはできなかったため、各銀行はVISAなどのスイッチング組織が提供するスイッチに接続し、これらのスイッチのHSMがトラフィックを変換します。スイッチは信頼されているため、何か問題が発生した場合、結果は深刻になります。  
あるケースでは、スイッチマネージャーが正義から逃亡し、別のケースでは、スイッチでのY2K関連のソフトウェアアップグレードが失敗し、その結果、1か国のカード所有者は、アカウントが空でも、1日または2日間、お金を引き出すことができることに気付きました。 。  
1980年代に私が1人だったATMネットワークとセキュリティシステムを設計したエンジニアは、犯罪者は比較的洗練されており、システム設計についてはかなり知識が豊富で、攻撃方法の選択は合理的であると想定していました。  
 銀行は承認応答で認証コードを省略するなど、手抜きを心配していました。  
 私たちは、デュアルコントロールを適切に実施できないことを知っていました。銀行のマネージャーは、キーボードに触れることは尊厳の下にあると考えたため、メンテナンスの訪問後にATMマスターキーコンポーネント自体を入力するのではなく、ほとんどの場合、両方のキーコンポーネントをATMエンジニアに提供します。  
 これが私たちの終末のシナリオでした。  
 2017年12月、南アフリカのPostbankの鍵が、データセンターの移動中にラップトップに保管されている間に侵害されました。  
 コピーは目撃者の前で破壊されることになっていたが、どういうわけか棒が失われた。  
4分）は56,000回のトランザクションで盗まれましたが、その多くは貧しい人々に発行されたカードからのものです。セキュリティエンジニアリング400ロスアンダーソン12。  
 自動テレラーマシン  
ただし、過去50年間のPINベースの支払いカードに対する数百万の詐欺は、非常に多様であることが判明しました。  
4。  
 カードの詐欺の相次ぐ波があり、そこで脆弱性が発見され、悪用され、最終的に修正されました。  
1990年代初頭の最初の波は、初期の磁気ストリップカードシステムの貧弱な実装と管理を悪用しました。  
 彼は偶然の「暗号化の置き換え」のトリックで発見したときに彼を始めました。彼は銀行カードの口座番号を妻の口座番号に変更し、彼のPINを使用して彼女の口座からお金を引き出すことができることに気付きました。  
 これは、銀行が暗号化されたPINをアカウント番号にリンクせずにカードの磁気ストリップに書き込んだためです。  
 当時のほとんどの銀行は伝票に完全な口座番号を印刷しており、カードは他の正しい情報がなければ機能しました。  
 彼（およびその他）の詐欺の犠牲者約2,000人が団結して、13の銀行に対して集団訴訟を起こし、彼らのお金を取り戻しました。  
 私はこの事件の専門家であり、何がうまくいかなかったかについてのいくつかの論文を書くためにそれを使った[54、55]。  
 ここで、私たちが学んださらに重要で興味深い教訓を要約します。  
先進国では、1か月あたり1か月あたり約4つのトランザクションが行われます。それは英国だけでも月2億4,000万です。  
 コアバンキングシステムに適切なバランス制御がある場合でも、それを供給する周辺システムは不安定になる可能性があります。  
4。  
 また、他の顧客の取引で口座から引き落とされた顧客や、カードの取引で引き落としされなかった顧客も見つかりました。  
）•郵便による盗難は、1990年代に英国のすべてのペイメントカードの損失の30％を占めると見なされ、郵便管理手続きは何年も変わらなかった。  
 2003–5年に、磁気ストリップカードがチップカードに置き換えられたとき、郵便物からの盗難がさらに急増しました。図12を参照してください。  
 主な修正は、コールセンターに電話をかけるか、Webサイトにアクセスしてカードを使用できるようにすることでした。  
 ATMサービスが盗聴器をATM内に設置して顧客カードとPINデータを記録するケースが時折ありました。また、1990年代に、盗まれたカードのPINを一度に£50で盗んだ内部関係者のケースが1つありました。  
インサイダー詐欺は、法律により詐欺の費用が一般的に支払われた英国のような国では特に一般的であり、米国のように銀行が支払った国ではまれでした。英国の銀行は、顧客の苦情は慎重に調査されないことを知っていました。  
•ATMキューに立って、顧客のPINを観察し、破棄されたチケットを受け取り、データを空白のカードにコピーするという肩を並べるトリックは、1980年代中頃にニューヨークで最初に報告されました。そしてそれは1990年代半ばにベイエリアでまだ働いていました。ビジュアルコピーは簡単に停止できます。現在の標準では、チケットにアカウント番号の最後の4桁のみを印刷します。1990年代初頭以来、カードには磁気に3桁のカード確認値（CVV）があります。印刷してはならないストリップ。  
•バグや誤解による損失が多かった。  
 ある銀行がこの手順書を支店のマニュアルに印刷しましたが、3年後に突然の損失が発生しました。  
 そして、私がこれをセキュリティエンジニアリング402ロスアンダーソン12で文書化したという事実にもかかわらず。  
 自動電話機1993年、および2001年のこの本の初版でも、同様の事件が2007年の遅くまで報告されています。  
 これを知っていた通行人は、マシンまで散歩したり、請求額をリセットしたり、400ドルを引き出したり、口座から20ドルだけ引き落とされたりする可能性があります。  
•多くの銀行の運用上のセキュリティ手順は悲惨でした。  
 窓口係は、カウンターの後ろのPCに接続されたプリンターから彼女に新しいPINmailerを役に立ちました。  
 ハンドバッグをひったくりした人が通りを歩いていて、どこかの支店でカードのPINを取得できる場合、暗号化技術はそれほど役に立ちません。  
）•40年間一貫して機能しており、現在でも多くのATMで機能している1つの手法は、レバノンループです。  
 カードはループに引っ掛かり、被害者は放棄します。  
 一部のATMにはこれを挫折させるメカニズムがありますが、そうでないものもあります。  
 彼女のカードが略奪された後、彼女のカード発行銀行が彼女を非難し、これは論争として終わった。  
 最初の報告は1988年のアメリカからのものでした。そこで、詐欺師はカードとPINを受け入れてタバコのパックを分配する自動販売機を作りました。  
•偽の端末攻撃がヨーロッパや90年代のPOSシステムに広がりました。  
5、ガレージPOS端末のタップがオランダのユトレヒトでカードとPINデータを収集するために使用され、1994年にロンドンの詐欺師が偽の銀行支店全体に設置されました[943]。  
 2015年までに、ルーマニアのギャングがメキシコの観光スポットで100ATMを操作し、月額2,000万ドルを盗んだ[1094]と見られました。  
•2010年代半ば以降、詐欺師がATMをハッキングして、空になるまで手形を出し続ける「ジャックポッティング」攻撃が時折見られました。  
4。  
•インサイダーがバックエンドシステムのサーバーの1つに到達したとき、またはサーバーの1つが安全に失敗したときに、不正が発生することがあります。  
 そのような失敗の1つは意図的なものでした。9月11日、ATMネットワークが損傷した後、地方信用組合はニューヨークの顧客に、問題が修正されるまで残高を確認せずに出金を許可することを決定しました。  
1980年代にATMセキュリティシステムを設計するときに最初に間違ったことは、顧客（銀行のシステム設計者、実装者、テスター）が設計したセキュリティシステムを使用できないことを心配する必要があるときに、犯罪者が賢いことを心配することでした。 。  
 数学は興味深いのでセキュリティ専門家は暗号に注意を向けますが、専門家ではない人が実際に使用できるツールを作成するなどの「退屈」なビットにはそれほど注意を向けません。  
 また、最近の支払いネットワークには非常に多くのユーザーがいるため、あまりにもあいまいすぎてテストに捕らえられない脆弱性が発見される可能性を期待する必要があります。  
 ATMの場合、偽端末攻撃は最終的に大きな時間を費やしたものです。  
 2005年頃から、EasternEuropeで製造されたスキマーは地下の市場で販売され、ATMの喉に取り付けて磁気ストリップを読み取り、小さなカメラまたはキーボードオーバーレイを使用してPINをキャプチャするように設計されています。  
 救済策は、磁気ストリップカードからチップカードに移行していますが、これには15年以上かかり、その間、磁気ストリップ詐欺には多額の費用がかかります。  
 重要な要素は、セクション2で説明したように、犯罪者が専門化して組織化し始めたことです。  
12。  
3インセンティブと不正行為米国では、銀行は新しいテクノロジーに関連する多くのリスクを抱えています。  
 裁判官は、「信頼できる証人がセキュリティエンジニアリングに直面したときにロスアンダーソン12を裁定するまで、裁判にかける準備はできていなかった」と裁定した。  
 自動預け払い機は、機械の不利な「証言」であり、法の問題として、立証できないという立派な負担にも直面している」-そして彼女に彼女のお金を返しました[995]。これは、いくつかの軽微な虐待をもたらしましたが、通常、破壊行為からの損失よりも少ないです[2046]。  
彼らが維持したファントムの撤退は起こり得ず、1つを訴えた顧客は誤っているか嘘をついているに違いない。  
 1つの例は、Mundenケースでした[55]。  
彼は1992年9月の休暇から帰宅し、ハリファックスビルディングソサエティでの彼のアカウントを空にしました。  
 ハリファックスハディムは詐欺でお金を得ようとしたとして起訴しました。  
 それにもかかわらず、それは彼らに対する彼らの言葉でした。  
 控訴審が行われる直前に、検察はハリファックスの監査人から彼らのシステムが安全であると主張する報告を出しました。  
 ハリファックスはこれを拒否したため、裁判所はすべてのコンピュータの証拠を拒否しました。  
大騒ぎが収まった後、銀行はシステムが安全であると主張し、イギリスのバートンオントレントのジェーンバジャーがファントムウィズドロウについて訴えられたときに同じドラマが再び現れました。  
システムが証拠を提供する場合は、二重管理では不十分です。  
 銀行が本当に必要とするセキュリティプロパティは、二重管理ではなく、否認防止でした。トランザクションの元本が後で何が起こったかを証明する機能です。  
実際、1992年から4年にかけてのATM詐欺の波の中で、ATMカメラを設置した少数の銀行は、他の銀行から撤退を迫られました。カメラによる証拠は、銀行のシステムが完全ではないという集団的スタンスに対する脅威でした。  
2。  
1は最終的に銀行のシステムを徹底的に調査し、高等法院では信頼できないと非難されます。  
5。  
5クレジットカード現代のカード決済システムにつながった2番目のコンポーネントはクレジットカードでした。  
 結局、商人とカード保有者の数は臨界量に達し、取引量は減少した。  
クレジットカードを使用して店舗での購入の支払いを行う場合、取引は販売者からその銀行（取得銀行）に流れ、小規模な販売者に対して通常2％未満の販売者割引を差し引いて支払います15。  
 各トランザクションには、2つのコンポーネントが含まれます。つまり、カードを販売者に提示し、商品を提供するかどうかをすぐに知りたい場合の承認と、別のシステムを経由して販売者にお金を受け取る決済で、多くの場合2〜3日後です。  
12。  
1クレジットカード詐欺1950年代から1990年代にかけて、クレジットカード取引は、カードのエンボスを使用してマルチパートフォームに紙の販売ドラフトを作成し、金額を書き込んで、顧客に署名させ、小切手と同様に処理することで処理されていました。 。  
各販売者は、ローカルの「ホットカードリスト」に加えて、オンライン承認を要求する必要がある取得銀行によって設定された制限を取得しました。  
 The Crooksの対応は偽造されたカードの大洪水でした。1989年から1992年の間に、磁気ストリップの偽造が、時折の迷惑行為から詐欺の総数の半分にまで増加しました[12]。  
 銀行は、有効期限をパスワードとして使用し、フロアの制限を下げ、商人の割引を増やし、認証時に数値部分がチェックされることになっているカード所有者の住所への配達を主張することにより、リスクを管理しました。  
 オンラインクレジットカード取引（またはCNPルールに基づいて行われた取引に影響を与える）に異議を申し立てた場合、全額が多額の手数料とともに直ちにマーチャントに引き落とされます。  
15Debitカードの方が安価で、大手の販売者はクレジットカードの取引でも1％未満で支払うことができます。  
5。  
増大するカード偽造とオンライン詐欺に対するVISAの対応は、カード検証値（CVV）–カードストリップの内容（アカウント番号、バージョン番号、有効期限）で計算され、ストリップの最後に書き込まれた3桁のMACでした。  
Mastercardは5％、67％上昇しました[386]。  
彼らはまた、技術的にクレジットカードと融合したデビットカードにも登場しました：これは銀行が最初にATMでクレジットカードを使用することを許可し、次に販売時点で異なる時点でデビットカードを使用できるようにした拡張プロセスでした異なる国。  
（PINがPOS端末で既に使用されている国では、この低レベルの偽造カードはATMで直接使用されます。1990年代後半までに、より賢く曲がったビジネスは、顧客のトランザクションのコストを吸収することを学びました。  
 1か月か2か月後、ジュエリー、電気製品、さらにはカジノチップさえも莫大な請求が発生します。  
2000年代初頭、電子犯罪が専門化されるにつれて、ハイテク犯罪者はより適切に組織化されました。  
 これは、オンライントランザクションのターゲット設定から小売端末への攻撃に波及しました。  
 極東では、2000年代中頃からカードデータを盗聴するために盗聴器が使用されていました[1158]。  
 それらの一部は、EMVプロトコルの脆弱性を使用していたため、次のセクションでEMVとチップカードについて説明した後で、それらに戻ってきます。  
 迷惑メールで届く「事前承認済み」カードのメールからの盗難を含む、発行前の不正行為があります。  
 そして、詐欺師が不注意に銀行のカードを盗んで、自分のアカウントの交換用カードを彼らが管理するアドレスに送信する詐欺があります[2013]。  
5。  
セキュリティエンジニアリング407ロスアンダーソン12。  
 クレジットカード12。  
2オンラインカード詐欺今では、従来のクレジットカード詐欺からオンラインのさまざまな方法に転じて、1987年に警察がオンラインクレジットカード詐欺の調査を支援しました。  
 当時のホットカードリストには、その国で悪用されていたカードのみが掲載されていました。海外で地元のホットカードを使用するということは、銀行が無実の顧客ではなく缶を運ぶことを意味しました。  
暴風雨が彼の家の反対側の川岸を洗い流し、警察が彼を締め出すために建てた皮を露出させました。  
 「悪意のあるハッカー」が電子メールやウェブフォームを傍受し、クレジットカード番号を数百万人が収集したため、インターネットでのクレジットカードの使用が詐欺の雪崩につながるのではないかという不安がありました。  
現実はもう少し複雑です。  
 Lotsof Webサイトは暗号化なしで、または弱い暗号化で何年もの間実行され、本当の問題は盗聴ではなくフィッシングであることが判明しました。  
 中間者攻撃を設定できる悪意のあるユーザーは、証明書を取得してトラフィックを暗号化できるため、TLS自体は役に立ちません。  
次に、オンラインで取引されるクレジットカード番号のほとんどは、誰かが商人のコンピュータをハッキングしたために手に負えなくなりました。  
その後、Payment Card Industry Data Security Security Standard（PCI-DSS）、Payment Card Industry Security Standards Council17が共同で発足した。  
最後に、施行がかみ合い始め、2007年10月までに、米国NationalRetail Federationはクレジットカード会社にクレジットカードデータの保存を強制するのをやめるように求めました（チャージバックの場合にカード番号を一時的に保存することになっていた）[1957]  
5。  
17これは、Visa、MasterCard、Amex、JCB、Discoverによって設定されました。現在、他の利害関係者もいます。  
 これは、ドキュメントのかなりのバンドルとそれをチェックする会計士のための多くの仕事に追加されます。  
5。  
商人が直面する他の真のインセンティブは、第一に、紛争のコストであり、第二に、セキュリティ違反の開示に関する法律です。  
 紛争に関しては、多くの国の消費者保護法により、取引の否認が容易になっています。  
 これは、ほとんどすべてのクレジットカード取引がローカルで行われ、ほとんどがかなりの金額であった時代に機能しました。  
 今日、多くの取引は国際的で、金額は少なく、クレジットカードシステムを介した海外住所の確認は不安定です。  
一方、一部の市場セクターには、顧客を利用する多くのWebサイトがあり、ポルノサイトは痛々しいものでした。  
 一部のサイトでは、一度も訪問したことがない他の消費者に請求しました[921]。  
comはそのような慣行について批判され、ポルノ業界の最下層では物事はひどいです。  
 第26節で鉱石作戦のケースについて説明します。  
3。  
 Bankwillは通常、商人にそれぞれ100〜200ドルの手数料を請求し、取引金額を口座から引き落とします。  
 チャージバックがおそらく10％を超えると、銀行がサービスを終了する場合があります。  
g。  
 しかし、それらとの通信販売トランザクションの責任の大部分を残すことは次善の策です：銀行は詐欺のパターンについてより多くを知っています。  
 法律が制定されたときに1人のロビイストが別のロビイストを打つか、主要な判例が設定されたときに1つの法務チームが別のロビイストを打って、私たちはそれで行き詰まります。  
 すべてのウェブサイトでメインのアカウント番号と有効期限を尋ねる必要がありますが、販売者はカードの裏面に印刷されたCVVとカード所有者の住所からの数字を尋ねることもあります。これがVISAカードで機能するのに十分なウェブサイトがあります。マスターカードには、中央監視、セキュリティエンジニアリング409ロスアンダーソン12があります。  
 クレジットカードと、約10回の推測に失敗した後、番号をホットリストします（ただし、これはサービス拒否攻撃につながる可能性があります）[1]。  
 このような攻撃に加え、アンダーグラウンドマーケットで盗まれたクレジットカードデータの利用可能性が高まっていることから、少なくとも大規模なトランザクションでは、より優れたカード所有者認証の開発が推進されています。  
5。  
販売者は、あるしきい値を超えて支払いトランザクションをキャプチャすると、銀行のサーバーにリダイレクトし、パスワードまたはモバイルのSMSに送信されたコードなどの第2要素を使用して、トランザクションを認証するように顧客を招待します。  
3DSは、それを使用した顧客が可能な限り詐欺の責任を負うため、ユーザーを急速に獲得しました。  
 多くの銀行では、最初に3DSサーバーに顧客を直接登録させ、カードが加盟店で初めて使用されたときにパスワードを要求しました。これは、ショッピング中のアクティベーション（ADS）と呼ばれるプロセスです。  
 また、URLが銀行とは関係のないサイトで銀行のパスワードを入力するのに慣れていました。ある銀行では、顧客にそこでATM PINを入力することもできました[1362]。  
 Afactorは政府が2要素認証の使用を義務付けているため、ほとんどの銀行は顧客の携帯電話番号を知っています。  
4。  
7。  
 一部の3DS実装では、依然として銀行のパスワードが使用されています。  
5。  
 2つのアプローチがあります。さまざまなしきい値やその他の手法を使用して異常なパターンを探す異常検出と、既知の不正パターンを探す悪用検出です。  
 私たちは皆、カードがブロックされた経験があり、多くの場合、トリガーは明白です。  
 別の問題は海外での複数の取引でした。 1990年代、私が米国に行ったときはいつでも、私のデビットカードは3つの取引を行い、その後機能しなくなりました。  
セキュリティエンジニアリング410ロスアンダーソン12。  
 EMV支払いのカーディング、しかし、毎秒数万のトランザクションを持つ最新の支払いシステムの完全なスケールは、0であることを意味します。  
より説得力のあるのは、既知の誤用のパターンを探すプロジェクトです。  
そのサービスに加入している銀行は、カードが盗まれた、PINが間違っている、アカウントが空であるなどの理由で、取引が拒否されたときに通知します。  
 詐欺師が1枚以上の盗んだカードをATMに持ち込むと、3〜4枚のカードの中でリストの一番上に到達し、FICOのサービスに加入している銀行が発行したカードをすべて拒否します。  
 世界の銀行の40％以上が、カード発行量で、今や購読しています。  
 英国のウェブサイトは、その詐欺エンジンのために、買い物かごの4％を拒否する可能性があります。  
優れた詐欺エンジンの中核は、よく知られている一連の脅威ベクトル（不正なIPアドレス、または同じIPアドレスからのログオンが多すぎるなど）と一連の品質に基づいてトランザクションストリームから抽出された数十の信号である傾向がありますシグナル（「カードは古くても良い」など）。  
 信号は、SVMまたはベイジアンネットワークのどちらを使用するかではなく、設計の最も重要な部分であるように見えます。  
 詐欺エンジンがどのように失敗するかについては、テスコ銀行に対する2016年の詐欺に関する規制当局の報告は、従業員が詐欺検出ルールに対して「十分なスキル、注意、勤勉さを行使」すること、および「十分な厳密さで攻撃に対応すること」に失敗したことを発見しました、スキル、緊急性 '[687]。  
 このケースについては、セクション12でさらに説明します。  
3チップカードについて説明したら。  
6EMVペイメントカード2003年以来の最大の投資は新しいカードテクノロジーへの投資であり、銀行はクレジットカードとデビットカードの両方をEMVスマートカードに置き換え、続いてカードと電話の両方で非接触型決済を行っています。  
1960年代に集積回路が登場し、1970年代にマイクロプロセッサが登場したとき、さまざまな人々がそれらを銀行カードに入れることを提案しました。  
6。  
 フランスの会社Honeywell-Bullは、メモリ、マイクロコントローラ、および1982年にトランザクションを実行するために必要なその他すべてを含むチップの特許を取得しました。彼らは1983年にフランスの公衆電話で、そして1980年代半ばから銀行で使用され始めました。  
 イギリスのNatWest Bankは、90年代初頭にMondex電子財布システムを開発し、Swindonで試験運用し、Mastercardに販売しました。ソフトウェアは、現在使用されているカードオペレーティングシステムであるMultosに進化しました。この本の第2版の第3章に、これらの初期のパイロットプロジェクトの詳細があります。  
 しかし、支払いカードが本当に役立つためには、国際的に機能する必要があります。特に、多くの小さな国が密集しているヨーロッパでは、何百万もの人々が毎週の店や通勤通勤のために国境を越えています。  
12。  
1チップカードEMV規格は、ATMおよび小売決済端末で使用するためのチップカードとサポートプロトコルを指定しています。  
 チップカードは、2003年から6年にかけてイギリスで導入され、その後ヨーロッパのその他の国でも導入されました。そのほとんどが店舗での認証にATMと同様にPINを使用しており、このシステムは「チップとPIN」と呼ばれています。  
 標準は何千ページにも及ぶ。彼らは現在、非接触型決済、オンライン決済、その他多くのものに拡張されています。また、特定の国や個々の銀行に固有のドキュメントもあります。  
最初に、カードはそのクレデンシャルを、プライマリアカウント番号（PAN）とカード発行銀行によって署名された証明書で構成されるPINエントリデバイス（PED）またはターミナルに送信します。  
 カードはPINをチェックし、それが正しい場合は、N、d3、Xのメッセージ認証コード（MAC）である認証要求暗号文（ARQC）を計算します。  
C�！ T：PAN、d1、CertKB（PAN、d1）T�！ C：N、t、X、d2、PINC�！ T：d3、MACKCB（d3、T、N、t、X）ARQCは、カードとバンクの間で共有されるキーKCBを使用して計算されます20。  
 そのようなセキュリティエンジニアリング412ロスアンダーソン12は省略しています。  
 EMV PAYMENT CARDSOine支払いまたは支払いネットワークを通じてカード発行銀行にトランザクションを送信します。  
 カードは、トランザクション証明書と呼ばれる追加のMACで応答します。  
 ほとんどの銀行が代行処理に依存できるようにしたいので、暗号を本当に制約するのはVISAとMasterCardからのスイッチ仕様です。  
 プロトコルスイートを理解する最も簡単な方法は、この履歴をたどることです。  
6。  
1静的データ認証多くの国で2011年までのデフォルトのEMVバリアントは、静的データ認証（SDA）でした。  
 そのため、EMVが置き換えていた磁気ストリップカードと同様に、man-in-the-middleデバイスによる攻撃に対して依然として脆弱です。  
 これまでと同様に、販売者には最低限の制限があり、それを下回ると取引が許可されるため、ネットワークや買収銀行がダウンしたときに取引を停止する必要はありません22。  
 証明書には当初、マグストリップカードを偽造するために必要なすべての情報が含まれており、チップとPINの導入により、人々は現金自動預け払い機ではなく、どこでもPINを入力するようになりました23。本物の端末から、そしてマグストリップの偽造によって現金化されます。  
2000年代後半から、犯罪者は米国やタイなど、EMVをまだ採用していない国を標的にしました。  
2006年から2010年の間に急増する4。  
 ケンブリッジのローカルBPガレージへの攻撃には、PINをキャプチャするために天井に取り付けられたCCTVカメラと、カードデータを取得するための盗聴が含まれていました。 200人以上の地元住民が、カードのコピーがタイのATMで使用されていることを発見しました。  
21バンクはしたがって、好きなアルゴリズムを使用できましたが、デフォルトは最後のブロックのDES-CBC-MAC withtriple-DESでした。  
23英国では、900,000のショップターミナルと50,000のATMがあります。  
6。  
7439。  
6580。  
8479481。  
7499。  
4597。  
6768。  
4844。  
4：– 2004年から2018年までの英国におけるカード詐欺。  
最も壮大な詐欺は、2008年に発見されました。このとき、ギャングがドバイの倉庫にあるPINエントリーデバイスを中国の工場からイギリスとオランダに向かう途中で傍受し、ギャングにカードとPINデータを送信する小型携帯電話をインストールしました。 。  
 ギャングは逮捕され、英国で裁判にかけられましたが、銀行が証拠を提供することを拒否したため、訴訟は失敗しました。  
 たとえば、図12に示すように、2007年に英国で最も広く展開されている端末であるIngenico i3300には、ユーザーがアクセスできるコンパートメントがありました。  
 シリアルデータ信号を伝送する直径1 mmのビアは、外部の跡を残さずにプラスチックの穴から挿入できる曲がったペーパークリップを使用して簡単にアクセスできることがわかりました。そのようなデバイスの「共通基準評価」は価値がないことが判明しました。セクション28で、その失敗の政治的および組織的な理由について説明します。  
7。  
そのようなデバイスは、PCIによって設定された標準に認定されており、問題の増大はソフトウェアの複雑さです。今日のPINentryデバイスは、8ビットマイクロコントローラーに基づいているのではなく、より大きな攻撃対象となるLinuxまたはAndroidプラットフォームで構築される傾向にあります。  
これらは、任意のPIN（したがって名前）を受け入れ、正規のカードの証明書を使用してEMVプロトコルに参加するようにプログラムされたカードですが、MACにはランダムな値を返します[179]。  
セキュリティエンジニアリング414ロスアンダーソン12。  
 EMV支払いカード図12。  
 デバイスの前面が右上に表示されます。  
 各カードと各端末には、優先カード所有者検証方法（CVM）の優先リストがあり、補足データd1およびd2で共有されます。  
 「認証なし」がオプションであることは意外に思われるかもしれませんが、PINpadを持たないパーキングメーターなどのデバイスをサポートする必要があります。  
 カードと端末の両方に、さまざまな方法の金銭的制限を設定するリスク管理ロジックを含めることができます。  
中間者デバイスを使用すると、多くの攻撃が可能になります。  
 カフェのジャーナリストが1人の学生が運営するTILLにケーキ5ポンドを支払うために行ったとき、トランザクションは50ポンドで本を買うのを待っている書店でのんびりしている他の人が持っていた偽カードに中継されました。  
6。  
 テーマには多くの面白いバリエーションがあります。  
詐欺の規模は国によって大きく異なります。これは、EMVの実際的なセキュリティは状況要因と実装の詳細に依存することを示しています。たとえば、ローカルATMがフォールバック磁気ストリップ処理を実行する程度、さまざまな場所に開かれているローカルショップの割合などです。一種のスキマーアタック、そして–いつものように–インセンティブ。  
 多くの国で、規制当局は銀行がEMVが使用されなかった場合に商人が係争されたトランザクションに対して責任を負うように条件を変更することによってEMV端末をインストールするように商人に腕をねじるのを許可しましたが、そうであった場合は銀行が責任を負うようになりました。  
」だから、理論的には、詐欺はもはや銀行の問題ではなかった。  
4。  
 その後、偽造品が急増し、ショップが端末を入手し始めると、人々はPINを入力することに慣れ、悪意のあるユーザーは不正な端末を使用してカードデータを盗み、ATMで使用するための磁気ストリップコピーを作成しました。  
 正味の影響は、2007年10月までに詐欺が前年比26％増加したことでした[126]。  
 英国の銀行の顧客は、2007年4月から警察へのカード詐欺の報告を中止されました。この取引は、ブレア政府によって犯罪統計を下方にマッサージするために銀行と警察との間で交渉されたものであり、議会委員会によって2度批判された。  
 図12の赤い線の落ち込みから、この影響を確認できます。  
銀行はまた、カード詐欺を調査する小さな警察ユニットの資金調達の多くを引き継いだので、彼らはそのような訴訟をある程度制御することができます。  
6。  
2ICVV、DDA、およびCDA磁気ストリップのフォールバック詐欺を阻止するために、銀行は2000年代半ばから開始し、CVVであるICカード検証値（iCVV）を実装しました。これにより、商人と銀行の間で何年にもわたる悪循環が生じました。  
 2007年から2015年にかけて、他と同様にオンラインで移動し、オンライン部分が適切にカウントされていなかったため、犯罪は着実に減少しました。  
 ボリスジョンソンは、2019年に彼女に代わって立ち上がったとき、2008年から16年までロンドン市長であったときに犯罪が発生したと主張しました。  
セキュリティエンジニアリング416ロスアンダーソン12。  
 EMV支払いカード磁気ストリップ（マグストリップATMトランザクションで読み取られます）と署名ストリップ（オンラインで使用されます）のバージョンからのチップ内のカードデータで異なります。  
 3つのCVVはすべて同じ方法で計算されます。PANの3桁のMACとして、バージョン番号と有効期限は、トリプルDESを使用して計算されますが、計算ではサービスコードの値が異なります。  
最初はドイツで使用され、2011年からヨーロッパ全体で使用されました。  
 暗号化は2つの機能に使用されます。  
 次に、端末は「予測不可能な番号」とカードの公開鍵を使用して暗号化されたPINを含むブロックを送信し、その後にトランザクションデータが続きます。カードは、以前と同じようにアプリケーションデータの暗号文を返します。2000年代に戻ると、DDAカードの価格はSDAカードの2倍です。現在、カードは非常に安価であり、DDAの主な追加コストは、カードのパーソナライズが遅いことです。  
 カードもMAC上の署名を計算することを除いて、DDAに似ています。  
 これは、トランザクションデータを公開鍵と、PIN検証が実行されたという事実に結び付けます。つまり、銀行がトランザクションデータにPIN検証フラグを含めるオプションを選択したと仮定します。  
12。  
1。  
 Steven Murdoch、Saar Drimer、および私は調査し、中間者デバイスがカードにPINを受け入れたことを端末に通知する一方で、端末がチップと署名のトランザクションを開始したことをカードに通知できることを発見しました[1364]。  
プロトコルでは、カードデータd3に、PINが検証されたかどうかを示すフラグが含まれており、端末は、同じ情報を使用してフラグを取得銀行に個別に返します。  
セキュリティエンジニアリング417ロスアンダーソン12。  
 EMV PAYMENT CARDSissuer、EMV標準ではなく、デフォルトではチェックされていません。  
No-PIN攻撃は、盗まれたカードからチップを切り取り、それを趣味のスマートカードのチップの下に接着することによって達成されました。その後、man-in-the-middle攻撃を実行するようにプログラムされました[680]。  
英国の銀行の1つが2010年後半に攻撃をブロックしましたが、おそらく2011年の初めにブロックが解除されました。厳密なエラー処理により誤検出が多すぎたためです（ターミナルフラグがないか、間違っている可能性があります）。  
 攻撃が英国で明確に機能しなくなったのは2017年まででした。  
オーバーレイスマートカードは、2018年後半のそのような攻撃のために中国とおそらくイタリアで使用された可能性があります。  
 これらは、携帯電話のローミングをサポートするために中国で開発されました。アイデアは、通常の電話SIMの上に1つを貼り付けて、代替を提供することです。  
 これらのデバイスは攻撃に最適です。それらは広く利用可能であり、面倒なカスタムハードウェアを構築する手間を省き、使いやすい（JavaCardでプログラムする）。  
6。  
彼は前の晩にレストランのレストランで食事をしていたので、彼のカードは疑わしく、自分のカードがコピーされていたかどうか疑問に思いました。  
 そこで彼は私たちに連絡し、トランザクションログを要求するようにアドバイスしました。  
DDA / CDAカードの場合、EMVの認証ステップは次のとおりです。 C：T、N、t、X、d2、{PIN} KCC�！ T：d3、MACKCB（d3、T、N、t、X）日付tが明日であるときに特定の端末がどの「予測不可能な数」Nを生成するかがわかっていて、今日あなたのカードを手に持っている場合、私はワークアウトできますそのマシンで明日機能するARQC MACKCB（d3、T、N、t、X）。  
6。  
それらのほぼ半分がカウンターを「予測不可能な数」として使用していることがわかりました。  
 次に、EMV仕様に戻り、端末のテストルーチンでは、テスターが3つの「予測不可能な数値」を引き、それらが異なることを確認するだけでよいことがわかりました。  
 彼はEMVカードでe33を支払った、またはそう思った。  
 銀行は、チップとPINが使用されたため、法的責任を負ったと主張した。  
 10のトランザクションは等間隔で3つの異なる取得銀行に提出され、同じターミナルで行われたものの、ターミナルはこれらの銀行ごとに異なる特性で登録されていることがわかりました。  
 本質的には古いトランザクションを再生するのではなく、将来予約するトランザクションを記録するということなので、これを「プレプレイ攻撃」と呼んでいます。  
それ以来、ヨーロッパの多くの国で、通常はストリップクラブやその他のセックス業界の企業の顧客に対するプレプレイ攻撃の事例を見てきました。  
記者発表に続いて、ベッドに戻ってから借方を負わされた人々[1948]を含む、12人以上の犠牲者が前に現れました。  
 しかし、警察にクラブを襲撃して証拠を探すように説得することはできず、最終的に完全なライセンスを取り戻しました。  
 Europetooの他の場所では、難しいことが判明しました。ポーランドのクラクフにあるそのようなクラブの1つが襲撃されましたが、警察は技術的な証拠を探していませんでした。  
 そのため、プレプレイの問題が解決せず、最終的には殺人事件が発生するのではないかと心配しています。  
セキュリティの使いやすさについての興味深い点は、ウォレットまたは財布に4枚または5枚のカードがある場合、それらの残高と与信限度を合計すると、追加の「無許可の当座貸越」に加えて、カード会社があなたに与える可能性があることです。27DixonsCarphoneは£マルウェアが5,390のティルに感染した後の2020年の500,000は、1,400万人の個人データと5のデータを危うくしています。前年には、同様の失敗に対して40万ポンドが支払われました[2039]。  
6。  
 あなたがポケットにたくさんの現金を持っているなら、あなたはおそらく町の悪い部分に入らないでしょう。  
 支払いカードは、この慎重な反射を覆い隠し、穏やかで冷静なときよりもはるかに多くを費やすことができます。  
 たとえば英国政府は、カジノでのクレジットカードの使用を禁止したところです。  
12。  
3非接触型非接触型決済は、1997年にモービルによって米国で先駆けとなり、2000年代にロンドンから東京までのさまざまな輸送システムに採用されました。  
 バークレイズは同じ年に最初の非接触型銀行カードを発行しました。 VISAとMastercardは、支払い用にEMVの非接触バリアントを開発しました。そしてGoogleは2011年にマスターカードPayPass標準を使用してAndroid Payをリリースしました28。  
 AppleがApple Payをローンチしたとき、市場は2014年に転落した。  
 2020年のコロナウイルスの流行により、現金から非接触型にさらに大規模な切り替えが行われ、英国のATMトランザクションは1月の2億3200万から4月の9100万に、現金取引は3分の1から10分の1に減少し、非接触の制限は£30から45ポンド。  
 米国では、端末が「予測不可能な数」Nを生成し、カードはKCを使用して、選択されたトランザクションデータの3桁のMACとして動的CVVを生成し、これがNとともにカード発行銀行に送信されます。  
リスクはトランザクションの制限によって軽減されます– 2020年には、米国では100ドル、英国では30ポンドです。  
 英国とヨーロッパには、ランダムにチェックするために銀行ネットワークに送信される可能性のあるARQCを生成するためにカードが作成されるバリアントがあります。  
 ただし、カードから電話への非接触型支払いの延長により、さらに複雑になり、システムが完全に開示されました。設計については、Googleでいくつかの作業を行いました。  
セキュリティエンジニアリング420ロスアンダーソン12。  
 EMVペイメントカードシェーブは、2つのカードスキームからの競合する提案のマッシュアップになりました。  
 他のAndroidフォンは、NFC機能がソフトウェアで提供されるホストカードエミュレーションを使用します。  
 多くの場合、tok-enizationを使用しています。電話やその他のデバイスには、銀行に代わって機能するオンライントークン化サービスプロバイダー（TSP）によってトークン30とキーマテリアルがプロビジョニングされています。  
非接触型カードが導入されたとき、通常の実装障害がありました。  
 研究者たちはまた、詐欺師が被害者のカードを通りにブラッシングするときに被害者のカードを使ってRFIDトランザクションを実行することによって、または封筒を開かずに郵送されたカードを読み取ることによって、クレジットカード番号、セキュリティコード、および有効期限を取得できるかどうかも疑問に思いました[894] 。  
 2016年11月5日、これは英国のテスコ銀行に対する重大な詐欺につながりました。ブラジルの詐欺師は、モバイルデバイスの非接触型インターフェースでマグストリップデータを使用することにより、高額の取引を行いました。  
顧客アカウント8,261から2分、最終的な損失はわずか700,000ポンドでしたが、攻撃により、銀行の週末の作業手順では対応できない一連の詐欺警告が発生しました。  
 この失敗と顧客への苦痛のために、規制当局は銀行に16ポンドを支払いました。  
2019年に、Leigh-Anne GallowayとTim Yunusovは、電話を装うことで非接触型の制限を£30から£5500に増やすことができることを発見しました。また、悪用可能なプレプレイ攻撃もあります。  
 Androidフォンには、画面がオフかオンか、およびユーザーが最近認証されたかどうかに応じて複数の制限があり、電話と端末は認証されていないフラグを互いに送信します[736]。  
 おそらく、そのような攻撃は銀行の詐欺エンジンによって拡大を防ぐことができる可能性があり、統計にはまだ表示されていません。  
30ペイメントアカウントリファレンス（PAR）、カード番号の恒久的な仮名がありますSecurity Engineering421Ross Anderson12。  
 オンラインバンキング特定のハードウェアに依存せず、QRコードなどの他のチャネルを使用してプロトコルを実行できる革新的なバリアントが登場し始めています。  
第2世代EMVの設計者は、すべての平文ギャップを閉じ、オプションとして距離の境界を追加することさえ話し合っています。  
 しかし、数年前から実行されてきた非接触型の主な問題はより平凡であり、カードの衝突が含まれています：ウォレットに3枚のカードがあり、地下鉄の改札口にウォレットを振った場合、どれが引き落とされますか？カード選択メカニズムは、反復可能な回答を提供するほど堅牢ではありません[1287]。入口と出口の改札口が異なるカードを財布に入れると、最大額の2倍を支払うことになります。  
 PINが販売店のiPhoneに入力された場合、現在Apple Storeに表示されているように、電話に接続して顧客のカードを受け入れる、セキュアカードリーダー-PIN（SCRP）と呼ばれる別のコンポーネントがあります。  
 また、電話はお客様のPINをSCRPに渡し、そこでSCRPは暗号化されてオンライン検証のために送信されます。  
 以下のセクション12で説明するように、ケニアやバングラデシュなどの国では、電話から電話への直接支払いはすでに何千万もの人々にとって日常的です。  
1。  
12。  
1985年、世界で最初のホームバンキングサービスが提供されたのはBankof Scotlandで、その顧客はBritish Telecomが運営する独自の電子メールシステムであるPrestelを使用して支払いを行うことができました。  
4。  
4 –それはマスコミと銀行家を怖がらせた。  
 このシステムでは、指定された口座への支払いのみが許可されていました。送金できるのは、自分の口座と、ガスや電力会社などの銀行に通知した口座の間だけです。  
1990年代初頭にはテレフォンバンキングが急速に成長し、1990年代後半から銀行のウェブサイトが続き、フィッシャーマンが到着しました。  
7。  
7。  
3。  
 悪者はhttp：// wwwのような誤植されたドメインからの粗野なルアーから始めました。  
http：// wwwのような不正なものにcom。  
他のサイト。  
 通常の経済と同じように専門化の増加をサポートする地下犯罪フォーラムが2005年頃から始まったので、ギャングは急速に洗練されていきました。  
 通常の手法は、できる限り顧客アカウントを略奪し、回復が最も遅い銀行のどこにいても侵害されたアカウントにお金を送ることでした。  
 その競合他社の1人は、秘密はアカウントの乗っ取りをすばやく見つけて積極的にフォローアップすることだと私たちに言いました。お金がラバの口座に送金された場合、彼はウエスタンユニオンに歩く前に凍結された口座を見つける必要があります。  
業界はフィッシングWebサイトをできるだけ早く削除することを学び、専門の削除企業がこれに成功しました。  
2番目の戦いの分野は資産の回復でした。詐欺師はお金をすぐに海外に持ち出してそれを洗浄しようとしましたが、業界と法執行機関はそれらを阻止しようとしました。  
 eGoldがFBIに襲撃され閉鎖された後、悪党はフィンランドの銀行を通じてバルト諸国の子会社とロシアに送金し始めました。  
 彼らは彼らの仕事が週に数回の支払いを受け取り、彼ら自身のコミッションを差し引いてからウエスタンユニオン経由で残高を送金するように言われている[789]。  
 規制当局は、もぐらたたきをしました。あるチャネルが閉鎖された後、別のチャネルが開放されます。  
 この戦いは続いており、資金は暗号通貨からアマゾンのギフトカードに至るまですべて洗浄されています。  
2。  
 認証だけでは十分ではなく、キルチェーンの他の脆弱なポイントを見つけることができない場合、それらを補完する侵入検出メカニズムを強化する必要があります。  
7。  
7。  
 チップ認証プログラム（CAP）31は、EMV銀行カードを入れることができる携帯型パスワード計算機で構成されています。  
 ログオンにワンタイムパスワードを取得したり、ログオンチャレンジに回答したり、通常は受取人の口座番号と金額から一連の数字を認証したりできます。  
 応答コードは、切り捨てられたMACとatruncated ATCです。  
 CAPリーダーを利用できるということは、ATMに行かなくてもCCTVで見られる危険を冒さずに、カードを手に持っている強盗がPINを要求して確認できることを意味します。  
3。  
12。  
3マルウェアのバンキング銀行は、部分的なパスワードの質問から初期の2要素認証スキームまで、これまで以上に手の込んだ認証メカニズムを使用することにより、単純なフィッシング攻撃を難しくしました。  
他の悪者は、バンキングマルウェアの形で自動化に目を向けました。  
2011年までに、中間者攻撃がブラウザ内攻撃に発展しました。感染したPCのユーザーが銀行口座を使用しようとすると、ブラウザーマルウェアはトランザクションデータを積極的に変更して、見えないものに変えることができます。何を許可するか。  
 CAPを使用しない銀行は、代わりに専用の認証デバイスを使用するか、電話ベースの第2要素を使用します。7。  
 確認を送信するのは当然のことです31。これは、それを発明したマスターカードのブランド名です。 VISAはこれをDynamic PasscodeAuthentication（DPA）と呼んでいます。  
7。  
’これは、CAPと同じ利点をもたらすようですが、ユーザーインターフェイスが優れています。  
 ヨハネスブルグの詐欺師の中には、孤児で脆弱な子供たちの世話をする慈善団体のCFOの電話番号用の新しいSIMを入手し、銀行口座からR90,460を盗んだ[1514]。  
 セクション3で説明したように。  
1、そのような詐欺は南アフリカからナイジェリアに広がり、その後、2014年からInstagramのアカウントを盗むために最初に使用された2014年から5月にかけてアメリカに広がりました。  
 2019年のケースでは、アリゾナ州ツーソンのAT＆Tcontractorが、SIMスワップギャングが29人の犠牲者から200万ドルを盗むのを助けました[711]。  
 脆弱性には、最近の通話と最近の補充について尋ねることによる人々の認証が含まれ、どちらも攻撃者によって操作される可能性があります[1136]。  
 何万もの顧客サービス担当者が不注意、ハッキング、またはSIMswapギャングから賄賂を受け取る立場にあります。  
 また、ドイツとイギリスでは、攻撃者がSS7シグナリングプロトコルを悪用してターゲットの携帯電話をリモートで盗聴し、その方法で盗み出すケースもいくつかあります[489]（これについては、セクション22で詳しく説明します。  
3）。  
 ただし、米国とヨーロッパでの旅行の方向は、SMSから2番目の要素として離れており、カスタム電話app32に向かっています。  
。  
 誰もがiPhoneの使用を開始したり、ワイヤレスアクセスポイントを介してVoIPテレフォニーを行ったりすると、独立性の前提が崩れます。  
 だから、それは普遍的になりつつあり、悪者たちはそれを破る際に多くの練習をしている。  
org /＃banking。  
7。  
 そのようなメカニズムの歴史は良いものではないので、これは経験豊富なセキュリティエンジニアを悩ませます。それは著作権とDRMに関する章で述べられており、RASPについてはセクション24で詳しく説明します。  
3。  
 そして、おそらく、攻撃者が行う必要があるのは、認証交換を含む文字列を取得するために、ネットワークスタックのメソッドの1つをシムすることだけです。  
12。  
5責任1つの長期にわたる議論は責任を超えてきた。  
 残念なことに、2007年と2015年のEUの決済サービス指令は、紛争解決手続きに抜け穴を残すことでこれに対応しました33。  
 たとえば、HSBCは、顧客にすべてのPINをカードの1つに対して発行されたPINに変更することを推奨した英国銀行の業界団体による以前のアドバイスに反して、アカウントごとに一意のPINとパスワードを必要としました。  
 それや他の多くの銀行は、顧客にアンチウイルスソフトウェアの使用を要求しました。ソフトウェアに最新のパッチを適用する必要が少なくなった。  
 私は個人的にマイバンクから「こんにちは、ロイズTSBです。お母さんの旧姓を教えていただけますか？」という迷惑な電話を受けましたが、迷子になるように言いたくてたまらないのですが、そうした場合、それを再開するのは嫌です。または、お支払いカードを交換してください。  
しかし、2015年頃、悪者たちはより良い方法に進化し始めました。  
7。  
 数字は2017年に収集され始め、33の英国の銀行は英国政府に第72条（2）に「必要に応じて」挿入しました：「支払いサービスのユーザーが、実行された支払いトランザクションの承認を拒否する場合必要に応じて支払い開始サービスプロバイダーを含むプロバイダー自体は、支払いトランザクションが支払者によって承認されたこと、または支払者が不正に行動したか、または意図的または重大な過失により、以下の1つ以上の義務を履行したことを証明するのに必ずしも十分ではない第69条  
8。  
4。  
300万は、リモートでの購入詐欺に次いで2番目であり、残りの合計よりも多いです。  
もう1つは、脆弱な高齢者を対象とすることです。  
 2日後、彼の息子は訪問し、何が起こったのかを学びました。  
 数日後、銀行B（「ミュール銀行」としての評判が良かった）が手際よく返金しました。  
 銀行が大規模な支払いを容易にしたため、大規模な詐欺が容易になりました。昔は、120,000ポンドの持ち出しには、最低でも銀行のマネージャーとの打ち合わせが必要でした。英国では、これは非常に悲惨な点になり、議会の財務省委員会は、取消不能な迅速な支払いは単に誤ったデフォルトであった[1361]と指摘し、決済サービス規制当局がルールを変更して、銀行が現在一部の責任を負うようにしました。  
 中規模のトランザクションも保留されます。バスルームを改修するために配管工に数千ドルを支払おうとすると、銀行から不安な電話を受けたり、セキュリティセレモニーが行われたりする可能性があります。  
 ビジネスメールの侵害（BEC）として知られ、現在では数十億ドルの損失を占めています[91]。  
ロンドンのアートディーラーから4分。ただし、詐欺師が美術館のメールアカウントをハッキングし、ディーラーから送信されたように見えるメールを送信した後、お金を間違ったアカウントに送金した。  
被害者の企業は、消費者よりもはるかに少ない保護しかありませんが、両方を助けるいくつかの緩和策があります。  
 それでも、今や慎重な慣行は事業契約で会社の銀行口座番号をハードコーディングすることです。そのため、A社がB社ではなくC社に支払いをした場合、誰の過失であるかについて議論の余地はありません。  
12。  
 PayPalは、セキュリティエンジニアリング427ロスアンダーソン12を起点とする多くの電子メールベースの決済サービスプロバイダーの生き残りです。  
 ドットコムブームの時のノンバンクペイアップは、今や伝統的および小説の両方の決済サービスのポートフォリオを備えた銀行に成長しました。  
彼らは、ビクトリア朝の電信ネットワークとともに成長したウエスタンユニオン、および低コストの外国為替取引を提供するより近代的な決済サービスプロバイダーと競争します。  
 犯罪者は多くの支店のいずれかに送金し、現金で引き出すことができるため、ウエスタンユニオンは法執行機関にとって特に問題です。  
 ビットコインなどの暗号通貨もあり、一部の規制当局は現在電子マネー規制を免除しており、高度な暗号工学の章で説明します。  
12。  
1M-PesaM-Pesaはケニアの携帯電話バンキングサービスで、2007年にVoda-foneによって開始されました。  
 200を超える同様のサービスが非先進国で開始され、そのうちの約20で変革を遂げています。現在、そのようなサービスの最大のものはバングラデシュのB-Kashです。  
M-ペサはナイロビとモンバサトの移民労働者が田舎の親戚に家にお金を送るための手段として動き始めました。  
 携帯電話が普及すると、人々は価値を伝達する手段として通信時間を購入し始め、そこから実際の価値を伝達する小さなステップがありました。  
重要な成功要因は、電話会社が、現金をデジタルクレジットに変換し、過去の銀行とは異なり、最も小さな村に到達する数万の販売代理店のネットワークを構築したことです。  
12。  
2その他の電話支払いシステム他の国の多くは、電話支払いシステムを持っているか、電話で合理的にうまく機能する広く使用されている所有権支払いシステムを持っています。  
 2013年まで、これは世界のセキュリティエンジニアリング428ロスアンダーソン12でした。  
 NONBANK PAYMENTS一流の電話決済システム。  
 TencentのWeChat Payがすぐ後に続きます。 2020年には、中国のモバイル決済市場のそれぞれ54％と39％を占めていました。  
 それらは中国のデフォルトの支払いメカニズムになり、視覚的な支払いチャネルを使用しています。販売者はQRコードを表示し、顧客がこれをスキャンして正しい金額を正しいアカウントに送信します。  
 これは、セクション2で説明した情報主権に対する中国のアプローチと一致します。  
2。  
3。  
12。  
3Sofort、およびオープンバンキングクレジットカードは伝統的にドイツでは使用されていなかったため、人々がオンラインショッピングを始めたときには不便でした。  
Sofort¨uberweisungはドイツ語で「即時支払い」であり、産業化された中間者攻撃によってこの問題を解決しようと試みました。  
 その後、Sofortはあなたとして銀行にログオンし、銀行の認証チャレンジを提示します。  
 次に、航空会社にリダイレクトし、チケットを取得します[79]。  
銀行は不公正な競争のためにSofortを訴え、顧客にSofortのWebサイトに資格情報を入力して銀行の利用規約に違反するように仕向けました。  
 ソフォートは銀行業の免許を取得し、他の銀行はただ競争しなければならなかった。  
 2018年1月以降、銀行は、顧客が要求した場合に標準形式のトランザクションデータを他の規制金融機関にリリースするだけでなく、他の機関が顧客のように行動できるようにすることで、システムを開放する必要があります。9。  
 欠点は、詐欺やマネーロンダリングが銀行口座を開くように急速に移行していることです。  
 結局のところ、詐欺やマネーロンダリングに対する従来の規制は、効果がはるかに低くなります。  
 これがどのように発展するのかを待つ必要があります。  
 顧客が支払い手段をQRコードとして提示するだけでなく、販売者はこの方法で支払い要求を提示できるため、顧客の電話でオンライン銀行支払いを開始できます。  
 ここには革新と収束の余地があるかもしれないので、それがどのように発展するかを待つ必要があります。  
9SummaryBankingシステムはセキュリティエンジニアにとって非常に重要です。なぜなら、それが盗難の動機であり、他の点でも魅力的だからです。  
 クラーク・ウィルソンのセキュリティポリシーは、何世紀にもわたって進化したこのアプローチのモデルを提供します。  
 脅威モデルは内部関係者に特に重点を置いています。  
最後に、2000年代半ば以降、電子バンキングシステムに対する攻撃の波がいくつか見られました。アカ​​ウント資格情報のフィッシング、特殊なマルウェアによるman-in-the-browserattacks、2番目の認証要素として使用される携帯電話へのSIMスワップ攻撃、ソーシャルエンジニアリングのお客様は、お金を悪意のある人に直接送金します。  
 パンデミックによって引き起こされた混乱はこれを強調する可能性が高いですが、少なくとも先進国での非接触型支払いや他の国での電話支払いなど、その使用が急増しているメカニズムには数年かかりました。  
これにより、8バイトのPINブロックから16バイトに、つまり3DESからAESに移動できます。トランザクションのバッチ決済からリアルタイムのグロス決済までそして、はるかに。  
9。  
学生と私はかつて、大規模な会計事務所のクライアントであることが不正行為の合図であるかどうか疑問に思いましたが、簡単な分析ではどちらの方法でも証拠がありませんでした。  
 私が大学の統治機関に勤務したとき、私はこのカルテルを1年に100万回も揺さぶり、見返りに何も提供しないことに我慢しなければなりませんでした。ほとんどの作業はジュニアによって行われました。  
 英国政府は、このスキャンダル（およびその他の多くの問題）が発生した後も、2024年以降、監査会社は監査とコンサルティングの慣行を分離し、監査パートナーの報酬が監査事業からのみ得られ、コンサルタントからの相互助成を受けないようにする必要があると決定しました[1050] 。  
1。  
よりよく理解する必要があります。  
 多くのセキュリティ障害は、ユーザー（デフォルトとして危険な選択肢を持っている）とプログラマー（アクセス制御とめちゃくちゃ扱いにくい他のツールを与えられている）の両方のレベルでの使いやすさの悪さに起因するのと同じように、多くの内部制御障害は実際の組織で実際に使用できるようにするのではなく、監査人の快適さのために設計された管理メカニズム。  
 攻撃の進化（SIMスワップの場合など）や環境の変化（オープンバンキングの場合など）によって地面も変化します。  
 EMVの実装が厳しくなり、EMVの2番目のバージョンがここで説明する残りの脆弱性に取り組み始めると、詐欺が周辺に移動することが予想されます。ハッキング攻撃を介して商人に、詐欺、クーポン詐欺などを払い戻します。承認と決済のためのシステムへの事前発行詐欺と技術的攻撃を介して銀行に。  
2。  
 経営幹部が詐欺師であるのか、会社が破産している間に取引されているのかを検出するのにほとんど役に立たないのに、ほとんどの大企業や大規模大学でさえ有名で高価な企業を選ぶのはなぜですか？セキュリティエンジニアリング431ロスアンダーソン12。  
 一般の顧客が他のシステムによって設計されたシステムに悪影響を与えた場合の損害について要約することは間違っています。  
 ソーシャルメディアは、ダウンタイムをさらに苦しくしています。ゲートウェイへのDDoS攻撃が原因で銀行のモバイルアプリが15分間ダウンした場合、ツイッターストームが発生し、取締役が最高経営責任者に電話をかける可能性があります。  
 コロナウイルスのパンデミックはペイメントサービスプロバイダーに最適で、PayPalの株価は約半分に上昇しています。それがフィンテックのイノベーションを推進する可能性のある場所については、おそらくビデオに関連するでしょう。  
 Monzoなどの最新の技術者は、オンボーディングプロセスの一部としてすでに顧客に自分のビデオを録画させていたため、紛失または盗難にあった電話から顧客がアカウントを回復するのを支援するコールセンターのスタッフは、自分がアカウントを開いたのと同じ人物であることを確認できました。 。Bank of International Settlementsから利用可能な支払いシステムに関する多くの論文がありますが、コアバンキングシステムに関する包括的な本は知りません。最も最近では、2020年7月にプレスに行き、サービスの品質とノートを分析しています。ヨーロッパ内での支払いはほとんどが30分未満であり、複数の仲介業者、営業時間、タイムゾーン、資本管理、流動性、および古代のテクノロジーの組み合わせにより、アジアとアフリカへの支払いには数時間から数日かかる可能性があります[162]  
 このトピックについては、パート3で再度取り上げます。  
ATM PINを生成および保護するIBMシステムは、[521]や[951]などの多くの記事で説明されていますが、初期のATMネットワークは[763]で説明されています。  
 アンダーグラウンドマーケットの最初の調査は、2007年にJason Franklin、Vern Paxson、Adrian Perrig、Stefan Savageによって行われました[714]; Security Engineering432Ross Anderson12。  
 要約それでも、焦点はドラッグやマルウェアではなく銀行詐欺にありました。  
同僚と私は、2012年[90]と2019 [91]のサイバー犯罪の大規模な調査に貢献しています。  
cl。  
交流。  
html。  
 これは、不正がどのように行われたかを示すだけでなく、制御が複数のポイントで失敗した方法と、規制当局がどのように詳細を計算したかを示しています。  
セキュリティエンジニアリング433ロスアンダーソン