– KARENSP¨ARCKJONESあなたはそれを壊す方法を知らなければ、何かを安全にすることはできません。  
1はじめに多くのコンピューターシステムは、保護の重要な側面を保証するために、安全な印刷、パッケージング、およびシールにある程度依存しています。  
 シールと不正開封防止パッケージは、一般に、信頼できる配布に役立ちます。つまり、製品が工場から出荷されてから改ざんされていないことをユーザーに保証します。  
 暗号がどんなに洗練されていても、シールの敗北はシステムの敗北となります。  
 エンジニアをホスティングセンターに派遣する前にエンジニアのIDを精査している場合は、IDを目で見て、電子的に読み取ることをお勧めします。  
•一般に、認証情報を改ざん証明ではなく悪用して改ざんするほうが現実的な目標かもしれません。誰かがスマートカードを解体してキーを取り出した場合、詳細な試験に合格するものに再構築することはできません。  
50216。  
 歴史これらの印刷およびシーリング技術の直接的な適用とは別に、現代のカラースキャナーおよびプリンターを使用して簡単に偽造できるようにすることで、新たな可能性が開かれました。  
 これらには、偽造に使用されている準拠スキャナーおよびプリンターを停止する透かし、および自動販売機で偽造を検出できるようにする非表示の著作権マークが含まれます[830]。  
 そのため、デジタルの世界と「面白いインク」の世界はますます近づいています。  
2HistorySealsには、長くて興味深い歴史があります。  
5000年以上前、ブラシステムは、倉庫の管理者にマークが書かれた粘土の封筒でブラを焼き上げることによって紛争を解決するように適応されました。  
 それらは紙が登場する前の社会的統制の手段として中世ヨーロッパで使用されました。カーターは1つの料金所でリードシールが与えられ、次の場所で引き渡されますが、巡礼者は神社からリードトークンを取得し、巡礼を行ったことを証明します（実際、若いグーテンベルクは、埋め込みの方法を考案することにより、ビジネスの最初の一歩を踏み出しました。偽造を防止し、教会の収入を保護するための鉛の封印の鏡のスライバー）[825]。  
 19世紀まで、手紙は封筒には入れられず、何度も折り重ねられ、ホットワックスと印鑑リングを使って封印されました。  
 他の場所では、以前の重要性の痕跡が重要な文書に添付された会社の印鑑と公証人の印鑑、および一部の国の国家元首が法律のアーカイブコピーに適用する国の印章、および一部のヨーロッパ諸国での電子署名の要求に残っています-EUのeIDAS規格に準拠する自然。  
ゆるい商品からパッケージ商品への移行とブランドの重要性の高まりにより、品質管理が向上する可能性だけでなく、悪意のある人々が商品を改ざんする可能性のある脆弱性も生まれました。  
 これは、多くの製造業者が製品を不正開封防止にするのに役立ちました。  
 それはまさにセキュリティエンジニアリング503ロスアンダーソン16でした。  
 セキュリティ印刷香水やタバコから航空機用スペアパーツ、医薬品まで、高価値のブランド品の偽造を防止するための、より大きな市場の一部。  
残念ながら、ほとんどのアザラシはまだかなり簡単に倒せます。  
 したがって、最初にセキュリティ印刷を検討する必要があります。  
16。  
 写真（1839）は攻撃者を助け、次にカラー印刷とスチールエッチング（1850年代）は防御者を助けました。  
政府の諜報機関が別の政府のパスポートを偽造しようとしたとき、またはその通貨さえも、第二次世界大戦のときと同じように、時々同じ人々が両側に関与していました。  
 その例は、1990年代のイギリスの紙幣の偽造から来ています。  
 したがって、反射光でノートを見ると、金属線が点在しているように見えますが、それを押し続けて透過光で見ると、金属ストリップは暗くてしっかりしています。  
 イエタの犯罪集団が美しいハックを思いついた。  
 彼らは裁判で数年の期間にわたって数千万ポンド相当の紙幣を偽造したことが判明した[697]。  
16。  
1脅威モデルいつものように、脅威のモデルのコンテキストで保護テクノロジーを評価する必要があります。紙幣ビジネスでは、20世紀の最後の数年間の大きな成長分野はアマチュア偽造でした。  
3。  
 しかし、高品質のカラースキャナーとプリンターの普及により、汚いウェットインクが必要な時代に偽造をすることを夢見たことのない多くの人々を魅了しました。  
 アマチュアの偽造者は多数存在するため、戦闘が困難です。ほとんどの場合、製品が権威の注意を引くまでに時間がかかるほど小規模です。そして、彼らは犯罪歴を持っている可能性が低くなります。  
業界では、偽造された紙幣または文書の3つの異なるレベルの検査を区別しています[1935]。  
 多くの場合、一次検査官には動機がないか、否定的な動機さえありません。  
 二次検査とは、禁止事項の場合は経験豊富な銀行の出納係、製品ラベルの場合は訓練を受けた製造業者の検査官など、有能でやる気のある人が現場で行う検査です。  
 ただし、装置はコストとバルクの両方に制限があり、深刻な偽造者によって完全に理解されます。3。  
 セキュリティ印刷（およびおそらくは基礎となる産業プロセス）を設計した専門家が、充実した設備とサポートを提供します。  
 一次検査を過ぎて偽造品を入手することは通常簡単ですが、製品と検査プロセスが適切に設計されている場合、二次検査を入手することは通常不可能です。  
 現場の副検査官がどのような偽造品を検出できるかについての主な制限は、必要な機器の大きさとコストに関係しています。  
3。  
3。  
これは、紙幣やパスポートのスクロール作業によく使用されます。•凸版タイプのインクを回転させて、ページに押し付けてくぼみを残す凸版。  
 したがって、前面と背面の印刷を正確に調整できます。パターンは前面と背面の一部に印刷できるので、ノートをライトに近づけると完全に一致します（シースルーレジスタ）。  
Simultanプレスには、インクの色を線に沿って変化させるための特別なダクトもあります（レインボー）。•文書の裏書き、または写真への封印に使用されるゴム印。•写真の封印にも使用されるエンボス加工とラミネート、およびプッシュする銀行カード偽造のコストを引き上げます。  
それらは、製造時にその厚さを変化させることにより、紙に挿入されるより半透明な領域です。  
より近代的な手法には、次のようなものがあります。•オーストラリアで最初に導入された近代的なプラスチック製のメモは、さまざまな機能をシースルーウィンドウに埋め込むことができます。•視野角に応じて緑色から金色に変化する光学的に変化するインク;•インク磁気、フォトクロミック、またはサーモクロミック特性を備えています。•拡大鏡を必要とする米国の紙幣へのマイクロ印刷、紫外線、赤外線、または磁気インクでの印刷など、特殊な機器でのみ表示される印刷機能（これらの最後に使用されているもの）米国の紙幣の黒色の印刷）;•金属糸と箔、単純な虹色の特徴から箔のカラーコピースルー、ホログラムやキネグラムなどの光学的に変化する効果を持つ箔まで。  
3。  
 最もよく知られているのは、サザンクロスの形をした黄色の星のパターンです。これは、多くのBan-knotesのデザインに埋め込まれ、準拠するスキャナーやプリンターの処理を停止します。•Sandia提案の紙などのユニークなストック製造中に光ファイバーがランダムに広がるため、各シートにはデジタル署名を付け、バーコードを使用してドキュメントに印刷できる特徴的なパターンがあります[1746]。  
一般に、紙幣の真正性は、単一のセキュリティ機能の検査では簡単に確認できません。  
 凹版と活版印刷の触覚効果は摩耗するため、しわくちゃとダーティガの偽造紙幣は標準的な方法であり、熟練した紙幣偽造者は淡い灰色の印刷で透かしを模倣します（ただし、透かしは意外にもアマチュアに対して効果的です）。  
1988年にシェイクスピアーのホログラムが英国の銀行カードに導入されたとき、私は銀行の代表として工場を訪問し、業界が第2の供給源を要求していたため、プレートのスペアセットを大規模なセキュリティ印刷会社–そして、彼らのこの競争相手は、許容できるホイルを製造することは全く不可能でした。確かに、正規の印刷版にアクセスできる大手のセキュリティ印刷会社でさえ、偽造できなかったデバイスは、完全に保護する必要がありますか？しかし、7年後にシンガポールを訪れたとき、シェアピアの同様の（しかしより大きな）ホログラムをﬂ ea市場で購入しました。  
 それまでに、警察の専門家は、中国に100人を超える偽造者がいると推定しました。  
 しかし、2018年までに私たちは偽造品を見つける方法を教えられていました。  
 私がそれを本物のメモと比較したとき、銀の帯が緑であるのを見たことがある[1611]。  
そのため、テクノロジーは常に進歩し続けており、単一の保護テクノロジーに依存することは賢明ではありません。  
セキュリティエンジニアリング507ロスアンダーソン16。  
 セキュリティ印刷しかし、セキュリティドキュメントの設計はこれよりもはるかに困難です。  
 長年にわたり、紙幣の設計者は、偽造品をより一般的な一次検査ではなく二次または三次検査に合格させることを防止することを目指していました。  
 言い換えれば、技術的な焦点がビジネスの焦点を奪っていたのです。  
 したがって、真珠光沢のあるインクを使用して、誰も見ないいくつかのあいまいな機能よりも紙幣の金種を印刷する方が良いです。明白で、明確で、わかりやすいものであること。•模倣の基礎を提供できる既存の競合他社がいないこと。•標準化されていること。  
 （セキュリティ製品の主な欠点の1つは、ユーザビリティが無視されることです。  
二次検査では使いやすさも重要ですが、ここでは問題はより微妙であり、本物と偽物を区別するために検査員が従わなければならないプロセスに焦点を当てています。  
 銀行のような二次検査官には多くの機能が知られています。  
 時間が経つにつれて、ますます多くの機能が明らかになります。  
 強調が手動検証から自動検証に切り替わると、このプロセスは困難になる可能性があります。  
 これを数週間または数か月かけて1回行ったので、2回目はずっと簡単に見つけることができます。  
 そのため、障害は手動システムの場合よりも突然、完全になる可能性があり、機能の寿命、死、再生のサイクルは、過去よりも速く変わります。  
3。  
製品のパッケージ化では、典型的なビジネスモデルは、偽造品のサンプルが発見されて実験室に運ばれ、そこで科学者がそれらが異なるいくつかの方法を見つけることです。おそらくホログラムが正しくない可能性があります。  
 これらのキットがかさばって高価である場合、設置できる数は少なくなります。  
 プラスチック製品のシュリンクラップに個々の顕微鏡の紫外線バーコードを印刷するなどのアイデアは、検証に必要な顕微鏡、ラップトップ、およびオンライン接続のコストが原因で失敗することがよくあります。  
金融商品、特に小切手では、改ざんはコピーや偽造よりもはるかに大きな問題です。  
 被害者は小切手を正式に送ります。小切手ははるかに大量に変更され、すぐに入手できる国産の溶剤を使用することがよくあります。  
 しかし、レーザープリンターのトナー（およびタイプライターの修正リボンなどの簡単なもの）を取り除くためのトリックのため、保護は完全ではありません。  
小切手詐欺は、カード詐欺よりも価値が何倍も高く、毎日処理される小切手の量が膨大なため、対処が困難でした。  
 極東では、人々が個人チョップまたは署名スタンプを使用して小切手に署名する場合、低コストの自動検証が可能です[929]。  
2）。  
 現在、SEPAでの支払いは、ユーロ圏での小切手による支払いよりもはるかに迅速かつ安価に電子決済を行っています。  
 ほとんどのfaketravel文書は最初から偽造されるのではなく、変更されています。  
 この理由から、先進国は主にチップベースのパスポートに移行しています。電子パスポートをまだ持っていない国からの訪問者は、チップを含むビザ、または旅行者の生体認証を保存するオンラインデータベースを指すビザを取得する必要がある場合があります。  
4。  
4パッケージングとシールサプライチェーンのセキュリティには、パッケージングとシールの問題があります。  
’ほとんどのシールは、何らかのセキュリティ印刷を素材に適用してタグを取得し、このタグを保護対象の材料に固定することで機能します。他の製品は同じ一般的な哲学に従いますが、異なる材料を使用します。下部には、締め付けが簡単で、切断せずに緩めることができるプラスチックストラップがあり、上部には、保護されたオブジェクトの周りをループし、アクティブに監視されている光ファイバーがあります。付属のレーザータグによるストレッチ用。  
4。  
 光ファイバーを紙にセットするコツについて述べました。また、ランダムな高保磁力信号がカードストリップに埋め込まれている透かし磁気があり、標準の低保磁力機器を使用して、ユニークなランダムパターンが乱されることなく読み書きできます。  
同様のアイデアが冷戦時の兵器管理にも使われた。  
紙の表面は1。  
パターンはレーザースペックルテクニックを使用して測定され、ログに記録されるか、機械読み取り可能なデジタル署名としてデバイスに添付されます[1749]。  
 レーザースペックルを使用して紙を認証し、折り目、乾燥、落書き、均等焼けに強いコードに表面粗さをエンコードすることもできます[332]。  
16。  
2接着剤の問題タグの一意性は製造の副次的な影響になる可能性がありますが、ほとんどのシールは、セキュリティ印刷されたタグをターゲットオブジェクトに固定することで機能します。  
不正開封防止パッケージの特定のケースでは、取り付けは工業プロセスの一部です。それは、ポップアップボタンまたはブレークオフ蓋付きの加圧容器である可能性があります。  
4。  
1：–引き抜いた紙の走査型電子顕微鏡写真（Ingenia Tech-nology Ltd提供）。  
ただし、ほとんどの製品では、実装はかなり貧弱です。  
鋭利なナイフを持って、セルフシールの封筒に入った次の数文字を試してください。  
 しかし、この期待される改ざんの証拠は通常、人々が封筒のフラップを身体から引っ張って開けることを前提としています。  
（一部の接着剤は、最初にヘアドライヤーを使用して柔らかくするか、凍結により壊れやすくする必要があります。  
 どちらの方法でも、慎重に調べたときにわずかにしわくちゃに見える封筒が得られるでしょう。  
 この攻撃は通常、一次検査に対して機能し、おそらく三次検査に失敗し、二次検査に合格する可能性があります：とにかくポストでcrumpleshappen。  
 悪名高い例は、スイスとオーストリアで使用されているビネット、または高速道路通行料のステッカーです。  
 別の車で使用するためにウインドスクリーンのステッカーをはがすと、一部のウインクがフロントガラスにくっつく間に、一部のインクが付いてきます。  
 これは現在オフェンスであり、あなたが捕まれば[1468]罰せられます。  
4。  
 昔は、PINメーラーはマルチパートの文房具とインパクトプリンターを使用していました。封筒を開封し、PINが記載されていた伝票を引き出すことにより、PINを取得しました。SecurityEngineering511Ross Anderson16。  
 体系的な脆弱性に感銘を受けました。  
 この考え方は、目に見える証拠を残さずにアザラシを移動することができないのと同じように、この文房具では、目に見える証拠を残さずに秘密を抽出することはできないということです。  
 フィルムの後ろには、紙のダイカットタブがあり、背景を覆い隠してPINを表示できます。  
初期の生成物は、それらを光にかざすことで読み取ることができ、その結果、光は約10度で表面を見ます。不透明なトナーは、光沢のある接着フィルムに対してはっきりと現れた。  
 もう1つは熱伝達でした。メーラーの上に白紙を置き、アイロンをかけます。  
 この研究は2004年に銀行業界に報告され、最終的に2005年に発表された[284]。  
 それでも今日まで、PINが読みやすいメーラーを入手しています。  
 新しい銀行カードを受け取っていることをacrookが知っていて、メールから盗むことができる場合、彼はカードとPINの両方を受け取るだけです。  
 家族が誤ってPINを学習するのを妨げることがあります。同様に、タブを引き裂かずにPINを読み取り、多額の現金を引き出し、それを行わなかったと主張する顧客が時折存在する可能性があります。その場合、銀行はおそらく「私たちを訴える」とだけ言って、独自のメーラーを否認します。  
 このような動作の原動力はおそらくコンプライアンスです。インパクトプリンターの時代に進化したカードスキームルール、監査手順、保険検査を再考するのは面倒です。5システムの脆弱性特定の印刷のトリックや接着剤に対する特定の脅威から、システムレベルの脅威に変わります。  
 約20分ごとに異なる色が発行され、特定の色の領域を残してすべての人が退去することが時々あります。  
 一方の端には、パターンとシリアル番号が印刷されており、もう一方の面には接着剤が貼られています。用紙は横方向にカットされているため、不注意で引き裂くと完全に破壊されます。図16を参照してください。  
 （一部の空港で使用されている手荷物シールと似ています。  
 お金をかけたくない場合は、各帯域を使用できますSecurity Engineering512Ross Anderson16。  
 体系的な脆弱性図16。  
 印刷は無傷ではありますが、しわくちゃになっています。損傷は、プールサイドの担当者が確認できるほどのものではなく、実際には不注意なアプリケーションが原因である可能性があります。  
 さらに強力な攻撃は、シールからバッキングテープをまったく取り外さず、安全ピンまたは独自の接着剤を使用して固定することです。  
 不正行為をするインセンティブはほとんどありません。ストレッチで2時間泳ぐオリンピックの希望者は、混雑していないときにプールを使用します。  
 しかし、それは失敗する可能性のある多くのことを示しています。  
（それでも、このスイミングプールシールは、高価値の産業用アプリケーション用に販売されている多くのシーリング製品よりも、倒すのが難しいです。  
5。  
 核監視システムでは、ホスト国政府が、認可された民間人のセキュリティエンジニアリング513ロスアンダーソン16から核分裂性物質を迂回させようとしている可能性があります。  
 システミック脆弱性リアクター。  
最も困難な封印作業の一部は、封印を適用するのが敵である場合に発生します。  
 過剰生産は、世界中の偽造品の主な原因である。加害者は許可された製造プロセスと原材料にアクセスでき、グレーマーケットは自然な流通チャネルを提供します。  
化粧品などの高価値商品の典型的な解決策は、最終組立工場を運営する企業からその身元が秘密に保たれている、多くの異なる会社からの包装資材の調達を含む場合があります。  
 メーカーのフィールドエージェントがショップでランダムに購入したサンプルのシリアル番号を確認できるオンラインサービスがある場合や、すべてのさまざまなシリアル番号をリンクしてオフラインチェックを行うパッケージにデジタル署名がある場合があります。  
 ブドウ畑が誤ってヴィンテージとラベル付けされたとき、実際に買い取られたブレンドされたブドウから作られた膨大な数のワインのケースのように、ブランド所有者自身が悪人である場合があります。  
シーリングメカニズムは通常、補完的な制御プロセスを考慮して設計する必要があります。  
 正規品であると信じて、グレーマーケットで偽造品を購入した販売業者は、犯罪者の意図なしに検査官を騙そうとする可能性があります。  
 また、ディストリビューターが完全に暗闇にいる可能性もあります。偽造品を売っている人がいるかもしれません。  
 航空会社の倉庫（および飛行機が着陸した後の免税カート）の在庫はすべて完全に本物です。  
16。  
2ガンガン対策シールがシール対象物に適切に付着しているかどうかは、低レベルの状態の誠実さと勤勉さにも依存します。  
3。  
2トラックスピードリミッターシステムでは、ギアボックスセンサーは、特別なトングで所定の位置に圧着されたリードディスクで校正用ガレージが密閉する1本のワイヤーを使用して固定されます。  
5。  
 これは、アマチュアの彫刻家のクラスに行くよりも簡単なので、アザラシのキャストを取り、青銅から一対のシーリングトングを鍛造できます。  
 一部の空港では、チェックインキューの近くにある機械を使用してX線撮影した後、チェックバッグにテープシールを貼っています。  
 とにかく、空港のセキュリティはとにかくほとんど劇場です。  
 大きな問題の1つは、アザラシを検査することになっている職員が実際にそうしたかどうかを確認することです。  
 したがって、港に到着する何千もの輸送用コンテナのシールを検査することがタスクである場合、実際に各コンテナを確認するにはどうすればよいですか？1つのアプローチは、暗号化キーストリームジェネレータを生成する小さなプロセッサを各コンテナに含めることです。 1分ごとに新しい番号。改ざんイベントが検出されると、デバイスはそのキーを消去し、それ以上番号を生成できなくなります。  
 そのようなシールは「証拠防止」シールとしても知られています。つまり、デバイスが改ざんされていない情報を保存し、改ざんが発生した場合は破棄して、敵に偽造品を残さないという考え方です。  
シールを貼ったり確認したりするための十分な不注意が不注意である場合、私がそれらの1つを買収すると、結果として生じる欠陥はそれ自体が不誠実であることを証明しません。  
5。  
たとえば、スピードリミッターのシールは、トラックのエンジンが蒸気洗浄されたときに壊れることが多いため、壊れたシールが交通警官が発見できるすべての証拠である場合、改ざんされたとしてドライバーが起訴されることはありません。  
）封印されすぎた封筒を開いた後、スパイは「通関により開封」または「輸送中のバースト-PostOceにより封印された」とステッカーで再度封印できます。  
このような障害や攻撃の結果は、慎重に検討する必要があります。  
 極端な場合、シールの堅牢性に信頼を置くと、正義の流産につながり、シール製品の証拠（したがって商業的）価値を損なう可能性があります。  
5。  
4。  
 テロ容疑者は、彼らの統制命令がもはや正当化できなくなったときに解放され、最終的にタグ会社は犯罪行為の契約を失った。彼らは法務省に死んだ人または刑務所にいる人にタグを付けたことに対して法務省に請求し、何百万ポンドもの罰金を支払った彼らの監査人[193]。  
5。  
 コーポレートシールはその良い例です。  
 数社のサプライヤーがプレートを製造しており、数百枚を注文した弁護士は、これまでチェックが行われなかったと言っています。  
 封印の本当の目的は、偽造を防止することではなく、シールを添付する必要のある文書に対して弁護士事務所が追加料金を請求できるようにすることです。  
これらのテクノロジーはすべて、購入を希望する人なら誰でも自由に利用でき、特に高価でもありません。  
 通りを歩き、倉庫で未使用の封筒を受け取ることができる限り、ある程度の時間を費やして攻撃の計画を考えている人を阻止することはできません。彼は宅配便のネットワークを介しての小包の旅行の前または後のいずれかにパッケージを置き換えることができます。  
 これは完全に信じられないことです–警察の研究室がセルロテープ用の魔法の溶剤を発明していなくても、19世紀のツァリスト警察はすでにフォークの棒を使って封をした封筒の中に手紙を巻き取り、引き出し、読んでから戻すことができました[1001 ];そこに、そして実際にヨーロッパ中の手紙作家はレターロックを使用しました-改ざんを明らかにすることを望んだ折り目、スリット、シールの複雑なシステム[366]。  
 会社のロゴが入った封筒を簡単にスキャンし、安価なカラープリンターを使用して複製できることを考えると、これらの前提条件はかなり野心的です。  
これにより、偽造者の仕事がはるかに簡単になります。  
5。  
5。  
 1980年代後半に銀行が磁気ストリップを読み取る認証端末を導入したため、クレジットカードは偽造に対して脆弱になりました。一方、ほとんどの業者が顧客が署名するためのバウチャーを印刷するために使用するインプリンティングマシンはエンボス加工を使用し、ほとんどの業者は署名済みのバウチャーを小切手だったら。  
 部分的な変更を伴う攻撃もあります。  
 銀行がクレジットカード番号を生成するために使用したアルゴリズムがわかっていた場合、これはカードの残りの部分を平坦化、再印刷、および再エンボス加工するだけであり、安価な装置で実行できました。  
 いずれにせよ、言ったすべてのホログラムは「これはかつて有効なカードでした」であり、ほとんどの銀行は現在それを中止しています。  
 ただし、防御策を選択するときは、脅威モデルについて非常に明確にする必要があります。それは、偽造、改ざん、複製、シミュレーション、転換、希釈、置換、または他の何かですか？ [1524]脅威モデルが注射器に毒がいっぱいの精神病薬である場合、単純なブリスターまたはシュリンクラップパッケージでは十分ではありません。  
 （そのような膜は存在しますが、消費者製品にはまだ高すぎます。  
）16。  
6検査の費用と性質悪用者の業界には、銀行カードのホログラムを別のものに置き換える-鳩の代わりにウサギと言う-の話がたくさんあります。そこで、店主の反応は次のように言うだけです：「ああ、見て、彼らはホロを変えました-gram！ 'これはホログラムの批判ではありませんが、応用心理学と公教育のはるかに深い問題です。関連する問題は、多種多様なパスポート、運転免許証、レターヘッド、企業印鑑、パッケージのバリエーションです。  
 銀行の店員は、外国の紙幣の写真が入った本を持っていますが、入国管理者も同様に外国のパスポートの写真を持っていますが、セキュリティ機能に関する大まかな情報しかありません。  
）ああ、そして実際の物理的なサンプルがないことは、触覚の側面を適切に検査できないことを意味します。  
 彼女はセキュリティエンジニアリング517Ross Anderson16を改ざんしました。  
 評価手法：30種類の食品のうち9種類を使用し、低テク攻撃のみを使用して、71の改ざん検出専門家を招待し、それらを区別しました。  
 エキスパートは、ほとんどの場合、指示された製品あたりの4秒よりも大幅に長い時間を費やしましたが、ランダム以上のことはしませんでした。  
 不正開封防止パッケージの主な目的は、顧客を安心させることです。二次的な目的には、製品の返品の最小化、デューデリジェンス、審査員賞の規模の縮小などがあります。  
高級品メーカーのように偽造を真剣に受け止める企業は、紙幣印刷業者が開拓した技術の多くを採用しています。  
 親しみやすさは重要です。人々は、地元のお金など、頻繁に扱うものに「感触」を覚えますが、ファンシー化粧品や高価なワインのボトルなど、めったに見ないパッケージに問題があることに気づくことはほとんどありません。  
 一部の製品はこの目的のために電子機器を取得していますが、すでに電子機器を持っている他の製品はwifiチップを取得しています。  
 これらの番号をRFIDチップで非表示にする代わりに、ベンダーは製品のラベルに番号を印刷できます。また、正規の製品を入手したかどうかを心配している人が電話で確認することができます。  
 たとえば、マイクロソフトが最初にアンチスパイウェアベータを出荷したとき、私はそれを家族のPCにインストールしました。そのWindowsのコピーはすぐに悪であると非難されました。  
 私は特に彼らの最初の交渉の立場、つまり私は彼らにもっとお金を送るべきだということを好きではありませんでした。  
 しかし、その後は別のWindowsマシンを購入しませんでした。  
6評価方法この説明では、所定の用途のシール製品を体系的に評価する方法を提案します。  
 尋ねられるべきいくつかの質問は次のとおりです。•シールが偽造されている場合、誰がそれを発見するはずですか？それが一般に公開されている場合、彼らは本物のシールをどのくらいの頻度で見るでしょうか？ベンダーは適切な実験を行って、誤った受け入れ率と誤った拒否率を確立しましたか？それが現場の検査官である場合、彼らの機器とトレーニングにどれくらいの費用がかかりますか？セキュリティエンジニアリング518ロスアンダーソン16。  
 評価方法と、これらの検査官（公共または専門家）は、欠陥を見つけて報告する動機がどれだけ上手か？•自分のしていることを本当に知っている人がシステムを打ち負かそうと懸命に努力しましたか？とにかく、敗北とは何か–証拠価値の改ざん、偽造、改ざん、侵食、または商業的信頼性に対する「PR」攻撃？•それを設計したチームの評判は何ですか？敵の製品を無事に破った歴史はありましたか？ •フィールドでの期間はどれくらいですか。また、進歩により敗北が大幅に容易になる可能性はどれくらいありますか？•シール材を購入、偽造、または盗むことができる他の人は誰ですか？•シールを貼る人は不注意または腐敗しますか？その場合、どのように対処しますか？•シールは製品の正しい部分（または十分な部分）を保護しますか？•品質の問題は何ですか？汚れ、油、騒音、振動、洗浄、および製造上の欠陥の影響についてはどうですか？製品は屋外の天候、ガソリンの飛沫、皮膚の隣に運ばれたりビールのグラスに落としたりしても耐えられますか？それとも、そのようなことが起こった場合、目に見える形で反応するはずですか？ランダムなシールの失敗はどのくらいの頻度で発生し、どのような影響がありますか？•法廷に出廷する場合、相手側が信頼できる専門家（またはベンダー）以外の専門家がいますか？答えが「いいえ」の場合、これは良いことですか、悪いことですか？陪審はなぜドックの甘い小さな老婦人ではなく、システムの発明者であると信じるべきなのでしょうか？裁判官は公正な裁判を根拠に彼女を許可しますか–あなたの技術的な主張に反論することは彼女が解雇する証拠の不可能な負担になるでしょう？また、会社を詐欺師に売った場合はどうなりますか？•製品を使用したら、シールはどのように処分されますか？誰かがゴミから古いシールをいくつか回収した場合、あなたはうんざりしていますか？ハードウェアを打ち負かすのではなく、人々をだます。シールが（契約製造の場合のように）敵によって、または腐敗しそうな誰か（トラック会社の事業に勝つことを熱望しているガレージなど）によって適用される場合は特に注意が必要です。  
このライフサイクル全体の保証プロセスは、システム全体に適用する必要がある保証プロセスの縮図にすぎません。  
セキュリティエンジニアリング519ロスアンダーソン16。  
 概要16。  
 シーリングは、製造から材料管理、適用、検証、最終的な破壊まで、シールの全寿命にわたって評価する必要があります。重要なアプリケーションでは、敵対的なテストを強くお勧めします。  
研究の問題これは、多くのアイデアが影響を与えずに出て行ってしまった領域です。  
 1つの例は、コールドチェーン保証です。  
 しきい値を超えた場合に、化学反応に基づいて異なるバーコードを表示するわかりやすいペーパーストリップもあります。  
さらに難しい問題は、規制の厳しい業界で消費者をどのように支援するかです。  
 しかし、技術はそれを修正しており、おそらくソリューションはパッケージングではなく、Amazonのような大規模小売業者に対する規制措置にあります。  
 これは、政府とビッグテックの間の大きな規制上の戦いの1つになるように見えます。  
 最終的に、Facebookが数万のコンテンツモデレーターを雇うように強いられたのと同じように、Amazonは何万もの製品の安全性とコンプライアンスの検査官を雇わざるを得ないと思う。  
セキュリティエンジニアリング520ロスアンダーソン16。  
 概要さらに読むセキュリティ印刷に関する最も明確な教科書は、van Renesse [1935]で、ホログラムやキネグラムなどの技術的なトリックだけでなく、銀行券の印刷からパスポートのパッケージングまで、さまざまなアプリケーションでどのように機能するかを説明しています。  
シールに関する重要な記述は、Roger Johnstonのシール脆弱性評価チーム（e。  
、[989]）。  
 独立からCivilWarまで、アメリカ人は政府ではなく民間銀行が発行した紙幣を使用し、偽造が蔓延しました。  
最近、Supernoteの論争がありました。  
 米国政府は北朝鮮を偽造であると非難し、これを使用して制裁を課した。他の人たちは、現金の流れを追跡するために、CIAがメモを作成した可能性が高いと提案しました。  
 それらは、マネーセンターの銀行が使用する計数機以外のすべての検査に合格するように注意深く設計されていました。そして、出来上がった量は、偽造者が生産するよりも少なくとも1桁少なく、機器の代金を支払うために生産する必要があったでしょう[622]。