1つの方法は、単純にすることで明らかに欠陥がないことです。  
– Tony HoareSecurityのエンジニアは、技術の訴訟弁護士です。  
– Dave WestonToの改善とは変化することです。完璧であることは頻繁に変更することです。  
1はじめにこの本では多くの資料を取り上げましたが、その一部はかなりトリッキーです。  
 これらは保証の問題です-システムが機能するかどうか。その従順なコンプライアンス–これについて他の人々をどのように満足させるかそして持続可能性–それがどれだけ長く働き続けるか。  
 2008年版では、この章を「評価と保証」と呼び、最終的には脆弱性の開示と製品の更新のための適切なプロセスが市販前テストと同様に重要になり始めていると述べました。  
 その世界は今瀕死です。5年前に誰かが100,000ドルを使ってそれをテストするために評価ラボをテストしたので、デバイスは安全であるという考えは、今日ほとんどの人を趣味の悪い人たちにぶつけます。  
1。  
10年前、私たちは2種類の安全なシステムを作成する方法を知っていました。  
 そして、ソフトウェアを含んでいたがオンラインではなかった車や医療機器のようなものを持っていた。あなたはそれらが発売される前にそれらを死ぬまでテストし、そしてパッチが物理的なリコールを意味するので、それから最高のものを望んだ。  
一般的なプラットフォームで報告された脆弱性の数は非常に多く、プロセスを自動化する必要があります。  
新製品では、有能な意欲のある人々がシステムを十分に打ち負かしたかどうかによって、おおよその保証を測定できます。  
 彼らが捕らえられると、怪我のクレームや詐欺紛争が巻き起こり始めます。  
 何度も見たように、1つのプリンシパルが保護のコストを負担し、別のプリンシパルが失敗のリスクを負担するため、多くの場合失敗します。  
 分類された情報を保護するシステムは、広範なコンプライアンス要件の対象であり、評価された製品を攻撃面で使用する必要がありました。支払いシステムについては、詳細は異なりますが、ほぼ同じです。  
コンプライアンスは依然としてセキュリティの設計と投資の主な推進力ですが、特定のトラストバウンダリでの評価済み製品の要求にはあまり重点が置かれていません。  
 医療システム、自動車、航空機を見てみると、セキュリティが組み込まれ始めている安全性に基づく規制体制がわかります。  
 前の章で、それらの特定の要件の一部に触れました。ここでまとめようとする、より広範な問題と原則があります。  
1、私はインセンティブ、ポリシー、メカニズム、保証に基づくセキュリティエンジニアリングのフレームワークを提示しました。  
 それらはしばしば正式な保証プロセスの範囲外になりますが、セキュリティポリシーを定義する必要がある環境の最も重要な部分です。  
1。  
 さまざまなアプリケーションのセキュリティポリシーを調査する本のパートIIの大部分を費やしました。  
•保証とは、システムが特定の方法で失敗しない可能性の推定です。  
 これは従来の評価についてでした。合意されたセキュリティポリシーとメカニズムの強さを考慮して、製品が正しく実装されたかどうかです。  
どのくらいの期間、そしてどのくらい熱心にシステムにパッチが適用されますか？2008年のこの本の第2版までに、大きな欠落要因は使いやすさであると指摘しました。  
ユーザビリティは、上記のフレームワークにおける分野横断的な問題です。適切に行われると、ポリシーに微妙な影響を与え、メカニズムの選択に大きな影響を与え、システムのテスト方法に大きな影響を与えます。  
 しかし、設計者は、保証を明らかなバグがないと単純に見なし、人間の脆弱性を考慮することを止めずに技術的な保護メカニズムを設計しました。  
）使いやすさは純粋にエンドユーザーの問題ではなく、開発者の問題でもあります。  
 多くの場合、開発者はオペレーティングシステムのアクセス制御を使用せず、代わりに管理者権限でコードを実行しました。携帯電話がこれを許可しなかった場合、彼らはアプリに対してあまりにも多くの権限を要求し続けました。暗号化は多くの場合、多くの暗号ライブラリーのデフォルトであるため、ECBモードを使用します。  
 政府が独自の複数のアジェンダを持っているため、規制が常に役立つとは限りません。衝突することがよくあります。諜報機関、安全規制当局、競争当局が異なる方向に進んでいます。  
したがって、保証は政治的および経済的プロセスです。コードと仕様にバグがあるのと同じように、セキュリティポリシーと安全ポリシーにも問題があり、テストスイートでの脱落やエラーにつながります。  
この警告が表示されたら、単一のプロジェクトで構築された静的な製品を評価するという古典的な問題から始めることが役立ちます。  
2。  
2評価製品評価は、セクション8で説明したレモン市場の問題に取り組みます。  
3：顧客が品質を測定できない場合、不良製品は優れた製品を追い出します。  
 1853年の本の錠前屋は、泥棒がすでにそれらを知っていたという理由で、取引の「秘密」を開示することを正当化しました。無知だったのは錠前屋の顧客だった[1895]。  
 単にブランド名に依存する場合は、ベンダーはセキュリティエンジニアを雇うのではなく、広告を購入することもできます。  
 以前の章では、さまざまな製品が評価および認定される静的セキュリティ標準の多くの例について説明しました。  
それは50年前にコンピューターのセキュリティが始まった場所かもしれませんが、コンピューターはどこにでも行き着くので、私たちは他の業界にも目を向ける必要があります。  
 セクション23で、送電と配電についてすでに説明しました。  
1。  
3。  
 トラックと車の両方に運転支援のための複数のシステムがあり、インターネットに接続されているため、重要なセキュリティと安全要件があります。  
これについては、いくつかのケーススタディで説明します。  
28。  
1アラームとロック米国の保険業界は1894年に共同試験所を設立し、電球からの危険を警戒した。それは1901年に火災安全およびその他の基準を開発する非営利団体であるUnderwriters’Laboratoriesとして組み込まれ、1913年にセキュリティ製品の承認を開始しました[1916]。  
 評価者は固定の予算を使ってフローとレポートを探し、その後ラボはデバイスを承認するか、デバイスを却下するか、いくつかの変更を要求します。  
 リスクの1つは慣性です。標準が進歩に追いつかない場合があります。  
セクション13で説明しました。  
4バンピングツールが十分に改善された方法120代後半から30代前半に私は銀行で働き、銀行間セキュリティ基準委員会に行ったとき、話していることを知っていたのはたった4人でした。 IBMから。  
セキュリティエンジニアリング914ロスアンダーソン28。  
 EVALUATIONa 2010年までの主要な脅威。  
2。  
 ドイツなど一部の国の保険研究所は、攻撃が改善するにつれて認定を取り下げる用意ができています。アメリカでは、彼らは、おそらく訴訟を起こすことを恐れて、消極的です。  
28。  
2安全評価体制安全基準は、主要な事故やスキャンダルに対応して、一度に1つの業界で出現する傾向があります。  
 アメリカで最も売れている薬は、硫酸とテレピン油の希薄溶液であることがわかりました–製造するのに本当に安価でありながら、人々がそれが彼らにとって良いことであると信じるのに十分な味わいがありました[2050]。  
 FAAは後に、グランドキャニオン上での2つの旅客機間の1956年の墜落で2人の飛行機に乗っていた128人全員を殺害した後、アイゼンハワー大統領によって設立されました[684]。  
 ラルフネイダーの著書「Unsafe at Any Speed」が1970年に国道高速道路安全管理局（NHTSA）を設立するように議会に拍車をかけるまで、ベンダーは自動車をシートベルトで取り付けるのではなくクロムで装飾することを競っていました。その権力と影響力は相次ぐ安全スキャンダルで増大した。  
 それ以来、欧州連合は世界の主要な安全規制機関に発展し、その機関は航空業界から鉄道信号機、おもちゃまで、業界の安全基準を設定しています[1148]。  
 この意味で、ヨーロッパは「規制超大国」になりました。  
 自動車などの深刻な害をもたらす多くの製品は、通常、独立した研究所での試験後に、明示的な承認を得る必要があります。  
これにより、非準拠2Europeが型の承認を加盟国に委任するときにベンダーが使用する可能性のある言い訳の一部が削除されます。加盟国には、テストを専門ラボに委任するType ApprovalAuthorityがあります。  
 一部の小規模な国ではTAAがあり、メーカーはTAA検査官が立ち会い、独自のテストを行うことができます。2。  
28。  
3医療機器の安全性安全規制は複雑なエコシステムであり、多くの点で不完全です。  
これは、Therac 25医療用加速器のバグが原因で3人の患者が死亡し、さらに3人が負傷した1980年代に顕著になった。  
 ケーススタディは、今日でもソフトウェアエンジニアリングの学生に読まれています[1149]。  
1：–明らかに同じモデルの2つの輸液ポンプ（Harold Thimblebyの写真提供）現在、最も致命的な医療機器は、輸液ポンプであり、静脈内薬やその他の輸液を病院の患者に投与するために使用されています。  
 図28をご覧ください。  
 緊急治療室には、ダースの異なるベンダーからの機器があり、すべてに異なるユーザーインターフェイスが備わっています。  
 輸液ポンプは、cardosと同じくらい多くの人を殺し、その数は英国では数千人、米国では数万人にのぼります[1878]。  
 たとえば、「リットル」は大文字の「L」でマークされることになっているため、「1」と間違われることはありませんが、「0L / h」はこれに準拠していますが、「500ml ' ではない。  
 単なる書類審査です3。  
 これを比較すると、同僚と私が小さなお店や家などの重要度の低いリスク用に設計された盗難警報機の評価を手伝ったとき、私たちの予算は2週間でした。  
2。  
 2つの異なるデバイスが同じ製品として販売されているという事実は、コンプライアンスコストを最小限に抑えるための一般的な戦略です。  
これは多くの分野をカバーする重要な進歩ですが、使いやすさは非常に大きな分野です。  
エンジニアが使用できるいくつかの評価手法について説明していますが、「医療機器の種類に関する経験不足」は、使用エラーの原因となる可能性のある要因のリストの1つにすぎません。  
 数値入力のみでの安全性は複雑な分野です[1879]。おそらくすべてのベンダーは、その専門家や他の何十ものテクニックで専門家を訓練する必要がありますが、多くの人は、彼らがうまくやることができると思うほどのことはしません。  
 しかし、看護師が競合他社の機器の異なるインターフェースを使用するときに生じる混乱が、本来あるべき程度に真剣に受け止められるかどうかは不明です。  
 これは、欠陥のある乳房インプラントに関するスキャンダルに続いて、2017年にヨーロッパ全土に導入され始めました[233]。  
 2020年5月、新しいEU医療機器規制（2017/745）には、市販後監視システムと匿名化されたインシデントレポートのパブリックデータベースが必要になると想定されていました。実装は2021年5月まで延期されました。  
しかし、そこでのムードミュージックは、英国を製薬会社や医療機器メーカーにとって魅力的な場所にするためのものであり、患者にとって安全な場所ではありません。  
ここで興味深い質問です。  
 地元の病院では、そのような事故はおそらく1人月未満で死亡し、輸液ポンプの人はとにかくかなり病気になる傾向があるため、その多くは気づかれません。  
セキュリティエンジニアリング917ロスアンダーソン28。  
 評価営業担当者との素敵な昼食後、6ダースの異なるサプライヤーからの評価。  
（例外は、人々が実際に敵意に非常に敏感であるため、安全障害にセキュリティの角度がある場合です。  
4。  
）ユーザーインターフェイスの標準化は、事故とその原因がより明確にわかる業界でより適切に管理されます。  
 車のコントロールは今やかなり標準的で、右側がアクセル、中央がブレーキ、左側がクラッチです。  
 しかし、それははるかに悪いことに使用されました。  
 平均的な現代のドライバーは、そのような車をレンタルロットから出すのに苦労するでしょう。  
2。  
 パイロットは事故報告に注意を払い、それぞれのタイプの惑星を訓練する必要があります。  
 看護師が同様に各輸液ポンプの型格を取得するように要求された場合、それは実際の費用がかかり、病院の幹部が注意を払い、最終的にベンダーはボーイングに従い、多くの命を救うことができます。  
 ボーイングが1997年にマクドネルドゥグラスを購入し、大型航空機を製造する唯一の米国企業となったため、連邦航空局はボーイングを支援する役割を果たしてきました。  
 買収のさらに有毒な影響は、マクドネルダグラスの幹部が引き継いだことであり、同社は本社をシアトルからシカゴに移し、エンジニアではなく、すでに1つのエンジニアリング会社を破壊し、現在はその目標を掲げている金融関係者によって運営されていました。新しい独占から最大の利益を得る。続いて2回の墜落事故が発生し、インドネシアとエチオピアで346人が死亡しました。  
ボーイングは、エアバスの最新モデルと競合するために、737の燃料効率をより速くする必要があり、これは、より大きなエンジンを意味し、さらに前方に装着する必要がありました。そうしないと、機体を再設計して、規制目的の新しい機体であり、認証にはるかに長い時間がかかっていたでしょう。  
2。  
MCASソフトウェアは航空機の迎え角を知る必要があり、重要な設計エラーは2つではなく1つの迎え角センサーに依存することでしたが、これらは地上ハンドラーや鳥の攻撃によって損傷を受けることがよくあります。  
 これは、安全分析のエラーによって悪化しました。MCASソフトウェアの意図しないアクティブ化は予期されていませんでした。  
 パイロットは、問題を診断する方法またはMCASを切り替える方法を訓練していません。  
同社はまた、2009年のオランダでの同様の過去の墜落事件に対するいじめの捜査官たちから逃れ、最初はインドネシアの墜落がパイロットの誤りのせいになることを望んでいた[857]。  
S  
 ;しかし、パイロットに2つのセンサーの不一致を警告する警告灯は、自動車のサンルーフのように航空会社のオプションになり、MCASを無効にすることができるスイッチの操作が変更され、直感性が低下しました[155]。  
S  
エチオピアでの2回目の墜落後、他の国の規制当局は737Maxを根付かせ始め、FAAはもはやそれらを保護できませんでした。  
2020年3月までに売上高70億ドル、コロナウイルスのパンデミックにより商業用航空の売上が終了し、時価総額600億ドル。  
 2020年8月に承認された修正には、ソフトウェアの変更だけではなく、MCASが両方の迎角センサーを読み取り、飛行ごとに1回だけ、限られたスティック力で展開するようにします。ただし、両方のセンサーが飛行前にチェックされるように手順が変更されました。パイロットトレーニングの更新。規制上の変更により、ボーイングではなくFAAが製造後に各飛行機をチェックするようになりました[592]。  
心理学、インセンティブ、制度、権力も重要です。  
 時間が経つにつれ、リスク評価とリスク低減のために設計された対策は工業化され、コンプライアンスの問題になりがちです。企業はそれを最小限のコストで合格しようとしています。  
 優れたエンジニアになりたい場合は、セキュリティエンジニアリング919ロスアンダーソン28というシステム全体のあらゆる側面を理解する必要があります。  
 評価は関連しているかもしれません。  
2。  
 このセクション9に触れました。  
 Orange Bookの評価は、1985年から2000年にかけてNSAで政府による使用が提案されているコンピューターシステムと暗号化デバイスなどのセキュリティ製品について行われました。  
オレンジブックとその裏付けとなるドキュメントは、3つのバンドで、いくつかの評価クラスを示しています。  
 次のバンドでは、B1は必須のアクセス制御を意味しました。 B2は、ユーザーからTCBへの信頼できるパスである隠れチャネル分析と、厳しい侵入テストを追加しました。一方、B3は、TCBが最小限で、改ざん耐性があり、正式な分析とテストを受ける必要があることを要求しました。  
 （そのレベルに到達したシステムはほとんどありません。  
 セクション9で示した例。  
2つ目は、B3に評価されたシステムが、機密情報、機密情報、秘密情報、または機密情報、秘密情報、および極秘情報で情報を処理できることです。  
 ButOrange Bookの評価は政府の業務慣行に従いました。  
 評価された製品は常に陳腐化していたため、市場は小さく、価格は高いままでした5。  
欧州諸国は情報技術セキュリティ評価基準（ITSEC）を開発しました。これは、防衛請負業者が米国のサプライヤーと競争するのを助けるための共有スキームです。  
 ベンダーは、質問を減らしたり、請求金額を減らしたり、最短時間で、または上記のすべてを行ったりして、製品を最も簡単に利用できるラボを探し始めました。  
 それは決して起こらなかった。  
 その理由は、標準よりもはるかに広く深いものです。  
4。  
国防総省の合同戦術無線システムの60億ドルの失敗に対する5。  
2。  
2。  
 これは、銀行業界と政府を支援することを目的としており、セクション18で説明しました。  
 1994年に発売され、現在も勢いがあり、米国の暗号化機器の顧客に支持されています。1つ目は、ソフトウェアではなく暗号化デバイスのハードウェアを対象としていることであり、FIPS 140で評価された多くのデバイス（最高レベルでも）は、固有の脆弱性を備えたアプリケーションを実行します。  
5。  
5。  
2つ目は、セクション18で説明した歴史的な理由により、FIPS 140-1標準にはレベル3とレベル4の間に大きなギャップがあるということです。  
 FIPS 140レベル3は簡単に入手でき（回路をエポキシに埋め込んでカジュアルプローブにアクセスできないようにします）、一部のレベル3デバイスは壊れにくくありません（エポキシをナイフで削り取ります）。  
 多くのベンダーは、業界が非公式に「レベル3」と呼んでいるものを目指しています。  
 これはFIPS標準では正式な表現がないため、米国外の顧客と話をする場合、ファームソフトンは代わりにCommon Criteriaに依存します。  
2。  
1989年のソビエト連邦崩壊後、軍事予算は削減され、未来の敵はどこから来るのかは明確ではありませんでした。  
作業は実質的に1994〜1995年に行われ、ヨーロッパのITSECモデルはオレンジブックアプローチに勝ちました。  
イノベーションは、複数のセキュリティポリシーのサポートでした。  
 これは詳細なセキュリティポリシーと考えることができますが、システムではなく製品を対象としており、数十ページの詳細に展開されています。  
 誰でも保護プロファイルを提案し、それをセキュリティエンジニアリング921Ross Anderson28に評価させることができます。  
 選択したラボによる評価。  
 しかし、評価は、何がどのように測定されたかに完全に依存します。  
Common Criteriaは限られた成功しか収めていません。  
 このようなデバイスの評価は、EU諸国の諜報機関の代表からなる委員会であるSOG-IS（シニアオフィシャルグループ–情報セキュリティ）が運営する非公式のカルテルによって、しばらく正直に保たれていました。  
 英国は2019年に撤退しました。  
2。  
1悲惨な詳細Common Criteriaについて詳細に説明するには、専門用語が必要です。  
 検査が実行される厳密さは評価保証レベル（EAL）であり、機能テストが十分であるEAL1から、徹底的なテストだけでなく正式に検証された設計を必要とするEAL7までの範囲が可能です。  
最初から何かを考案する場合、最初に脅威モデルを作成し、次にセキュリティポリシーを作成し、それを保護プロファイル（PP）に修正して評価し（適切なものがまだ存在しない場合）、次に同じことを行います。セキュリティ目標を設定し、最後に実際の製品を評価します。  
 製品やバージョン間で比較可能な評価を可能にするために、実装に依存しない方法で表現されることになっています。  
 OneはPPを評価して、それが完全で一貫していて技術的に健全であること、およびSTであることを確認できます。  
 最終結果は、保護プロファイルのレジストリと認定製品のカタログです。  
 たとえば、FCO\_NROは通信（CO）に関連する機能コンポーネント（したがってF）であり、発信元の否認防止（NRO）を指します。  
Tなどの脅威のカタログもあります。  
2。  
Role\_Man –「役割管理：TOEの役割の管理は安全な方法で実行されます」（つまり、開発者、オペレーターなどが自身で動作します）•Pなどの組織ポリシー  
Flt\_Ins –「障害の挿入：TOEは、誤ったデータの挿入による繰り返しのプロービングに耐える必要があります」•ADO\_DELなどの保証要件。  
 また、メカニズムの強度に関する保証レベルと要件の選択を正当化します。  
 品質は大きく異なります。  
 2007年の投票機のプロファイル[563]は、政治家の言葉でより多く書かれていましたが、少なくとも合理的な明快さでした6。  
 セクション18で説明したように、これは政治的な行に発展しました。  
4：スマートカードベンダーは、すべての暗号化製品が「高度な持続的脅威」に対して安全であることを要求するように評価ラボを推し進めました。  
これは本質的に、開発機関環境全体が、情報機関のトップシークレットシステムのように、エアギャップが必要であることを要求します。  
 そしてそれこそがポイントです。スマートカード会社はHSMや市場に侵入する飛び地を避けています。  
4。  
2。  
2。  
2。  
2 Common Criteriaの何が問題になっているのかこの本の第2版が2008年に発表されるまでに、業界の人々はCommon Criteriaについて多くの不満を抱いていました。HSMなどのデバイスを販売したいスタートアップは、現在、数百万ユーロと数年かけてプロセスをナビゲートする必要があります。  
•次に大きいのは、CCはEmsecや暗号アルゴリズムなどの「技術的な物理的」側面を回避するだけでなく、実際にはユーザビリティを無視することを意味する管理セキュリティ対策を無視することです。  
•保護プロファイルは、スポンサー企業が市場を不正に操作するために設計されています。  
ゲームはしばしば安全でない製品につながります：ベンダーはPPを書いて、簡単にできることをカバーします。  
 セクション20で説明したHSMに対するAPI攻撃を思い出してください。  
•保護プロファイルは適切な場合がありますが、アプリケーションに再マッピングする方法は適切ではありません。  
5。  
 このアプリケーションの主な問題は、セクション18で説明したとおりです。  
1、信頼できるインターフェイスがないことです。  
 この穴は、何層ものファッジでしっかりと覆われていました。  
 HSMとSAMは、適格な署名作成デバイス（QSCD）として評価されます[29]。  
7。  
 これがロビイストスキャンの目的です。CC認定HSMを使用して署名鍵を保持している限り、テント内のDocusignなどのサービスを許可するために、認証機構全体がねじられています。  
 経験に応じて進化するポリシーの方向性には同意がありますが、PPまたは製品の再評価は範囲外であると宣言されています。  
2。  
 （FIPSについても同様です。利用可能な標準のうち、PCIのみが更新に対応できます。  
 さまざまな理由から、手書きの紙の投票用紙が投票機よりも優れているという難しい方法を学んでいます。  
•評価の厳密さは国によって大きく異なりますが、ドイツは一般的にほとんど不可能と考えられており、オランダは中央にありますが、スペインとハンガリーは、CLEFがスポンサーに簡単に乗せるようにしています。  
 費用も異なりますが、ドイツでの評価はハンガリーで支払う金額のおそらく3倍です。  
セクション12で説明しました。  
1。  
 そのため、サプライヤーは欠陥のある端子を「CC評価済み」として説明し続けることができます。  
•より一般的には、責任については何もありません。「認定での評価結果の使用手順は、CCの範囲外です。」  
 このようなデバイスには、裁判官の共感を得るためから、悪党の政府からお金を乱用することまで、頭の周りで人々を強打することまで、あらゆる種類の用途があります。  
28。  
7。  
 アイデアは、EALレベルから安全なデバイスの各クラスの単一の保護プロファイルに移動し、政府および学者からの入力を使用して、そのプロファイルを業界の企業間の共同作業として開発することでした[462]。  
これの結果は、CC Webサイトで評価された製品のカタログを閲覧することにより、2020年に見ることができます。  
しかし、ヨーロッパ以外では、CCシステムはベンダーの利益に完全に捕らえられています。  
2。  
 安全なFAXマシンとは何ですか？FAXを暗号化しますか？どういたしまして;ファクシミリが期待するとおりに動作します（覚えている年齢の場合）。  
 電子署名システムを販売したい企業は、EAL4と見なされるacPPでそれらを評価することができます。ほとんどのお客様は、それと古いルールの下で行われたEAL4 +評価との違いを見分けることができません。  
2。  
 あなたが10代の明るい人なら、一流の大学に申し込んで二流の学位を取得するリスクがありますか、それとも地元の大学に行ってスターになるべきですか？どちらの場合もあなたの学位の価値を低下させる評定について心配する必要がありますか？スタートアップのために資金を調達する場合、ビジネスエンジェルから資金を得るか、または大規模なベンチャーファンドを取得しようとする必要がありますか？ある種の認証を取得するかどうか疑問に思っているITベンダーは、いくぶん同じような選択に直面しています。  
 ダブリンのポリシーは、ヨーロッパで最も緩やかなプライバシー規制と最低の法人税を課すことであったため、大手サービス企業はすべてアイルランドにEU本社を置いています。  
 彼らのモデルは3段階のゲームであり、スポンサーは認定者を選択し、認定者は提供者を調査し、おそらくいくつかの変更を要求し、最終的にエンドユーザーは購入するかしないかを決定します[1143]。  
 ほとんどの場合、最大の自己満足の原則が優先されます。所有者は、単一の認証者からの承認を求め、製品を改善するように彼らに要求する試みに抵抗します。1つの例は、製品を持続可能なものとして認定するためにNGOが競合する場合です。そこでは、認定者はスポンサーよりもユーザーの結果を重視しており、目的の物件は単一のスポンサーによって強く管理されていません。  
スポンサー、認証者、およびユーザーだけでなく、より多くのプレーヤーがいる場合、状況はさらに複雑になります。  
 ある会社がいくつかの新製品を発明し、それを一部の顧客に販売しています。  
 彼らは、発明者に、確立された供給業者、または少なくとも第2の供給業者に製品のライセンスを供与することを望んでもよい。  
 企業は、ロイヤルティのシェアを最大化するために、特許を取得するために長く困難な交渉を行っています。これにより、7チロールにある恐ろしい基準が2014年のノーベル賞を受賞し、市場勢力と規制に関するその他の多くの研究に貢献します。  
2。  
2。  
 特許プールは、新しい市場参入を妨げるカルテルになる可能性があります。この苦情は、5Gを中心としたGSMA規格についてなされたものです（セクション22を参照）。  
4）。  
 要するに、産業戦略は、独占やカルテルほどには優れた製品を最適化しません。  
5。  
 しかし、一般的なケースでは、カルテルによって支配されるいくつかのステップを持つ複雑なサプライチェーンの場合、それははるかに困難になる可能性があります。  
 したがって、複数の間接層を持たせることができ、「誰が認証者を認証するか」について競争することもあります。  
EAL4以上でスマートカードやHSMなどのCC評価済み製品の場合、アリスの会社がボブの銀行に製品を販売し、チャーリーにそれが安全であると認証を取得するとします。  
 チャーリーが自分のシステムに署名した場合、この議論はさらに強力になります。  
 そのため、アリスはチャーリーを満足させるために必要なだけ努力します。  
 現実の結果として、ペイメントカードブランドがチャーリーの役割を引き継ぐためにPCIをセットアップしたことがわかりました。  
5。  
セクション28で説明したように、電子署名デバイスの場合。  
7。  
 Docusignなどのオンラインサービス署名プロバイダーによるロビー活動も行われました。  
 （そして一部のEU諸国での税務申告には、そのようなサービスで署名してもらう必要があり、税理士の手数料にさらに20ユーロを追加します。  
 彼は、認定されたウェブサイトがマルウェアをコンピュータにロードしようとする可能性が高いことを発見しました。  
2。  
 この理由は、Trust-eの認定は自発的で安価であり、認定に対する技術的な障壁も低かったためです。  
 多くの規制制度は、新興企業が既存の企業にあまりにも簡単に挑戦するのを防ぐための堀として、また責任の盾として機能します。  
3 Amazon、Microsoft、Google、IBMが規制するまでの間、製品で最も物議を醸している中で、顔認識ソフトウェアの販売をどのように制限してきたか。  
2。  
 欧州は、サイバーセキュリティ法（規制2019/881）を通過させました。これにより、欧州ネットワークと情報セキュリティ局（ENISA）が強化され、戦略の中心に置かれます。  
 安全とセキュリティの規制が一緒になり、必然的に自動車、航空機、医療機器、鉄道信号などの標準化団体によってセクターごとに管理されるため、これは長期的には非常に重要になると思います。  
情報セキュリティ製品の認証に関しては、そのアプローチは「もう1つ盛り上がっている」と表現される可能性があります。これは、ENISAに基づくEUサイバーセキュリティ認証フレームワークを設定し、最上位の認証を引き継ぐことになります。  
 これは、サービスだけでなくプロセスにも適用されます。  
英国政府は長年にわたって認証を懸念しており、認証をより標準化するためにcPPを推進することに関与していました。  
 英国の組織は他の場所で作成された認証を引き続き使用することができますが、CLEFのライセンスを取得したり、認証を承認したりすることはありません8。  
2。  
2。  
 将来の法律では、デフォルトのパスワードの禁止やソフトウェア更新メカニズムの要件など、IoTデバイスの基本的なセキュリティが必要になります。これはETSIを利用して行われており、ドラフトヨーロッパ規格ETSIEN 303 645 V2に至っています。  
旅行の方向は、英国の国家インフラのための重要な機器を開発している企業にとって、そしてより一般的には、製品ではなくプロセスを検討することです。セクション12で説明したセキュリティ管理のISO 27001規格はすでに存在していました。  
4：これは高価であり、大手の会計事務所によって収入の流れに変えられており、CCと同じくらい役に立たない。  
 監査人は会社が彼らに言うことを頼りにしなければなりません、そして、そのシステムを保護する方法を知らない会社は彼らがそうしないとき、単に「私たちはXのための素晴らしいプロセスを持っている」と言うでしょう。  
 そのターゲットは中小企業でしたが、その下で実際に認定された最初の企業は、銀行や電話会社のような大企業であり、企業のデューデリジェンスにすべてのタッセルを追加したいと考えていました。  
 最初の章で、コーポレートワールドでは、信頼できるシステムが保険会社にとって受け入れられるものであることが多いということを思い出したことを思い出してください。  
2。  
6私たちは、NSAが脆弱なシステムを探してインターネットをクロールするMugshotと呼ばれるシステムと、サイバー戦士が関心のあるターゲットの近くで脆弱なシステムを見つけることを可能にするXkeyscoreと呼ばれるシステムをどのように持っているかについて説明しましたか？企業のシステムへの攻撃では、最新のパッチが適用されていないサーバーの数、および目に見える他の妥協の兆候がいくつあるかをカウントすることにより、企業のサイバーセキュリティリスクを評価します。  
 これはラーナー・チロールモデルでは理にかなっています。Bitsightは、エリート大学のように、競合他社に先んじるよう動機付けられているからです。  
 たとえば、サービス会社は現在、学校での旗揚げ競技会を後援することに消極的です。 Bitsightクローラーが、そのような演習のターゲットとして設定したIPアドレススペースに脆弱なシステムを見つけた場合、Bitsightの評価を10％以上カットし、実際のビジネスにコストをかける可能性があります。  
 次のセクションでは、障害分析、バグ追跡、製品間の依存関係、オープンソースソフトウェア、セキュリティエンジニアリング929Ross Anderson28の観点から、信頼性メトリックをさらに詳しく見ていきます。  
 開発チームの信頼性の指標とダイナミクス。  
3信頼性のメトリックスとダイナミクス信頼性はライフタイムプロパティになるため、より良い測定方法が必要です。  
5。  
 安全なコードを取得するには、適切なスキルの組み合わせを持つ賢い人を雇い、共有プロジェクトで一緒に仕事をしてもらい、一緒に仕事をすることを学ぶ必要があります。  
 しかし、これはどのように測定しますか？これには2つの主要な側面があります。テストとバグ修正によりシステムが時間とともに信頼性が高まるための信頼性の向上と、バグが発見され、修正される場合とされない場合の脆弱性の開示です。  
3。  
テスターがシステム内の単一のバグを見つけようとしている最も単純なケースでは、合理的なモデルはポアソン分布です。t統計的にランダムなテストが行​​われた後、バグが検出されない確率pは、p =e�Etであり、Eは、影響を与える可能性のある入力の割合[1175]。  
しかし、広範な経験的調査により、大規模で複雑なシステムでは、t番目の検定が失敗する可能性はe�Etに比例せず、一定のkの場合はtok / tであることが示されています。  
 これは、IBMメインフレームオペレーティングシステムのバグ履歴で最初に文書化され[18]、他の多くの調査で確認されています[1198]。  
 この結果は、多くの場合、セーフティクリティカルシステムコミュニティによって「100万時間の平均故障間隔が必要な場合、（少なくとも）100万時間テストする必要がある」と述べられています[355]。  
k / t動作の理由は[249]に現れ、理想的なガスをモデル化するために開発されたMaxwell-Boltzmann統計が統計的に独立したバグにも適用されることを観察することにより、より一般的な仮定の下で証明されました[312]。  
 バグが統計的に独立していると想定できる場合は、k / t信頼性の増加が最も可能性が高いです。100万時間を取得するには100万時間のテストが必要であるというルールは、MTBFが避けられず、最初のセキュリティエンジニアリングに依存する一定の定数倍までですアンダーソン28。  
 コードの品質とテストの範囲。  
これらの統計は、ソフトウェアの進化モデルと選択圧力下での生物種の進化との間のきちんとしたリンクを提供します。ここで、「バグ」は適合度を低下させる遺伝子です。たとえば、ヘビに捕食されたウサギの個体群は、速度よりも警戒心が強いために選択されます。  
進化的モデルは、オブジェクトやライブラリなどの再利用可能なソフトウェアコンポーネントから得られる信頼性の向上に関する基本的な制限も示しています。十分にテストされたライブラリは、全体的な故障率が新しいコードによって支配されることを意味します。  
 テスターに​​よって測定された障害時間は、プログラムの初期品質、テストの範囲、およびテストの数にのみ依存するため、別の環境でのプログラムのパフォーマンスの可能性に関する情報はほとんどありません。  
 最後に、異なるテスターは、プログラムではなく、並行して作業する必要があります。  
 これにより、機械がどのように失敗するかについて統計的知識が得られるため、機械の実証済みの設計に利点がもたらされます。  
 開発チームによる回帰テストの使用は、新しいビルドごとに数十億のテストケースを一晩で実行できることを意味しました。  
では、信頼性にはどのような制限がありますか？1つ目は、プラットフォームのビジネスモデルによって指示された新しいバージョンの新しいコードによって新しいバグが導入され、2つ目は、敵対的な行動が攻撃と防御の著しい非対称性をもたらすことです。  
 Windowsなどの製品に、それぞれ1,000,000,000時間のMTBFを持つ1,000,000のバグがあるとします。  
 SoheはAhmedがする前にバグを知る必要があります。  
 ブライアンは、完全なWindowsソースコード、数十の博士号、the9の監視を備えています。より自然に、自然淘汰の基本的な定理は、遺伝的差異が大きい種は、変化する環境により迅速に適応できることを示しています[695]。  
3。  
これはすべて、1年間のテストで1億時間に相当します。  
 しかし、ブライアンがアーメドのバグのいずれかを発見した確率はわずか10％であり、それらすべてを発見した確率はごくわずかです。  
 つまり、攻撃者は熱力学を持っています。  
 ただし、この問題を解決するのに何年もかかり、新しい問題が常に発生しています。  
 統計的トラップの単純さを回避する1つの方法–第9章で見たように、これは必須のアクセス制御、マルチレベルのセキュアメールガードなどのアーキテクチャなどのポリシーを意味するようになります。  
 これは、セクション27で説明したように、慎重なネットワーク監視、違反レポート、脆弱性の開示、迅速なパッチ適用を意味します。  
7。  
3。  
 最終的にはコストがかかりますが、システムが実装される前に実行すると、コストが低くなる可能性があります。  
 これが、Common CriteriaやISO 27001のように、競合する複数の評価者の1人からベンダーが支払う基本的な評価が根本的に壊れている理由です。  
2。  
 ワイヤーカードのショートから1億ドルを稼いだ1人のヘッジファンドマネージャーであるジムチャノスは、次のように述べています。  
）敵対的なレビューを行うために、お金または名誉のいずれかで攻撃者をやる気にさせることができます。  
 2番目の例は核の指揮統制の評価であり、Sandia National LaboratoriesとNSAはお互いの設計のバグを見つけるために戦いました。  
3。  
 さらにもう1つは、GoogleのProjectZeroであり、Linuxなどの製品とiOSなどの競合製品の両方で脆弱性を発見することに真のエンジニアリングを費やしており、修正を強制するために90日前の通知後に積極的に開示しています。 。  
学者によるレビューは、最高の状態で、このカテゴリにあります。  
 私たちは互いに競争します–ケンブリッジはバークレーに対して、CMUはワイズマンに対して。  
 セクション27で述べたように。  
上記7では、Appleは、ユーザーによるクリックを必要とせずにiOSカーネルをハッキングできるすべての人に100万ドルを提供しています。これは、iOSsecurity10の重要な指標の1つです。  
28。  
3無料のオープンソースソフトウェアセキュリティメカニズムを監視する必要がありますか？歴史的なコンセンサスは、彼らがそうあるべきだということです。  
 「水星、または秘密とスウィフトのメッセンジャー」で、彼は暗号化について、「悪用される可能性のある有用な発明をすべて隠す必要がある場合、合法的に公然となる可能性のある芸術や科学は存在しない」と再論して正当化した。ビクトリア時代には、錠前屋が錠前の脆弱性について話し合うべきかどうかについても議論が交わされました。セクション13で述べたように。  
4、ある本の著者は、錠前屋と強盗の両方が錠前を選ぶ方法を知っていて、無知だったのは顧客だけだったと指摘しました。  
8私は、核セキュリティにも見られる部分的な開放性について議論しました。  
多くのセキュリティ製品には一般に公開されているソースコードがあり、その最初のコードはおそらくPGP電子メール暗号化プログラムでした。  
オープンソースソフトウェアは完全に最近の発明ではありません。コンピューティングの初期には、ほとんどのシステムソフトウェアベンダーがソースコードを公開していました。  
セキュリティエンジニアリング933ロスアンダーソン28。  
 ユーザーからの厳しい批判にもかかわらず、メインフレームソフトウェアの「オブジェクトコードのみ」のポリシーは、依存性のメトリクスとダイナミックス。  
オープンソフトウェアを支持する強い議論がいくつかあり、反対しています。  
 第2に、システムが非常に複雑になり、ツールチェーンが長くなりすぎて、バストしようとしているバグが、記述したコードではなく、オペレーティングシステムまたは依存しているコンパイラにあることが多いため、そこでバグを見つけられるようにしたいと考えています。あまりにも迅速に、そしてそれらを修正してもらうか、またはあなた自身の修正に貢献してください。  
 第4に、このような製品にバックドアを挿入することはさらに困難になる可能性があります（人々は試みに巻き込まれていますが、エクスプロイトは7桁で販売される可能性があります）。  
プロプライエタリなソフトウェア業界は、オープン性がディフェンダーがバグを見つけて修正できるようにする一方で、攻撃者がバグを見つけて悪用することもできると主張しています。  
 第二に、セクション28で述べたように。  
4、異なるテスト担当者はテストの焦点が異なるため、異なるバグを見つけます。  
 実際には、主要な脆弱性が何年も潜んでいます。  
それでは、攻撃者や防御者はもっと助けられるのでしょうか？信頼性向上の標準モデルの下で、オープン性が攻撃と防御に役立つことを示すことができます[74]。  
 最後に、外に出てデータを収集する必要があります。例として、OpenBSDオペレーティングシステムで見つかったセキュリティバグの調査は、これらのバグがかなり相関していることを明らかにしました。これは、オープン性が良いものだったことを示唆しています[1488]。  
 セキュリティはこれらすべてのテストに合格します。  
3。  
 それでもなお、セキュリティに関する議論は広まり始めています。1999年頃の暫定的な始まりから、USDe国防総省は、特にセクション9で説明したSELinuxプロジェクトを通じて、オープンソースを採用し始めました。  
2。  
 重要な1次的な質問は、有能な人々があなたが構築したものをチェックおよびテストする際にどれだけの費用が費やされたか、そして彼らが発見したすべてをあなたに伝えるかどうかです。  
 そして、重要性が高まっているという2次的な問題があります。ビジネスがLinuxに依存している場合、少なくとも何人かのエンジニアがその開発者コミュニティに関与すべきではないので、何が起こっているのかを知っていますか？28。  
4プロセス保証近年、テストなど、製品に焦点を当てた保証手段に重点が置かれるようになり、開発者や方法などのプロセス手段に重点が置かれるようになっています。  
 他の組織よりもはるかに優れたコードを作成している組織もあります。  
高品質の開発者と低品質の開発者の違いのいくつかは才能次第ですが、多くは労働文化によって条件付けられています。  
リーダーシップが重要です。ボーイングのエンジニアリングリーダーシップの代わりに金持ちの男が737Max災害に貢献したのと同じように、CIOが官僚に置き換えられたときにIT部門の士気が崩壊したのを目にしました。  
 魅力的な要素の1つは魅力です。優秀な卒業生の多くは、大手のテック企業ではなく新興企業、あるいは退屈なオールドマネーセンターの銀行ではなく、際どいフィンテックやヘッジファンドに働きたいと考えています。  
 企業の成長が止まると、昇進は遅くなります。IBMでは、「これまでに辞任したのは財閥だけだった11。  
 一部の企業は、マネージャが毎年チームの最低10％程度の生産性を発揮することを要求する評価システムによってこれに対抗しようとしましたが、これが士気に与えるダメージは恐ろしいものです。人々はコードを書くよりも吸い込むことに時間を費やしています。  
 セクション27で説明した機能成熟度モデル。  
3は、優れたマネージャーが優れたチームをまとめ、長期にわたって改善するのに役立つツールの1つです。3。  
 ウォータークーラーチャットからトップリーダーシップまで、企業環境全体が重要です。  
昔ながらの企業の中には、設計、開発、テスト、文書化、監査、管理管理のプロセスを文書化することを要求するISO 9001規格を支持する者もいます。  
セクション28で説明したISO 27001のように。  
上記9は、効果的というよりは装飾的なものです。  
アジャイル開発方法論が置き換えられたウォーターフォールが近づくように、ISO 9001は能力成熟度モデルによって置き換えられています。  
しかし、信頼できるサプライヤーは認定するのが難しいです。  
 上記のセクション28で説明したように、民間の認証スキームは、カルテルを強化する傾向、または底辺まで競争する傾向があります。  
8。  
 あなたが仕事に長けている場合、それをどのようにして達成しますか？高品質の仕事をしている中小企業は、最も差別的な顧客に販売するとき、一般に、彼らが何をするのかを十分に賢く知っている少数の大企業にとって、より良い結果をもたらします。  
では、ダイナミクスはどうでしょうか？品質を測定することが難しく、品質へのインセンティブが混在しており、品質の向上が難しい場合、進化する製品の保証レベルについて何が有効に言えるでしょうか。それらは牛乳のようになるのでしょうか、それともワインのようになるでしょう[1488]。彼らは年齢とともに良くなるか、それとも衰退しますか？簡単な答えは、実際の測定を行わなければならないということです。  
 製品の機能強化によって新しいバグが導入される割合が、古いバグが検出されて削除される割合と等しい場合は、均衡を見つけることさえできます。  
 経験的に、新しいsystemsoftenの信頼性は、よりエネルギッシュなバグが発見されて修正されるとしばらく改善され、その後数年間平衡状態に留まり、コードが複雑になり、維持が困難になるにつれて低下します（ソフトウェアエンジニアが参照することさえある）老化として）。  
 つまり、現実の世界は複雑です。  
測定にはそれ自体の問題があります。  
4。  
 他の企業はそれをはるかに少なく言っており、Bitsightなどの企業を評価する機会を生み出しています。  
 しかし、医療機器などのアプリケーションでは、透明性を高めるために規制当局が介入する十分な公共の利益があり、セクション28で述べたとおりです。  
上記3で、EUは最近、医療機器規制に関する法律を変更して、アフターマーケット監視を強制しました。  
28。  
2。  
 ソフトウェアがすべてに取り組み、すべてがクラウドサービスに接続されるようになると、安全規制の性質は、単純な市販前の安全性テストから、ソフトウェアに定期的にパッチが適用される何年ものサービス寿命にわたってセキュリティと安全性を維持することまで変化しています。  
 セクション23でスマートグリッドについて説明しました。  
1、スマートメーターセクション14。  
3。  
1。  
 セキュリティエンジニアリングはかなりまとまりのある分野ですが、安全エンジニアリングは、時間の経過とともに、航空機、道路車両、船舶、医療機器、鉄道信号、およびその他のアプリケーションの個別の分野に細分化されてきました。  
3、そして安全エンジニアは、securitytooについて学ぶ必要があります。  
 コロナウイルスの封鎖のおかげで、選択はビデオで公開されています[89]。私は今、私の講義を何年も前に行ってもらいたいと思っています。  
 EUは最大の市場であり、米国政府よりも安全を重視しているため、EUは数十の業界で世界をリードする安全規制機関です。  
 以前は安全性のみを考えていた多くの規制当局も、セキュリティについて考え始める必要があります。  
 規制上の目標は異なります。  
状況が異なる場合、セキュリティ規制当局は攻撃者のコストを押し上げ、収入を減らしたいと思うかもしれません。防衛のコストを削減する;セキュリティエンジニアリングの影響を減らすために937ロスアンダーソン28。  
 安全性とセキュリティの絡み合いセキュリティの失敗;保険会社がサイバーリスクを効率的に価格設定できるようにするため;攻撃の社会的コストとそれらに対する社会的脆弱性の両方を削減する。  
彼らは、各市場の失敗の根底にある経済的な微妙さを無視し、傷害と死、そして直接的な物的損害に焦点を合わせる傾向があります。  
 すでに説明したように、飛行機事故で100人が一度に1人ずつ亡くなっていることは、医療機器の事故で1人が1人ずつ死んでいることよりも、国民の不安がはるかに高まっています。セクション28で説明した安全性の問題から単に解放された300以上のモデルに関する勧告は発行しませんでした。  
3。  
 安全規制当局は、これまで誰も殺していない安全とセキュリティの問題でパニックに陥っている間、毎年数千人のアメリカ人を殺す問題を無視します。  
3。  
このパターンは翌年も続き、FDAは、デバイスがハッキングされた可能性があるとの報告を受けた後、ファームウェアの更新を求めて、米国の465,000人のSt Judeペースメーカーをリコールしました。  
 セントジュードの株価をショートさせた投資会社によって宣伝されたため、レポート自体は物議を醸しました[1838]。  
 このテキストはすべての基礎を網羅しているわけではありませんが、有用な最初のステップです。 2021年に発効します。  
4。  
 2012年のディープニューラルネットワークを使用したコンピュータービジョンのブレークスルーに続いて、急速な進歩がありました。  
3とセクション25で説明したジープチェロキーのハイプロファイルハック。  
4。  
 テロリストはそれらをハッキングして群衆に追いやることができるでしょうか？それらは建物に偽の画像を投影することによって同じ結果を得ることができますか？そして、もし子供たちが電話を使って学校から車を家に呼び寄せることができれば、誰かがそれをハッキングして彼らを誘拐することができるでしょうか？ AndSecurity Engineering 938ロス・アンダーソン28。  
 安全性とセキュリティの絡み倫理についてはどうですか？自動運転車が衝突しかけ、1人または2人の歩行者を殺すことを選択できた場合、どうしますか？どうすればよいですか？安全と保証の側面を一度に1つずつ見ていきましょう。  
 RalphNaderの著書「Unsafe at any speed」[1370]に従い、米国議会はNationalHighwayTra�cSafety Administration（NHTSA）を作成しました。  
 影響は、2009年のChevyMalibuと1959年のChevy Bel Airの間の衝突テストのConsumer Reportsビデオではっきりと見ることができます。  
 50年の進歩のおかげで、マリブの客室は無傷のままです。フロントのしわくちゃのゾーンがエネルギーの多くを吸収し、シートベルトとエアバッグがダミーの運転手を保持し、人間の運転手が立ち去ったはずです[472]。  
 ビデオイラストが示す数十年にわたる進歩には、エンジニアリング、ロビー活動、複数の国にわたる標準的な設定だけでなく、安全運動家と産業の間の多くの闘争が含まれていました。  
 車の安全性には、ドライバーのトレーニング、飲酒運転と過度のドライバーの労働時間に対する法律、そのような行動を取り巻く社会規範の変化、道路交差点の設計の着実な改善などが含まれます。  
 これは、自動車がよりスマートに、より接続されるようになるにつれ進化する必要があります。  
 セクション25で説明しました。  
 支援技術には、さまざまなバグがありました。セクション23で、アダプティブクルーズコントロールの盲点について説明しました。  
1。  
 テスラなどの限られた自動運転機能を販売する企業は、公衆の信頼を損なうようになった事故を経験しました。  
2。  
 テスラの「オートパイロット」では、運転手に注意を払い、ハンドルを握ったままにして、制御を維持し、事故を回避する必要がありました。  
2020年でさえ、より優れた自動操縦システムは高速道路で車をほぼ無事に運転することができますが、小さな道路では不安定になり、ラウンドアバウトで混乱し、芝生の端を走ることができます。  
 次に、緊急ブレーキアシスト（EBA）を使用します。これにより、自分が思っている場合に完全なブレーキ力が適用されます。12このストーリーは、「自動車の安全のための闘い」[1235]で説明されています。  
4。  
 通常のアルゴリズムでは、300ms以内にアクセルからブレーキまで足を動かしてから2kg以上の力を加えると、できるだけ早く車が作動して停止します。  
 （私はかつて意図せずに鉱山を引き金にしたことがあり、ありがたいことに私の後ろに車の近くはありませんでした。  
 従来のロジックとディープニューラルネットワークに基づくマシンビジョンシステムの両方を使用する複雑な処理により、これまでの道のすべてを理解しようとしているため、これはさらに困難です。  
2、現在の製品は限られており、品質はさまざまです。  
しかし、それをどのようにテストする必要がありますか？そして、もし私たちが完全な自律性に移行したとしても、リスクと脅威の分析には、人類社会で発生する多くの悪いことを含まなければなりません。  
 実際の数字は物議を醸していますが。  
 テスラが主張したように、車両のオートステア機能がアクティブ化された後のエアバッグ展開の40％の減少ではなく、フルデータは0から57％の増加を示しました。21 [1565]。  
 AEBで懸念されていたのは、ウサギがその前を走っているときに車が急ブレーキをかけると、後面衝突が増える可能性があるということでした。  
 Tesla withAutopilotと同様の値のプラグインハイブリッドメルセデスを保証するのにどれくらいの費用がかかるかをオンラインで確認すると、同じ答えが得られます（ただし、より多くの保険会社がメルセデスに入札します）。  
 政治家はトラック運転手の仕事について心配し始めました。  
 マシンビジョンの進歩は非常に速いため、5年前のハードウェアでは現在実行されていないシステムであるため、5年ごとにまったく新しいビジョンを販売する必要があると想像できます。  
2020年までに、私たちはセクション27で述べたサイバーセキュリティに関するISO 21434規格ドラフトを含む、セキュリティ標準化の流れを手に入れました。  
5;接続されたvehi-13のサイバーセキュリティとソフトウェアの更新に対処するためのUNECE13の規制の修正案13欧州連合国連経済委員会は、1958年の条約によって設立されました。  
4。  
 それはすばらしいことですが、ターゲットは常に速く動いています。  
 20以上の機関が何らかの形で車両の安全性に関与しています（米国では、NHTSAが自動車の設計から制限速度まですべてをカバーしています）。  
 ecosys-temはどのように進化して対処する必要がありますか？フォルクスワーゲンが排出ガステストをだますために車にソフトウェアをインストールしたことが判明した2015年のディーゼルゲート排出ガススキャンダルの後、オシアルズは突然業界の安心感を信じる気を失いました。  
 脅威モデルはもはや外部のハッカーだけではなく、ベンダー自体も含まれていました。  
 彼らは何をする必要がありましたか？28。  
2安全とセキュリティ規制の近代化私たちのブリーフは、一般的にすべてのセクターにわたる政策問題を検討することでした。  
しかし、これは実際にはどういう意味ですか？これを解決するために、「エイリアンレバレット、リチャードクレイトナンドと私は、医療機器、自動車、配電という、私たちがある程度知っている3つの産業を研究しました。  
 完全なレポートには、ISO、IEC、NISTなどの組み込みデバイスの安全性/セキュリティ標準の既存のパッチワークの広範な分析が含まれています。  
 使いやすさはいくつかの点で重要です。  
 一部の国では、67歳以上のドライバーに医療従事者に運転テストを再受験してもらい、シートベルトとエアバッグを強く要求するよう求めています。  
 カーセキュリティは、テロリストがリモートで車を乗っ取り、歩行者に車を運転できるかどうかだけではありません。  
 どのようにしてヨーロッパとアフリカに加え、日本、韓国、オーストラリアの自動車製造国を組み込みますか。それは、自動車の3つの標準化ゾーンの1つであり、その他はアメリカと中国です。  
4。  
 自動車の安全がそうであったように、それは長くて困難なプロセスになるでしょう。  
どこから始めればよいのでしょうか？  
 最終的には、特に自動車のオートパイロットが致命的な衝突を引き起こしたときに責任をめぐる紛争がある場合は、事故の調査において自動車データの使用を規制する法律が必要になります。  
）データがなければ、学習システムを構築することはできません。  
 これは、技術標準ETSI EN 303 645 V2によって部分的に達成されるように設定されているように見えます。  
2。  
 ETSIは約800社の会員組織です。政府よりも迅速に移動できますが、依然として影響力があります。たとえば、携帯電話の標準化団体を設立しました。  
 そのためには、法の力を基準に与える必要があります。  
4。  
 欧州にはすでにEU政府機関間のセキュリティ侵害の報告を調整するEuropeanNetwork and Information Security Agency（ENISA）がありましたが、英国とフランスの諜報機関がロビー活動を行った結果、Creteから追放されました。 。  
2019年のサイバーセキュリティ法はこれを公式化した[655]。  
2。  
 ENISAが時間の経過とともにその能力と影響力を構築し、新しい安全基準がセキュリティにも適切な注意を払うことが期待されます。これには、少なくとも適切な開発ライフサイクルが含まれます（これは推奨事項の1つです）。  
 適切な人々はそれを信頼しなければならず、それは社会的および組織的プロセスに組み込まれる必要があります、セキュリティエンジニアリング942ロスアンダーソン28。  
 持続可能性は、より幅広いシステムとの整合性と、長期間にわたって安定した持続性を意味します。28。  
 セキュリティと安全性の脆弱性にパッチが適用されると、規制当局は移動するターゲットに対処する必要があります。  
 フォルクスワーゲンの大失敗からわかったように、多くのレガシーメーカーは協調的な開示に追いついていません。  
 では、デンマークの田舎で10年間過ごし、その後ルーマニアに輸出された25歳のランドローバーを、どうやって集めるのでしょうか。自動車業界はソフトウェアのパッチに対して6年以上の責任を負うことを望まなかったため、これは政治的な争いを引き起こしました。  
）ただし、新車の埋め込み炭素コスト（製造時に排出されるCO2の量）は、その生涯の燃料燃焼とほぼ同じです。  
 現在、廃車時の自動車の平均年齢は約15歳ですが、6歳に短縮すると、環境コストは許容できなくなります。  
ヨーロッパの機関で非常に準備の整った聴衆を見つけました。  
 修理する権利の活動家は、循環型経済で家電製品を再利用できるようにキャンペーンしており、「セキュリティ」メカニズムを使用して修理を防止したり、修理を違法にするためにそれらを悪用したりすることさえテック企業に嫌がらせをしていました。  
 消費者権利団体は、スマートデバイスの寿命が衝撃的に短いことを警告し始めていました。「スマート冷蔵庫」に余分な費用をかけて、ベンダーがサーバーの保守を停止した1年後、冷ややかなレンガになってしまったことを突き止めることができました[933]。  
 以前は電球が長持ちしました。生誕200年の光は1901年からリバモアで燃え続けています。  
 政府は押し戻しました。フランスは2015年に製品寿命を短くすることを違法にし、Appleが2017年に承認した後はセキュリティエンジニアリング943ロスアンダーソン28です。  
 ソフトウェアのアップデートを使用して古いiPhoneの速度を低下させ、ユーザーに新しいiPhoneを購入するよう促したという持続可能性が訴えられました。  
2B、反競争的慣行のため。ただし、これはフランスの販売業者の取り扱いにも関連している[1193]。  
）セキュリティ機関は、デフォルトのパスワードが設定されたネットワーク接続デバイスやパッチ適用できないソフトウェアなど、「Internetof Things」のリスクについてすでに警告を発していました。  
 デフォルトのパスワードがあり、ソフトウェアにパッチを適用できないXiaomi CCTVカメラを悪用していることがすぐにわかりました。  
その後の3年間で、Xiaomitoが脆弱性にパッチを適用する（またはパッチを適用できるようにする）ことで製品をサポートするなど、失敗したテクノロジー企業を押し戻すための法的手段を作成しようとする取り組みが複数ありました。  
28。  
1商品販売指令この指令は、2019年5月に欧州議会を通過し[656]、2021年から施行されます。  
 この表現は、商品自体のソフトウェア、商品が接続されているオンラインサービス、サービスを介してまたは直接商品と通信できるアプリを対象とするように設計されています。  
既存の規制では、自動車や洗濯機などの耐久財のベンダーがスペアを少なくとも10年間供給し続ける必要があるため、新しい規制体制が少なくとも同じくらい長く必要になることを期待できます。  
」多くの国では、自動車は使用を続けるために毎年の路上走行性テストに合格する必要があり、そのようなテストにはソフトウェアが予見可能な将来に最新のパッチが適用されているかどうかのチェックが含まれる可能性が高いことを考えると、セキュリティパッチの要件を拡張する必要があると考えられます。 10年以上。  
 アメリカの慣習はしばしばヨーロッパの安全問題を追っています。  
5。  
5。  
1960年代以降、ムーアの法則のおかげで、コンピューターをほぼ消耗品と見なすようになりました。  
私たちは、より精巧なパイプライン処理とキャッシングをサポートするために、数千個、さらには数百万個のトランジスタをチップに詰め込みました。  
 10年後のテクノロジーは今日のものとはまったく異なるものになると信じて、私たちはモノポリーを肩をすくめてきました。そのため、市場の競争を市場の競争に置き換えることができます。  
ムーアの法則は現在、使い果たされています。  
その後5％[882]。  
 これは、12ステージのCPUパイプラインによって引き起こされたSpectreのようなサイドチャネル攻撃から、当社のブロートウェアに蓄積された技術的負債を介して、すべてを駆り立てる独占的なビジネスエコシステムにまで及びます。  
 多くの人気のあるCAのルート証明書の有効期限が切れ始めています。これらが、ソフトウェアをアップグレードできないテレビなどのデバイスに組み込まれている場合、デバイスは本質的にブロックされています[117]。）CAルート証明書の有効期限が切れると、サーバーではなくクライアントを更新して修正する必要があります。  
6、SafariやChromeなどのブラウザは398日の証明書の有効期限を強制し始めており、これは頻繁な更新に対するもう1つの強力なインセンティブです。  
 システムの建物と土木工学のプロジェクトは、いくぶんハイブリッドです。一部のベンダーは、可能な限り安定して25年間維持されることが期待されるLinuxのバージョンに取り組んでいますが、他のベンダーは、システム全体のより積極的な定期的な更新を求めており、「すべてをクラウドに置く」ように要求しています。  
 複数の請負業者や下請業者が、変電所から空調設備、火や強盗まで、建物に関する完全なエンジニアリング情報を含むシステムへのオンラインアクセスを必要とすると、明らかなリスクがあります。  
 何百万もの利害関係者による行動の変化が必要となるため、新しい標準に適応するには何年もかかるでしょう。  
5。  
では、持続可能なセキュリティ研究はどのようなものでしょうか？最初のパイロットプロジェクトとして、Laurent Simon、David Chisnall、私は暗号化ソフトウェアのメンテナンスに取り組みました。  
4。  
 問題の1つは、OpenSSLなどの暗号実装に通常、暗号化操作を不定期に実行するように設計されたコードがあるため、使用中のキーが外部のオブザーバーに漏洩せず、キーマテリアルやその他の機密情報を含むメモリ位置をゼロ化することです。同じマシンの他のユーザーもキーを推測できないようにします。  
 それはそれらを離れて最適化し、突然何百万ものマシンのすべてが安全でない暗号ソフトウェアを持っています。  
 私たちのツールスミスは敵ではなく味方でなければならないため、これを適切に修正するために何が必要かを考え出しました。  
 コンパイラに一定時間のコードとsecureobjectの削除を適切に行わせることは、驚くほどトリッキーであることが判明しましたが、結局、LLVMのプラグインの形で機能の概念実証を行った[1758]。  
 低レベルのコンパイラー内部から中レベルの安全システムに移行すると、自動車業界が直面する大きな課題は、事故データをそこから学ぶことができる利害関係者に提供することです。  
 世界中で、年間100万回の死のようなものがあります。  
 ますます、データはベンダーのサーバーと破損した車両にあります。  
 緊密に争われた訴訟がある場合、データが要求される可能性がありますが、ベンダーはそれを共有することに消極的であり、通常は裁判所命令が必要です。  
 私たちは、Uberがアリゾナ州テンペのElaine Herzbergを殺害したときのように、自動運転車に殺されて人々が愚かな事故で殺されたという報告を聞き続けています。 ]。  
 では、パッチサイクルはどのようになるでしょうか。航空では、事故が監視され、パイロットや航空管制官などのオペレーターだけでなく、航空機の設計者や地上システムの設計者にもフィードバックが送られます。  
 そこでも、有害事象を監視し、データを収集するための必須システムが鍵となります。  
6。  
 自動車の自律性が高まるにつれ、自動車の学習システムも避けられませんが、それだけでは学習しません。  
手始めに、自動車が感知したもの、彼らが何をすることに決めたのか、そしてその理由からのきめの細かいデータが必要になります。  
 現在、EU加盟国は車両基準の市販後調査に責任を負っているので、実施されることはほとんどなく、Dieselgateに続いて欧州委員会に監視権限を与える提案が出されています。  
 安全性、プライバシー、管轄権に関する複数の対立する権利に対処する必要があるため、それらは大きく複雑になります。  
 テクノロジーが急速に変化している間、私たちはおそらくプライバシーと競争に対するさまざまな害を容認することができました。  
 Google+はあまりにも不格好でしたか？とにかく、FacebookやTwitterを試してみてください。  
 また、テクノロジーによって一部のプレーヤーが市場での優位性を固定できるようになった分野は他にもたくさんあります。 2020年に書いているように、Amazonは世界で最も価値のある会社です。  
 これが起こっている兆候がいくつかあります[1044]。  
6まとめ昔、セキュリティエンジニアリングプロジェクトの大きな問題は、いつ完了したかを知る方法でした。今、世界は異なっています。  
セキュリティの評価と保証のスキームは、多くの異なる生態系で育ちました。  
 安全認証スキームは、ヘルスケア、航空宇宙、道路車両など、さまざまな業界で個別に進化しました。  
 これで、すべてがconnec-Security Engineering947Ross Anderson28を取得しています。  
 要約すると、セキュリティなくして安全性を確保することはできません。これらのエコシステムは融合しています。  
 これは、ソフトウェアライフサイクルの標準を超えて、新しいハザードや攻撃から迅速に回復できる学習システムの目標に向かって進みます。  
 20世紀に戻って、多くのベンダーは情報セキュリティの権利を決して忘れませんでした。  
 将来的には、製品が故障したときに合理的に迅速に製品を修正し、妥当な期間、製品を修理することが誰もが期待されます。  
 テクノロジーによって私たちに与えられた安全とセキュリティのコストは、最も広い意味で、主権の国家的思想、そしてより実際的なレベルでは、個人の行動または市場の力では達成できない目標を集合的に達成することによって達成する人々の能力と緊張が高まるでしょう。  
研究上の問題持続可能なセキュリティの大きな課題に加えて、セクション28で説明します。  
上記の2には、保証に関して他にも多くの未解決の問題があります。  
 2つ目の問題の束は、いくつかの銀河がゆっくりと融合しているように、安全とセキュリティの世界がゆっくりと融合しているため、セーフティエンジニアとセキュリティエンジニアがお互いの言語を話せないことから、一連の標準と、互換性のない標準化へのアプローチ。  
もう1つの大きな機会は、軽量のメカニズムが実際に配備されたシステムを改善することです。  
’私たちには、証明可能なセキュリティ、正式な方法、および規模が拡大されていないために実際には発見されていないあいまいな攻撃についての論文を執筆している大規模な学術コミュニティがあります。  
プログラマーがstackexchangeから可能な限り多くのコードを盗もうとしている場合、バッファーオーバーフローを取り除くためにそこにある例をクリーンアップするために、公共の利益が必要ですか？また、暗号ライブラリやデバイス権限などのツールのセキュリティユーザビリティ標準を設定して、（たとえば）デフォルトでECBになっているライブラリを、MD5やSHA1と同じように強制的に廃止する可能性はありますか？展開前と継続的な評価の両方のためのAI / MLシステムの。  
6。  
 論争の的となる社会問題に触れると、学習システムはどのようになりますか？すべての生命が等しく評価されていない世界で、継続的な安全をどのように行うのですか？企業がとるセキュリティ、プライバシー、安全工学の決定が公の精査と法的課題に開かれていることをどのように保証するのでしょうか？さらに読むセキュリティと安全の保証ビジネスの促進に専念する業界全体が、あなたの税金の山々に支えられています。  
 残念ながら、異端を書くのに十分な人はどこにもいません。