– IMMANUEL KANT世界は、オンラインでもオフラインでも完璧になることはありません。 solet’sはオンラインに対して信じられないほど高い基準を設定していません。  
1はじめにセキュリティエンジニアリングとは、悪意、エラー、または不測の事態に直面しても信頼できるシステムを構築することです。  
セキュリティエンジニアリングには、暗号技術やコンピュータセキュリティからハードウェアの改ざん防止、経済学、応用心理学、組織、法律の知識に至るまで、分野横断的な専門知識が必要です。  
 セキュリティエンジニアも、チェスプレーヤーと同じように、敵対的思考のスキルが必要です。あなたは、それらの開口部からそれらの開発を通して結果まで、過去に働いた多くの攻撃を研究する必要があります。  
 それらの失敗は、人命と環境を危険にさらす可能性があり（原子力安全および制御システムと同様）、主要な経済インフラ（現金自動支払機およびオンライン決済システム）に深刻な損害を与え、個人のプライバシーを危険にさらす（医療記録システム）、実行可能性を損なう全事業部門（前払いユーティリティメーター）の、そして犯罪（泥棒​​と車の警報）を容易にします。  
2。  
 システムが実際よりも脆弱であるか信頼性が低いという認識でさえ、現実的なコストがかかる可能性があります。  
 現実ははるかに複雑です。  
 通常、ユーザー認証、トランザクションの整合性と説明責任、フォールトトレランス、メッセージの機密性、および秘密性のいくつかの組み合わせが必要です。  
したがって、保護を正しく行うには、いくつかの異なるタイプのプロセスに依存します。  
 また、システムを監視して維持する人々が適切に動機付けられていることを確認する必要もあります。  
次に、セキュリティシステムと安全システムが行う必要のあるさまざまなことを説明するために、銀行、軍事基地、病院、および住宅という4つのアプリケーション領域について簡単に説明します。  
1。  
ポリシーがあります：あなたが達成することになっているもの。  
 保証があります。特定のメカニズムにどれだけの信頼を置くことができるか、そしてそれらがどれだけうまく連携するかです。  
 これらすべてが相互作用します（図1を参照）。  
例として、9/11のテロ攻撃について考えてみましょう。  
 ポリシーが迅速に変更されました。最初にすべてのナイフを禁止し、次にほとんどの武器を禁止しました（現在、野球のバットは禁止されていますが、ウイスキーのボトルは許可されています）。それは多くの細部で揺れ動く（ブタンライターは禁止され、再び許可される）。  
 保証は常に不十分です。多くの無害な乗客の所有物が毎月ゴミ箱に預けられていますが、（偶然に、またはテストの目的で）スクリーニングを通して取り出された実際の武器の半分未満が発見され、没収されています。  
 たとえば、TSAは乗客のスクリーニングに数十億ドルを費やしており、これはかなり効果的ですが、コックピットのドアの強化に1億ドルを費やしたことで、ほとんどのリスクが排除されました[1523]。  
3。  
 ほとんどの旅客機にはドアロックがないので、悪人が飛行機に向かって階段を上って爆弾ボードを配置するのを止めることはあまりありません。彼が操縦技術と少しのchutzpahを持っていたなら、彼は飛行計画を提出し、それで成功することができた[1202]。  
なぜそのような政策の選択がなされるのでしょうか？簡単に言うと、意思決定者へのインセンティブは、効果的なものよりも目に見える制御を支持します。  
 ほとんどのプレーヤーはまた、テロの脅威を宣伝するインセンティブを持っています：政治家は「投票をおろそかにする」（大統領のオバマが言ったように）、ジャーナリストはより多くの論文を販売し、企業はより多くの機器を販売し、政府は構築する彼らの帝国、そしてセキュリティ学者が入学者に。  
 幸いなことに、有権者はこの過ごす時間を予測しており、現在– 9/11から19年後–無駄になっているお金が減っています。  
 それはイギリスのリスク登録のトップでしたが、テロリズムは政治的によりセクシーでした。  
セキュリティエンジニアはこのすべてを理解する必要があります。リスクと脅威を背景に置き、何が問題かを現実的に評価し、クライアントに適切なアドバイスを提供できる必要があります。  
 歴史はまた、それが複雑さをもたらし、複雑さが多くの失敗を引き起こすため、重要です。  
そのため、この本はケースヒストリーでいっぱいです。  
1。  
1。  
 これにより、顧客のアカウントマスターファイルと、着信および発信トランザクションを記録する多数のジャーナルが保持されます。  
 伝統的な防御は、何世紀にもわたって発展してきた簿記手続きから来ています。さらに、大規模な転送には通常、2つのセキュリティエンジニアリング24Ross Anderson1が必要です。  
 例1 –BANKPolicyIncentivesMechanismAssurance66--⇢⇢⇢⇢⇢⇢⇢⇢> ZZZZZZZZ〜??��ZZZZZZZZ}⇢⇢⇢⇢⇢⇢⇢⇢=図1。  
 異常な取引量や取引のパターンを探すアラームもあり、銀行のシステムにアクセスせずに定期的に休暇を取る必要があります。  
 公共の顔の1つは銀行の現金自動預け払い機です。  
 現金自動預け払い機は、暗号化の最初の大規模な商用利用であり、多くの暗号規格の確立に役立ちました。  
3。  
 現在、ほとんどの顧客は、支店ではなくオンラインで、手形の支払いや、普通預金と当座預金の間の送金などの日常業務を行っています。  
1990年代に設計された標準のセキュリティメカニズムは、犯罪者が銀行ではなく顧客への攻撃を開始すると効果がなくなることが判明したため、多くの銀行が認証コードを含むテキストメッセージを送信します。  
 この武装競争は、認証、ユーザビリティ、心理学、運用、および経済学の要素を混合する多くの魅力的なセキュリティエンジニアリングの問題を引き起こします。  
 舞台裏には、銀行間で高額を移動するために使用される高価値のメッセージングシステムがあります。証券を取引すること。信用状およびセキュリティエンジニアリング25ロスアンダーソンの発行1。  
 例2 –軍事基地の保証。等々。  
 防御は、簿記管理、アクセス制御、および暗号化の混合です。  
 銀行の支店は、大きくて堅固で繁栄しているように見えるかもしれません。  
 銃を持って中に入った場合、窓口係はあなたが見ることができるすべての現金をあなたに与えます。夜間に侵入した場合は、砥石車で数分で金庫に切り込むことができます。  
 暗号化は、強盗が通信を操作して、アラームが「問題ない」のときに「問題がない」と表示させるために使用されます。  
 銀行のコンピュータセキュリティは重要です。2000年代初頭まで、銀行は多くのコンピュータセキュリティ製品の主要な民間市場であったため、セキュリティ標準に大きな影響を与えていました。  
4例2 –軍事基地軍事システムは、20世紀におけるもう1つの技術的推進要因でした。政府が1980年代初頭以降、コンピューターセキュリティに資金を提供していた学術研究の多くを動機付けたためです。  
1。  
 しかし、メッセージを暗号化するだけでは十分でないことがよくあります。誰か他の人の鍵で暗号化されたトラフィックを見る敵は、送信機を見つけて攻撃するだけです。  
2。  
敵のレーダーを妨害するのを防ぎながら敵のレーダーを妨害しようとする軍拡競争は、他の場所にはまだ見られない、巧妙で繊細で幅広い戦略を駆使して、多くの巧妙な詐欺、策、および対策をもたらしました。  
3。  
 これらは通常「トップシークレット」のラベルが付けられ、別のシステムで処理されます。それらはコンパートメントでさらに制限される可能性があるため、最も機密性の高い情報はほんの一握りの人々にしか知られません。  
 複数のセキュリティエンジニアリングの管理26ロスアンダーソン1。  
 例3 –情報フローの制限があるHOSPITALシステムは困難な問題であり、軍事セキュリティの自動化に費やされたビリオンは、携帯電話やラップトップに現在備わっているアクセス制御技術の開発に役立ちました。  
 核兵器の保護の問題は、証明可能な安全な認証システムから、光ファイバーアラームセンサーまで、バイオメトリクスを使用して人々を特定する方法に至るまで、多くのクールなセキュリティ技術の発明につながりました。  
 たとえば、軍隊は最近まで、数十年間維持しなければならないソフトウェアシステムの数少ない顧客の1つでした。  
 2019年に欧州連合は、デジタルコンポーネントを使用して商品を販売する場合、それらのコンポーネントを2年間、またはそれが顧客の妥当な期待である場合はそれ以上維持する必要があるという法律を通過しました。  
 どのツールを使用する必要がありますか？1。  
 病院には多くの興味深い保護要件があり、主に患者の安全とプライバシーに関係しています。安全の使いやすさは医療機器にとって重要であり、決して解決された問題ではありません。  
 最大の単一の問題は、患者に薬剤を点滴するために使用される輸液ポンプにあります。典型的な病院では、半ダースのメーカーがあり、すべてが多少異なる制御を行っているため、致命的なエラーが発生する可能性が高くなります。  
 したがって、ますます多くの医療機器がソフトウェアではなく無線通信を取得するようになると、セキュリティ感度がより良い安全性につながる可能性があります。  
 患者記録システムは、すべての患者にすべての患者の記録を表示させないようにする必要があります。そうしないと、プライバシー違反が予想されます。  
つまり、システムは「看護師は過去90日間のいつでも自分の部門でケアされた患者の記録を見ることができる」などのルールを実装する必要があります。  
6。  
 （米国のHIPAA法はコンプライアンスの基準をより簡単に設定していますが、それでも情報セキュリティ投資の原動力です。  
 患者の記録は、研究で使用するために匿名化されることがよくありますが、これを行うのは困難です。  
 どのデータを効果的に匿名化できるかを理解することは困難であり、社会的および文脈的なデータがますます多くなるにつれて、それはまた、遠く離れた親族の遺伝的データは言うまでもなく、移動する目標でもあります。  
 新しいテクノロジーは、よく理解されていないリスクをもたらす可能性があります。  
 しかし、2017年5月にイギリスのいくつかの病院でWannacryマルウェアに感染したマシンがあった後、彼らはネットワークを閉鎖して感染を制限し、X線はX線から移動しなくなったため、事故と救急部門を閉鎖する必要があることに気付きました。封筒を操作する劇場への機械、しかし遠い町のサーバーを介して。  
 スタンバイジェネレータはありましたが、スタンバイネットワークはありませんでした。  
 コロナウイルスのパンデミック付属品制御によって表面化された問題：一部の医療機器は、プリンターがインクカートリッジを認証するのと同じように、スペアパーツを認証します。  
しかし、それは脆弱性をもたらします。サプライチェーンが中断されると、物事を修正するのが非常に難しくなります。  
これはバンキングITや軍事システムよりも若い分野ですが、ヘルスケアはすべての先進国でGNPのどちらよりも大きな割合を占めているため、その重要性が高まっています。  
1。  
 しかし、停止して考えてください。  
 おそらく、すでに説明したシステムのいくつかを使用しています。  
 糖尿病の場合、インスリンポンプがベッドサイドのドッキングステーションと通信することがあります。  
6。  
2。  
 それが2015年より前に作成された場合、キーのボタンを押すと、車のロックが解除され、暗号化されたロック解除コマンドが送信されます。  
 しかし、ボタンを押す必要がないため、鍵を玄関の近くに置いたままにすると、泥棒が無線リレーを使って車を盗む可能性があります。  
3。  
 そして、上で述べたように、多くの電話会社は、自分の電話が盗まれたと主張する人々にnewSIMカードを売ることについてリラックスしています。だから詐欺師はあなたの電話番号を盗み、これを使ってあなたの銀行口座を襲撃します。  
 100か国以上で、世帯は、ATMまたはオンラインサービスから購入した20桁のコードを使用して、電気とガスの前払いメーターを入手できます。  
5。  
これは多くの点で変化しています。  
 音声とジェスチャーのインターフェースが一般的になるにつれて、他のすべてのガジェットにマイクとカメラが搭載され、音声処理は通常、クラウドで行われるため、バッテリーの寿命を節約できます。  
 （米国とヨーロッパは、プライバシー法がこれをどのように扱うべきかについて異なる意見を持っています。  
今後数年間で、このようなシステムの数は急速に増加します。  
 たとえば、2019年、ヨーロッパはベンダーのクラウドサービスへの暗号化されていない通信を使用する子供用時計を禁止しました。盗聴者は子供の位置情報の履歴をダウンロードし、世界中のあらゆる番号に時計をかけることができます。  
この本は、あなたがそのような結果を避けるのを助けることを目指しています。  
セキュリティエンジニアリング29ロスアンダーソン1。  
 定義土木技術者は、立ち上がった数百の橋よりも、落ちる1つの橋からはるかに多くを学びます。セキュリティエンジニアリングでもまったく同じことが言えます。  
7定義セキュリティエンジニアリングで使用される用語の多くは単純明快ですが、いくつかは誤解を招く、または議論の余地さえあります。  
 このセクションでは、主な問題がどこにあるかを指摘します。実際には、これは以下を示すことができます：1。  
 上記の1つ以上、およびオペレーティングシステム、通信、その他のインフラストラクチャ3。  
 上記のいずれかまたはすべて、およびITステータス5。  
 上記の一部またはすべてに加えて、顧客およびその他の外部ユーザー。  
 大まかに言って、ベンダーと評価者のコミュニティは最初のものと（場合によっては）2番目のものに焦点を当て、ビジネスは6番目（場合によっては5番目）に焦点を当てます。  
人間のコンポーネントを無視してユーザビリティの問題を無視することは、セキュリティ障害の最大の原因の1つです。  
次の一連の問題は、プレーヤーが誰であり、何を証明しようとしているのかが明確でないことから生じます。  
 したがって、「Aliceがボブに自分を認証する」などのステートメントがたくさんあります。  
 アリスが自分の名前が実際にはアリスであることをボブに証明したということですか、それとも彼女が特定の資格情報を持っていることを証明したということですか？認証は、アリス（人間）によって、またはアリスのエージェントとして機能するスマートカードまたはソフトウェアツールによって行われたということですか？その場合、それはセキュリティエンジニアリング30ロスアンダーソン1です。  
 定義SAlice、およびおそらくAliceが彼女のカードを貸したキャロル、電話を盗んだDavid、または彼女のラップトップをハッキングしたEveではありませんか？  
プリンシパルは、セキュリティシステムに参加するエンティティです。  
 プリンシパルは、通信チャネルにもなります（状況に応じて、ポート番号または暗号鍵になる場合があります）。  
グループと役割は同じではないことに注意してください。  
 プリンシパルは、複数の抽象化レベルで考慮される場合があります。  
 「ボブがアリスの不在で行動する」とは、「ボブの不在時にアリスの行動をしているボブを表すスマートカード」または「ボブが不在でアリスのスマートカードを操作している」ことを意味する場合があります。  
アイデンティティという言葉の意味は議論の余地があります。  
 たとえば、「ボブのマネージャーとして行動するアリス」のボブは、「チャーリーのマネージャーとして行動するボブ」や「デイビッドと共同で銀行為替手形に署名する支店長のボブ」におけるボブと同じであることを知ることが重要かもしれません。  
信頼と信頼できるという定義はしばしば混乱します。  
 私はNSAの定義を使用します。信頼できるシステムまたはコンポーネントは失敗してもセキュリティポリシーを破る可能性があるものであり、信頼できるシステムまたはコンポーネントは失敗しないものです。  
企業の世界では、信頼されたシステムは、「時計にハッキングされても私に発砲されないシステム」または「私たちが保証できるシステム」である可能性があります。  
機密性とプライバシーと機密性の定義により、別のワームが開かれます。  
 私の隣人が私たちの共通のフェンスでツタを切り倒し、その結果、彼の子供が私の庭を覗き込んで私の犬をいじめる可能性がある場合、それは私の機密性ではありませんでした。  
 会社を投獄することはできませんが、罰することはできます。  
7。  
 かつての雇用主の態度について沈黙を守る義務は、プライバシーではなく、信頼を守る義務です。  
•機密性とは、暗号化やコンピュータアクセスコントロールなどの情報にアクセスできるプリンシパルの数を制限するために使用されるメカニズムの影響を指す工学用語です。  
•プライバシーとは、個人情報を保護する能力および/または権利であり、個人の空間への侵入を防止する能力および/または権利にまで及びます（正確な定義は国によって異なります）。  
たとえば、入院患者にはプライバシーの権利があり、この権利を維持するために、医師、看護師、およびその他の職員は患者に対して信頼する義務があります。  
通常、プライバシーは個人の利益のための秘密であり、機密性は組織の利益のための秘密です。  
 たとえば、多くの国には性感染症の治療を秘密にする法律がありますが、私立の眼科医が性感染症クリニックと暗号化されたメッセージを交換しているのを観察できれば、彼はそこで治療されていると推測するかもしれません。  
 したがって、匿名性は、機密性と同様にプライバシー（または機密性）の重要な要素となる可能性があります。  
 自分で匿名であることは難しい。通常は隠れるために群衆が必要です。（そして、それはしばしばより便利です。  
 セキュリティプロトコルに関するアカデミック文献では、真正性は完全性と新しさを意味します。つまり、以前のメッセージの再生ではなく、本物のプリンシパルと話していることを証明しています。  
 小切手は6か月後に無効になると地方銀行法に定められている場合、7か月前の現金化されていない小切手は整合性があります（変更されていない場合）。ただし、有効ではありません。  
 たとえば、警察の犯罪現場では、証拠バッグに入れて偽造小切手の完全性を維持します。  
）セキュリティエンジニアリング32ロスアンダーソン1。  
 定義私たちが望まないものは、しばしばハッキングと表現されます。  
 たとえば、税務弁護士は、税コードを調査して、税回避の戦略に発展する抜け穴を見つけます。まったく同じ方法で、ブラックハットは、ソフトウェアコードを研究して、彼らがエクスプロイトに発展する抜け穴を見つけます。  
 それらは複数のレイヤーで発生する可能性があります。弁護士は税コードをハッキングしたり、スタックを上に移動して議会やメディアをハッキングしたりできます。  
この本には多くの例が含まれています。  
ハッキングが一般的になった場合、ルールを変更して阻止することができます。しかし、正規化されることもあります（例としては、ライブラリからフィブリスタ、検索エンジン、ソーシャルメディアまでさまざまです）。  
 脆弱性は、システムまたはその環境のプロパティであり、内部または外部の脅威と組み合わせて、システムのセキュリティポリシーの違反であるセキュリティ障害を引き起こす可能性があります。  
セキュリティターゲットは、セキュリティポリシーを特定の製品に実装する方法（暗号化とデジタル署名のメカニズム、アクセス制御、監査ログなど）を規定する、より詳細な仕様であり、エンジニアがかどうかを評価するための基準として使用されます適切な仕事をした。  
 パート3では、セキュリティポリシー、セキュリティターゲット、保護プロファイルについて詳しく説明します。  
これは、安全性が重要なシステムに使用する用語を幾分反映しており、今後ますます多くのアプリケーションでセキュリティと安全性を一緒に設計する必要があるので、2つを並べて考えることは有用です。  
 危険は、ハザードが事故につながる確率であり、リスクは、事故の全体的な確率です。  
 不確実性とは、リスクを定量化できない場合であり、安全性は事故から解放されます。  
8。  
1。  
 企業にとって、それはすべての従業員の電子メールとWebブラウジングを監視する能力を意味するかもしれません。従業員にとって、監視されずに電子メールとWebを使用できることは意味があるかもしれません。  
ハンプティ・ダンプティは、ルイス・キャロルからの一節を思い出します。「言葉を使うとき」とハンプティダンプティは、かなり軽蔑して言いました。  
「問題は、です」とHumptyDumptyは言いました、「それはマスターになることです-それだけです。  
 これは、何かを回避したいクライアントには不便な場合がありますが、一般に、堅牢なセキュリティ設計では、保護の目標を明示的にする必要があります。