エンジニアリング？  
– 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決してありません。ですから、オンラインに信じられないほど高い基準を設定しないでください。  
  
1.1はじめに  
専門分野として、完全なシステムを設計、実装、およびテストし、既存のシステムを環境の変化に合わせて適応させるために必要なツール、プロセス、および方法に焦点を当てています。  
ビジネスプロセス分析からソフトウェアエンジニアリング、評価、テストまでのシステムエンジニアリングスキルも重要です。しかし、それらは悪意ではなくエラーとミスシャンクのみを扱うため、十分ではありません。  
多くのシステムには重要な保証要件があります。  
、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る  
、全事業部門の実行可能性を損なう（前払いユーティリティメーター）  
。  
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、実際の社会的コストを伴う可能性があります。  
、セキュリティは彼らが守らないことを保証することです（「中国政府はこのファイルを読むことができません」）  
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、システムを守って維持する人々が適切に動機付けられるように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実行する必要が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。  
  
本当に信頼できるシステムを構築するには、4つを組み合わせる必要があります。  
メカニズムがあります。暗号化、アクセス制御、ハードウェア改ざん防止、およびポリシーの実装に使用するその他の機構です。  
最後に、インセンティブがあります。システムを監視および維持している人々が適切に仕事をしなければならない動機、および攻撃者がポリシーを破ろうとする動機です。  
。  
ハイジャック犯が空港のセキュリティでナイフを手に入れることに成功したのは、メカニズムの失敗ではなく、ポリシーの失敗でした。ふるいは銃と爆薬を締め出す仕事をしましたが、当時、刃が3インチまでのナイフは許可されていました。  
;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、その後再び許可される）  
複合ナイフや爆発物など、窒素を含まないため、メカニズムは弱いです。  
 発見され、没収された。  
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、これはかなり効果がありませんが、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]。  
例1 –銀行ほとんどの地上スタッフはスクリーニングを受けておらず、地上に駐機している航空機を一晩警戒するようにほとんど注意が払われていません。  
しかし、スクリーニングスタッフと護衛機は優先事項ではありません。  
 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コントロールを支持します。  
ほとんどのプレーヤーはまた、テロからの脅威を扇動するインセンティブを持っています：政治家は「投票を疑う」（オバマ大統領が言ったように）  
結局のところ、テロリストによる民主主義国家への被害のほとんどは過剰反応によるものである。  
もちろん、私たちは社会のレジリエンス予算のはるかに多くがパンデミック疾患への準備に費やされるべきだったことをちょうど知りました。  
優先順位をより合理的に管理した国は、はるかに良い結果を得ました。  
それは、さまざまなシステムで時間の経過に伴って何がうまくいかなかったかについての幅広い理解に依存しています。どのような攻撃が行われたか、どのような結果をもたらしたか、どのように阻止されたか（そうする価値があった場合）  
歴史もまた重要です。複雑さが原因であり、複雑さは多くの失敗を引き起こします。  
ですから、この本はケースヒストリーでいっぱいです。  
  
銀行は多くのセキュリティクリティカルなコンピューターシステムを運営しています。  
銀行の業務は、中核的な簿記システムに依存しています。  
ここでの主な脅威は銀行自身のスタッフです。銀行支店のスタッフの約1％が毎年解雇されており、そのほとんどは小さな不正行為です（平均的な盗難は数千ドルにすぎません）。伝統的な防御策は、何世紀にもわたって進化してきた簿記手続きからきています。  
さらに、大規模な転送には通常2つの1.3が必要です。  
 ？  
異常な取引の量やパターンを探すアラームもあり、スタッフは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。  
 システムの抜け穴を見つけて悪用しました。  
ATM向けに開発されたメカニズムは、カード決済が現金に取って代わる店舗のPOS端末にまで拡張されました。また、前払いユーティリティメーターなどの他のアプリケーションにも適合しています。  
もう1つの一般的な顔は、銀行のウェブサイトと携帯電話アプリです。  
銀行のWebサイトは、2005年以降、フィッシング（顧客が偽のWebサイトにパスワードを入力するように求められる）からの攻撃を受けています。  
詐欺師の反応は、電話ショップに行って、あなたのふりをして、あなたの電話番号を盗む新しい電話を購入することです。  
4。  
例2 –軍事基地の保証。等々。  
防御は、簿記管理、アクセス管理、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。  
コンピュータセキュリティの銀行取引は重要です。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した。そのため、銀行はセキュリティ標準に大きな影響を与えました。  
1.4例2 –軍事基地  
バンキングと同様に、アプリケーションは1つではなく多数あります。  
軍事通信は暗号の発展を促し、古代エジプトとメソポタミアにさかのぼります。  
低傍受確率（LPI）  
2。  
敵が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武装競争は、他の場所ではまだ発見されていない深さ、微妙さ、および戦略の範囲を備えた、多くの高度な詐欺、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。  
複数の管理1.5。  
4。  
セキュリティエンジニアは、これからも多くのことを学ぶことができます。  
ソフトウェアとインターネット接続が自動車などの安全が重要な消費財への道を見つけている今、ソフトウェアの持続可能性はより広い関心事になりつつあります。  
7年間販売される自動車または冷蔵庫用のソフトウェアを作成している場合、ほぼ20年間それを維持する必要があります。  
   
銀行家や兵士から医療に移ります。  
1。  
安全性のユーザビリティの障害は、道路交通事故と同じくらい多くの人々を殺すと推定されています-たとえば、米国では年間数万人、英国では数千人。  
安全性のユーザビリティはセキュリティと相互作用します。ハッキング可能であることが判明した安全でないデバイスは、敵対的な行動が可能になると、リスクに対する国民の食欲が大幅に低下することを規制当局が知っているため、製品のリコールが注文される可能性が高くなります。  
2。  
実際、この本の第2版以降、ヨーロッパの裁判所は患者が自分の健康情報を自分の治療に関与する臨床スタッフに制限する権利を持っていると判決を下しています。  
これは1.6にすることができます。  
（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す。また、近親者や遠方の親族の遺伝的データは言うまでもなく、ますます社会的および文脈的なデータを取得するので、それは移動するターゲットでもあります。  
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月に英国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、その後、X線がX線装置を封筒に入れて手術室に送るが、遠くの町にあるサーバーを経由する。  
スタンバイジェネレーターはありましたが、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によって浮上した問題は、アクセサリの制御です。一部の医療機器は、プリンタ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。  
 詳細は後ほど。  
また、報告が義務付けられている国では、プライバシー侵害の最大の原因でもあります。  
1.6例4 –家  
しかし、ただ立ち止まって考えてください。  
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。  
例4 – HOMEは、何かが起こったときに近所を目覚めさせるのではなく、数分ごとにセキュリティ会社への「すべての健康」信号を暗号化しました。  
あなたの車はおそらく電子イモビライザーを持っています。  
それがより最近のモデルであり、ボタンを押す必要はなく、キーをポケットに入れているだけの場合、車はキーに暗号化されたチャレンジを送信し、正しい応答を待ちます。  
このテクノロジーが導入されて以来、車の盗難は急増しています。  
携帯電話は、車のドアロックやイモビライザーで使用されているものと同様の暗号化チャレンジ/レスポンスプロトコルによってネットワークに認証されますが、警察は偽の基地局（ヨーロッパではIMSIキャッチャー、アメリカではスティングレイ）  
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新しいSIMカードを販売することについてリラックスしています。そのため、詐欺師があなたの電話番号を盗み、これを使用して銀行口座を襲撃する可能性があります。  
100か国以上の世帯は、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購入できます。  
5。  
これは多くの点で変化しています。  
音声や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、他のあらゆる種類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、バッテリー寿命を節約するためにクラウドで行われます。  
（米国とヨーロッパでは、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かなり異なる見解を持っています。）  
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年にヨーロッパは、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て、世界中のあらゆる番号に時計に電話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。  
土木技術者は、倒れている1つの橋から、とどまっている100の橋よりも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。  
1.7定義  
関連する章には、専門用語のより詳細な定義があり、索引を使用して見つけることができます。  
最初に明確にする必要があるのは、システムとは何を意味するかです。  
暗号化プロトコル、スマートカード、電話のハードウェア、ラップトップ、サーバーなどの製品またはコンポーネント。 2。  
上記に加えて、1つ以上のアプリケーション（バンキングアプリ、ヘルスアプリ、メディアプレーヤー、ブラウザ、アカウント/給与パッケージなど–クライアントとクラウドコンポーネントの両方を含む）  
上記の一部またはすべてとITスタッフ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。  
大まかに言えば、ベンダーと評価者のコミュニティは、最初と（時折）に焦点を当てています  
。  
人間のコンポーネントを無視すること、したがっ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。  
 連続する頭文字–ハリケーンによく似ていますが、性別を交互に使用する点が異なります。これにより、より読みやすくなりますが、精度が犠牲になる可能性があります。  
 認証は人間のアリス、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るということですか？  
 対象とは、オペレーター、校長、または犠牲者の役割を含む、あらゆる役割の身体的な人を意味します。  
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）。  
プリンシパルは、他のプリンシパルの複合にすることもできます。例はグループ（アリスまたはボブ）  
、複合的な役割（アリスはボブのマネージャーとして行動）  
。  
グループとは、一連のプリンシパルを意味しますが、役割は、さまざまな人物が連続して引き受ける一連の機能です（たとえば、「USSニミッツの時計の将校」や「当面のアイスランドの大統領」など。医師会 '）  
プリンシパルは、複数の抽象化レベルで検討される場合があります。  
詳細を検討する必要がある場合は、より具体的に説明します。  
注意が必要な場合は、2人の校長が同じ人物または装置を参照していることを示す2つの校長の名前の間の対応を意味するために使用します。  
多くの場合、アイデンティティは「名前」、つまり「ユーザーのアイデンティティ」や「市民のアイデンティティカード」などのフレーズによって定着した虐待を意味するために乱用されます。  
次の例は、違いを示しています。NSAの従業員がボルチモアワシントン国際空港のトイレの屋台で中国の外交官に主要な資料を販売しているのが観察された場合（彼の操作が許可されていなかった場合）  
私はNSAの定義を使用しています。信頼できるシステムまたはコンポーネントは、失敗するとセキュリティポリシーが破られる可能性があるのに対し、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、信頼できるシステムは、「時計にハッキングされても私に発砲されないシステム」、あるいは「私たちが保証できるシステム」かもしれません。  
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、彼の子供たちが私の庭を見て犬をいじめる可能性がある場合、これまでの機密性ではありません。1周りのルールを開発し始めなければならないときに、企業に関する法律が役立つかもしれません。 AI。  
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。  
そして、元雇用主の事件について静かに保つ義務は、プライバシーではなく信頼の義務です。  
•機密性とは、暗号化やコンピュータアクセス制御など、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効果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、個人のスペース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）。  
プライバシーは家族にまで及ぶ場合がありますが、企業などの法人には及ばない可能性があります。  
病院には、その商取引に関してプライバシーの権利はありませんが、それらに関与している従業員には、信頼の義務があります（不正行為を公開する内部告発の権利を行使しない限り）。  
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、私立の目で性感染症クリニックとの暗号化されたメッセージの交換を観察できれば、彼はそこで治療されていたと推測するかもしれません。  
したがって、匿名性はプライバシー（または機密性）の要素と同じくらい重要になる可能性があります  
しかし、匿名性は難しいです。  
また、私たちの法的コードは匿名性をサポートするように設計されていません。実際の盗聴を行うよりも、警察が電話会社から項目化された請求情報を入手するほうがはるかに簡単です。  
 信頼性と整合性の意味も微妙に異なる場合があります。  
銀行のプロトコルにも同様の考え方があります。  
 しかし、もはや有効ではありません。  
たとえば、警察の犯罪現場の担当者は、証拠の袋に入れて、偽造小切手の完全性を維持します。私たちが望まないことは、しばしばハッキングと表現されます。  
たとえば、税務弁護士は税法を調査して、税回避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、彼らが悪用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。ただし、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）。  
ここで明確にする最後の事項は、私たちが達成しようとしていることを説明する用語です。  
セキュリティポリシーとは、システムの保護戦略の簡潔な説明を意味します（たとえば、「各トランザクションでは、クレジットとデビットの合計は等しく、$ 1,000,000を超えるすべてのトランザクションは2人のマネージャーによって承認される必要があります」）。  
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、その基準として使用されます。エンジニアが適切な作業を行ったかどうかを評価します。  
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、これまで以上に多くのアプリケーションでセキュリティと安全性を組み合わせて設計する必要があるため、2つを並べて考えることは有用です。  
危険は、危険が事故につながる可能性であり、リスクは、事故の全体的な確率です。  
不確実性はリスクを定量化できない場所であり、安全性は事故から解放されます。  
;次のレベルでは、航空機、航空機エンジン、さらには航空機エンジンの制御ソフトウェアなどの特定のコンポーネントに対して作成する必要がある安全事例を見つけるかもしれません。  
1.8まとめ  
企業にとって、それはすべての従業員の電子メールとWeb閲覧を監視する機能を意味するかもしれません。従業員にとって、監視されなくても電子メールとWebを使用できることを意味する場合があります。  
ルイス・キャロルからの一節を思い出す。「私が言葉を使うとき」とハンプティ・ダンプティはかなり軽蔑的な口調で言った。 「問題は、単語を非常に多くの異なる意味にできるかどうかです」とアリスは言いました。 「問題は、マスターになることです。それがすべてです」とハンプティ・ダンプティは言いました。セキュリティエンジニアは、単語がさまざまなアプリケーションで取得する意味のさまざまなニュアンスに敏感であり、セキュリティポリシーとターゲットが実際に何であるかを形式化できる必要があります。