情報処理技術が社会にとってますます重要になるにつれて、これらの懸念は、以前はオペレーティングシステムのように本質的に無害であると以前は考えられていた領域に広がりました。  
–英国市民サービスVERB9。  
 セキュリティポリシーは、私たちが達成しようとしていることを簡潔に説明したものです。それは、回避したい悪い結果を理解することによって推進され、次にエンジニアリングを推進します。  
。  
）、クリアランスレベルが少なくとも同じくらい高いプリンシパルだけがデータを読み取れるようにする必要があります。  
2999。  
 セキュリティポリシーモデルとは何ですか？政府の請負業者のために働くつもりがない場合でも、いくつかの理由で重要です：1。  
したがって、モデルは非常に詳細に検討され、熱意のある単一の政策目標を追求することの2次的な影響を理解することができました。2。  
 マルチレベルのセキュリティ概念はもともと軍事システムの機密性をサポートするために開発されましたが、現在、多くの商用システムはマルチレベルの整合性ポリシーを使用しています。  
詩人アルキロコスは、キツネは小さなことをたくさん知っているが、ハリネズミは大きなことを1つ知っていると有名に述べています。  
9。  
このプロセスの重要かつ無視されがちな部分は、セキュリティポリシーです。  
 それは、脅威に対する私たちの理解によって推進され、次にシステム設計を推進します。  
 これは、システムの保護要件を指定し、それらが満たされているかどうかを評価する際に、システム仕様が機能性について、安全性について安全性について行うことと同じ役割を果たします。  
図9に示すように、多くの組織は「セキュリティポリシー」というフレーズを使用して、虚偽のステートメントのコレクションを意味しています。  
発電の安全度レベルはBibaに似ていますが、自動車の安全度レベルは、ISO 26262で、予想される重大度と制御性とともに、障害が事故を引き起こす可能性に応じたハザード/リスクメトリックとして設定されています。セキュリティエンジニアリング300ロスアンダーソン9。  
 セキュリティポリシーモデルとは？Megacorp Incのセキュリティポリシー1。  
2。  
3。  
4。  
図9。  
 それは中心的な問題、つまり「誰が「知る必要があるか」をどのように決定するか」を回避します。次に、異なるレベルでステートメントを混合します（ポリシーの組織的承認は、論理的にポリシー自体の一部であってはなりません）。  
 政治家の仕事は社会の緊張を解決することであり、これにはしばしば異なる派閥が自分の願いを投影できる曖昧な言葉が必要です。企業幹部は、企業内の異なる派閥のバランスをとるために、政治的に活動していることがよくあります2。  
セキュリティポリシーモデルは、システムに必要な保護プロパティの簡潔なステートメントです。  
 これは、システム全体の保護目標がコミュニティ全体、または顧客のトップマネジメントと合意した文書です。  
セキュリティターゲットは、特定の実装が提供する保護メカニズムの詳細な説明であり、それらが制御目的のリストにどのように関連するか（すべてではありませんが、通常はポリシーモデルから派生しています）。  
保護プロファイルはセキュリティターゲットのようなものですが、製品に依存しない方法で表現され、製品やバージョン間で比較可能な評価を可能にします。  
 保護プロファイルは、コモンクライテリア[1396]に基づいて評価される製品の要件です。  
）それほど正確である必要がない場合は、「セキュリティポリシー」というフレーズを使用して、セキュリティポリシーモデルまたはセキュリティターゲットのいずれかを指します。  
2大きなプロジェクトは、仕様が政治的になると企業で失敗することが多く、政府が運営する場合はさらに失敗することがよくあります。この問題については、パート3で詳しく説明します。  
3。  
 より一般的には、モデルがすでに存在しています。適切なものを選択し、それをセキュリティターゲットに開発する必要があります。  
 本のこのセクションでは、いくつかのセキュリティポリシーモデルを提供し、それらを実システムのコンテキストで説明し、セキュリティターゲットがそれらを満たすために使用できるエンジニアリングメカニズム（および関連する制約）を調べます。  
3マルチレベルのセキュリティポリシー1940年3月22日、ルーズベルト大統領は大統領令8381に署名し、特定の種類の情報を制限付き、機密、または秘密に分類できるようにしました[978]。これは、文書の機密性のための一般的な保護マーキング方式に発展し、冷戦時代にもNATO政府によって採用されました。  
2）。  
 政府の被雇用者と請負業者は、綿密に調査されたケアに応じて許可を得ています。たとえば、米国では、「秘密」のクリアランスにはFBIフィンガープリントファイルのチェックが含まれ、「トップシークレット」には、以前の5〜15年の就職のバックグラウンドチェックと面接、および多くの場合、ポリグラフテストが含まれます[548]。  
アクセス制御ポリシーはシンプルでした。クリアランスがドキュメントの分類と少なくとも同じ高さである場合にのみ、ドキュメントを読むことができます。  
 したがって、情報は機密情報から機密情報から最高機密情報まで、上向きにしか流れないかもしれませんが、許可された人がそれを機密解除するために故意に決定しない限り、下向きになることはありません。  
2 –マルチレベルのセキュリティシステムは急速に複雑化しました。  
 それまでに、約100万人のアメリカ人が最高機密の認可を取得しました。 OPMデータは、以前の従業員と求職者、ならびにそれらの親族と性的パートナーもカバーしました。  
セキュリティエンジニアリング302ロスアンダーソン9。  
 MULTILEVEL SECURITY POLICY経済的危害、さらには政治的当惑。  
特にSe-cret以上の情報をさらに制限できるコードワードのシステムもあります。  
 一部のコードワードは特定の軍事作戦または情報源に関連しており、指名されたユーザーのグループのみが利用できます。  
 分類ラベルとコードワードのセットは、セキュリティカテゴリ、または（少なくとも1つのコードワードがある場合）コンパートメントを構成します。これは、同じアクセス制御ポリシーを持つレコードのセットです。  
記述子、警告、IDOマーキングもあります。  
 警告は、「UK Eyes Only」や米国の「NOFORN」などの警告です。彼らは制限を作成します。  
 コードワード、記述子、警告、IDOマーキングの間に明らかな違いがないため、システムが混乱しやすくなります。  
9。  
1アンダーソンのレポート1960年代、コンピューターが広く使用され始めたとき、分類システムは深刻な摩擦を引き起こしました。  
 同じデスクで異なるレベルの情報を処理する必要があることに人々はすぐに気付きましたが、秘密を漏らすことなくこれを行うにはどうすればよいでしょうか。オペレーティングシステムのバグが1つ修正されるとすぐに、他の脆弱性が発見されます。  
 CUIシステムを採用する前に、熟練していないユーザーでも4の懸念が常にありました。米国では、管理されているが分類されていないデータに対して、50を超える異なるマーキングがありました。施行センシティブ（LES）、専有（PROPIN）、連邦税情報（FTI）、センシティブだが未分類（SBU）、その他多数。  
 CONFIDENTIALとマークされた民間文書が最終的に国立公文書記録管理局に提出されると、さらなる問題が発生し、CONFI-DENTIALは国家安全保障の分類でした。  
 英国には、独自の冷戦後の単純化物語があります。  
セキュリティエンジニアリング303ロスアンダーソン9。  
 マルチレベルセキュリティポリシー抜け穴を発見し、日和見的に使用します。また、悪意のあるコードからの脅威に対する鋭敏で高まる認識もありました。  
）その後、ペンタゴンのワールドワイドミリタリーコマンドアンドコントロールシステム（WWMCCS）がトロイの木馬攻撃に対して脆弱であることが発見されたとき、深刻な恐怖がありました。これは、その使用を「トップシークレット」のクリアランスを持つ人に制限する効果があり、不便でした。  
 参照モニターの概念が導入されました。これは、アクセス制御の決定を仲介し、分析とテストの対象となるほど十分に小さいオペレーティングシステムのコンポーネントであり、その完全性は保証されます。  
 より正式には、TCBはコンポーネントのセット（ハードウェア、ソフトウェア、人間など）として定義されます。  
。  
 Andersonreportの目標は、TCBが慎重に検証できるようにセキュリティポリシーをシンプルにすることでした。  
3。  
 その基本的な特性は、情報が下方に流れることができないことです。  
これは、読み取りなし（NRU）とも呼ばれます。•\*-プロパティ：プロセスがデータを下位レベルに書き込むことはできません。  
\*プロパティはBellとLaPadulaの重要なイノベーションでした。クリアされていないユーザーがトロイの木馬を作成し、システム管理者が「シークレット」にクリアした場所で実行する可能性があります。その後、システムの「秘密」の部分に自分自身をコピーし、そこでデータを読み取り、何らかの方法で信号を送ろうとします。  
 その後、作成者がそれらを読み取ることができる場所までそれらを書き留めることができれば、セキュリティポリシーに違反したことになります。  
悪意のあるコードやバグのあるコードなどの脆弱性が想定されています。  
3。  
 そのため、既存の文化では、セキュリティポリシーはユーザーの操作とは無関係に実施されると想定されていました。Bell-LaPadulaは、ユーザーの直接の行為だけでなく、間接的な行為（ユーザーが実行するプログラムによって実行される行為など）からも実施することを目指しています。 。  
 より一般的には、HighのプロセスがLowのオブジェクトにシグナルを送ることを防ぐ必要があります。  
Bell-LaPadulaモデルにより、設計者は定理を証明できました。  
 話を簡単にするために、これからは、システムには高レベルと低レベルの2つのレベルしかないと一般的に想定します。  
3。  
 研究者はそれに打ち勝ち、それを洗練し始めました。  
 このようにして、LowユーザーはBLPの前提を破ることなく任意のHighファイルを読み取ることができます。  
 この問題は、静けさの特性を導入することによって処理されます。  
なぜ静寂が弱いのですか？実際のシステムでは、プロセスの所有者が「トップシークレット」にクリアされている場合でも、最小特権の原則を遵守し、クリアされていないレベルでプロセスを開始することがよくあります。  
 サブジェクトは通常、プロセスではなくメモリ管理サブシステムとファイルハンドルを抽象化したものであるため、データが実際に移動するのではなく、アクセス権が変化すると状態が変化します。  
 したがって、「Secret」と「Crypto」でファイルを読み取ったプロセスは、その後「Secret Crypto」とマークされたファイルを作成します。  
3。  
 その後、「Secret Nuclear」でファイルを読み取ると、その後作成されるすべてのファイルに「Secret Crypto Nuclear」というラベルが付けられ、「Secret Crypto」で一時ファイルに書き込むことはできなくなります。  
 セキュリティレベルのリアルタイムの変化は、リソースへのアクセスがトランザクションの途中を含むいつでも取り消されることを意味します。  
 注意と努力を払わない限り、すべてが最高のコンパートメントに到達すること、またはシステムが互いに通信しない何千もの小さなコンパートメントに断片化することを簡単に見つけることができます。  
BLPのもう1つの問題、そしてすべての必須のアクセス制御システムには、ユーザーとプロセスの分離が簡単な部分があります。難しいのは、制御された相互作用が必要な場合です。  
 BLPは、システムがこのようなアプリケーションをどのように保護すべきかについては何も述べていません。  
最後に、ハイウォーターマークの精緻化を行っても、BLPはサブジェクトまたはオブジェクトの作成または破棄を処理しないことに注意してください（これは、実際のMLSシステムを構築する際の難しい問題の1つです）。  
3。  
最初のマルチレベルのセキュリティポリシーは、IBM S / 360メインフレーム[2006]向けに開発された必須のアクセス制御システムであるADEPT-50用に1967年から8月に作成された最高水準点のバージョンでした。  
 （プロセスではなく）プログラムが対象であったため、トロイの木馬の侵害に対して脆弱でした。  
次の大きなステップはMulticsでした。  
 Paul KargerとRoger Schellによって行われた評価は非常に影響力があり、マルウェアがコンパイラに隠される可能性があるという考えが最初に現れ[1019]、ケントンプソンの有名な論文「Retrustions on Trusting Trust」を10年間導きました後で[1883]。  
4。  
セキュリティエンジニアリング306ロスアンダーソン9。  
 マルチレベルセキュリティポリシー1980年代からマルチレベルセキュリティに注がれた研究費の急増により、いくつかの代替的な定式化が行われました。  
 このプロパティを持つシステムでは、HighのアクションはLowが見ることができるものに影響を与えません。  
 99％の確実性でHigh入力についての推論を行うLowを止めることができないため、非推論は弱すぎることが判明しました。  
この革新の波の中で、現代のシステムに最大の影響を与えるモデルは、おそらくタイプエンフォースメント（TE）モデルです。これは、後にアールボーバータントディックケイン[271]がリーバッジャーや他の人々によってドメインおよびタイプエンフォースメント（DTE）に拡張したためです。 153]。  
これはSELinuxで使用されており、現在はAndroidのコンポーネントです。サブジェクトとオブジェクトの両方を型に入れ、許可された型のペアのマトリックスを持つことでそれを簡素化します[1187]。Linux Security Modulesフレームワークは、SIDを操作するルールを設定できるプラグイン可能なセキュリティを提供します。  
 DTEはBLPよりも一般的です。これは、DTEが完全性と機密性の懸念の範囲内で対処し始めるためです。  
 これは、少なくとも2つのステージが危険にさらされない限りバイパスできないガードとファイアウォールを組み立てるために使用できます[1430]。  
 これは物事をより扱いやすくすることができます。  
TE / DTEの柔軟性と表現力が高いことの欠点は、BLPなどのポリシーを実装することが必ずしも簡単ではないことです。セキュリティポリシーを作成するときは、異なるタイプ間で起こり得るすべての相互作用を考慮する必要があります。  
 しかし、これはこれを正しく行うために他にかなり多くのものが必要であるという保証はあまりありません。たとえば、低トラフィックがトラフィック分析を実行できないように高トラフィックをnullでパディングする–初期の例については、[1632]を参照してください。そのようなシステム。  
セキュリティエンジニアリング307ロスアンダーソン9。  
 マルチレベルセキュリティポリシーあなたが導き出したポリシーは正しいものです。  
 これは、個々のユーザーやマシンではなく、主にロールに適用されるルールを正式化します[678、679]。  
 ロールまたはグループは、何年もの間、銀行などの組織でアクセス制御を管理するために実際に使用されていたメカニズムでした。 RBACモデルはこれを形式化し始めました。  
 その変形であるアスペクトベースのアクセス制御（ABAC）はコンテキストを追加するため、「ラボのワークステーションにあるロス」と「地球上のどこかにある彼の電話のロス」を区別できます。  
SELinuxはTEの上にそれを構築するため、ユーザーはログイン時にロールにマップされ、ロールはドメインに対して許可され、ドメインにはタイプへのアクセス許可が与えられます。  
 したがって、たとえば、ネットからダウンロードされた信頼できないソフトウェアを呼び出すプロセスは、機密のシステムファイルへの書き込みに必要なロールメンバーシップを失う可能性があります。  
5。  
9。  
5Bibaモデルマルチレベルの整合性モデルをWindows 7に組み込むと、1975年にKen Bibaによって考案されたセキュリティモデル[237]に関心がよみがえりました。これは整合性のみを扱い、機密性を無視します。  
したがって、BLPを上下逆にすることで整合性ポリシーにリサイクルできます。  
 校正データは破損から保護する必要があるため、通常のユーザーはデータを読み取ることはできますが、書き込むことはできません。通常のユーザーがデバイスをリセットすると、現在のユーザー状態（i。  
、メモリ内のすべての患者データ）が、キャリブレーションは変更しないでください。  
このようなシステムをモデル化するには、より高いレベルでデータを読み取ることができるルール（i。  
、ユーザープロセスは、キャリブレーションデータを読み取り、下位レベル（i。  
、キャリブレーションプロセスはユーザープロセスのバッファに書き込むことができます）;ただし、高整合性オブジェクトが低–iで汚染される可能性があるため、決して読み書きしないでください。  
 信頼できない可能性がある–データ。  
これは整合性の最初の正式なモデルでした。  
たとえば、乗客の情報-Security Engineering308Ross Anderson9。  
 MLSシステムの歴史的な例鉄道のシステムは、信号システムから情報を取得する場合がありますが、影響を与えることはできません。また、電力会社の配電システムは、安全システムの状態を確認できますが、それらに干渉することはありません。  
Windowsは、バージョン6（Vista）以降、ファイルオブジェクトに整合性レベル（低、中、高、またはシステム）でマークを付け、NoWriteUpのデフォルトポリシーを実装しています。  
 そのため、IEを使用してダウンロードしたものは、Windowsシステムでほとんどのファイルを読み取ることができますが、ファイルに書き込むことはできません。  
ご想像のとおり、BibaにはBell-LaPadulaと同じ基本的な問題があります。  
 たとえば、実際のシステムでは通常、セキュリティモデルを上書きできる信頼されたサブジェクトが必要ですが、Biba自体では、BLPができる以上の保護と制限はできません。  
 パイプラインの保証など、Bibaでも表現できない真の整合性の目標は他にもあります。  
 実際、Type Enforcementmodelは、Biebaの代わりとしてBoebertとKainによって導入されました。  
9。  
9。  
1SCOMPAの主要製品は、1983年に発売されたMulticsの派生版であるセキュア通信プロセッサ（SCOMP）でした[710]。  
 正式に検証されたハードウェアとソフトウェアがあり、物事をシンプルに保つために最小限のカーネルを備えていました。SCOMPは、軍事郵便警備員などのアプリケーションで使用されていました。  
 （一般的に、一方向のフローをサポートするデバイスは、データダイオードとして知られています。  
 これは、セキュリティエンジニアリング309Ross Anderson9の時分割強制配備データ（TPFDD）システムで使用されていました。  
 MLSシステムの歴史的な例機能は、米軍の移動と関連する兵站を計画することでした。  
 これは、1985年に導入され、2000年12月に廃止された、安全なコンピュータシステムの最初の体系的な標準でした。  
Orange Bookを使用すると、システムをさまざまなレベルで評価できます。A1が最高で、B3、B2、B1、C2からC1へと下方に移動します。  
 また、公開された文献にも詳細に記載されていました。  
MLSバージョンのUnixは、AT＆TのSystem V / MLS [47]など、1980年代後半に登場し始めました。  
 この本の第2版（2007年）までに、SunのSolarisは、高保証のサーバーシステムや、あらゆるクライアントを形成するための最適なプラットフォームとして登場しました。  
 エンジニアリングについては、[635、636]を参照してください。  
4。  
 第一世代のMLSメカニズムは、リアルタイムサービスには不十分でした。  
3：– NRLポンプ米国海軍研究所（NRL）は、安全な一方向の情報フローを可能にする一方向のデータ転送デバイス（データダイオード）であるポンプを開発しました（図9。  
 主な問題は、データをLowからHighに送信するのは簡単ですが、伝送の信頼性を保証する必要があるということは、Security Engineering310Ross Anderson9を認めていることです。  
 MLSシステムの歴史的な例エッジメッセージは、高から低に送信する必要があります。  
 このアプローチの魅力は、データダイオードを使用して異なるセキュリティレベルで個別のシステムを接続することにより、MLSシステムを構築できることです。  
MLSを内部で適用することについて心配する必要はありません。物理的またはネットワークベースのいずれであるかにかかわらず、外部の攻撃からMLSを保護するだけです。  
 ポンプの話は[1015]で語られています。  
 一部の信号インテリジェンス機器は「トップシークレット」ですが、ジェット燃料やブーツレースなどはそうではありません。しかし、そのような単純な商品でさえ、その数量や動きが戦術的な意図に関する情報を漏らす可能性がある場合、「秘密」になる可能性があります。  
 英国では、イギリス空軍のLogisticsInformation Technology System（LITS）は10年間（1989〜99年）であり、RAFの80の基地に単一の店舗管理システムを提供するための5億ポンドのプロジェクトでした[1386]。  
 最初は、MLSプロパティを適用するためにポンプで接続された2つの個別のデータベースシステムとして実装されていました。  
 これらの変更の1つは、冷戦の終結に伴う分類規則の緩和でした。  
g。  
 お金を節約するために、「秘密」の情報はCDに保存され、金庫に保管されます。  
 インベスティゲーションのターゲットは、彼らが盗聴されていることを知らないはずです。そのため、サードパーティは沈黙している必要があります。電話会社が盗聴を無音の会議通話として実装し始めたとき、電話会議の料金は、ターゲットではなく、盗聴者に支払わなければなりませんでした。  
 隠れチャネルを排除することは、見かけよりも困難です。 2000年代半ばの調査については、[1707]を参照してください。 suspectscanが盗聴装置をハッキ​​ングまたは混乱させようとするため、純粋なMLSセキュリティポリシーでは不十分であり、したがってオンラインでの改ざんを再度阻止する必要があります。  
電話会社は7,600万ユーロ（ほぼ1億ドル）の資金を調達しました。  
セキュリティエンジニアリング311ロスアンダーソン9。  
 MAC：MLSからIFCおよび整合性へ軍用組み込みシステムも数多くあります。  
 船が港にいるときに機器が最高機密にならないようにする必要があるため、エンジニアリングが複雑になります。メンテナンスが複雑になるためです。  
 F-16パイロットがレーダーの速度が意味をなさない非常に速いUFOを見ている話を読むとき、2つと2つを組み合わせることができます。  
9。  
」政府機関は、MACがマルウェアを阻止するために必要なものであることを知っていました。  
9。  
1WindowsWindowsでは、すべてのプロセスが実行し、すべてのセキュリティ保護可能なオブジェクト（ディレクトリ、ファイル、レジストリキーを含む）に整合性レベルのラベルが付いている場合があります。  
 したがって、既存のファイルを変更する前に、ダウンロードしたコンテンツをアップグレードするためのユーザーアクションが必要です。  
 これらはデフォルトではインストールされません。マイクロソフトは、マルウェアがシステムにインストールされてから隠れることを懸念していました。  
 しかし、MACに対するこの整合性のみのアプローチは、低で実行されているマルウェアがすべてのデータを盗むことを意味します。そのため、一部のユーザーは、機密ディレクトリに「NoReadUp」を設定することに関心があるかもしれません。9。  
2SELinuxSELinuxのケースは、必須のアクセス制御メカニズムの当面の目標が妥協の影響を制限することでもあったという点で、Windowsにいくらか似ています。  
6。  
 セキュリティ識別子は、セキュリティサーバーによってマップされたセキュリティコンテキストへのハンドルです。  
 Linux 2から主流になりました。  
 サーバーは、残りのカーネルにセキュリティAPIを提供し、その背後にセキュリティモデルが隠されています。  
 2000年代半ば以降の典型的なLinuxディストリビューションでは、さまざまなサービスを分離するために使用されていたため、Webサーバーを乗っ取る攻撃者はDNSサーバーも取得していません。  
9。  
3組み込みシステムBibaモデルのいくつかのバリアントを実装する多くのフィールドシステムがあります。  
 たとえば、電力会社では、通常、最高の安全度レベルで完全に独立して動作する安全システムの階層があります。これらは、電力供給などの運用システムからは見えますが、影響を受けることはありません。小売レベルのメータリングシステムは、課金システムによって監視できますが、影響を受けません。  
ラジオでは悪意のあるアプリがブレーキを操作できるようにしたくないため、車ではほとんどのメーカーがパワートレイン用とキャビン用に別々のCANバスを備えています（ただし2010年にセキュリティ研究者は分離が完全に不十分であると発見しました[1085] ）。  
要約すると、初期のマルチレベルシステムで学んだ教訓の多くは、幅広い関心を持つ多くのアプリケーションに当てはまります。  
9。  
 高レベルの保証を備えた単純なポリシーに従うためにシステムを構築するために費やした数十億ドルは、情報フロー制御の多くの2次および3次の結果を明らかにしました。  
セキュリティエンジニアリング313ロスアンダーソン9。  
 何が間違っているか9。  
1Composability2つの「高」入力H1とH2を受け入れる単純なデバイスを検討してください。マルチプレックスヘム;ワンタイムパッド（i。  
、ランダムなジェネレーター）;パッドのもう一方のコピーをH3に出力します。図9に示すように、完全な機密性を与える暗号システムで暗号化されている暗号文は低いと見なされます（出力L）。  
H1-H2-XORRAND-H3XOR•--- L図9。  
 ただし、フィードバックが許可されている場合は、H3からの出力をH2にフィードバックできます。その結果、高入力H1が低出力Lに現れます。  
一般に、2つ以上のセキュアコンポーネントをセキュアシステムに構成する方法である合成の問題は、理想的なコンポーネントについての証明された結果が比較的雑然としないレベルでも難しい[1430]。  
）何らかのフィードバックが導入されると、低レベルの問題のほとんどが発生します。それがなければ、いくつかの正式なモデルの下で構成を達成できます[1277]。  
 たとえば、あるシステムが別のシステムに対してサービス拒否攻撃を実行するような速度でデータを生成する場合があります。  
 コンポーネントは、2つの異なるセキュリティポリシーに従って設計されているか、一貫性のない要件に従って設計されている可能性があります。  
6。  
5）。  
 たとえば、B3に評価されたシステムは、通常、Security Engineering314Ross Anderson9に許可されました。  
 機密情報を機密扱い、機密、秘密、または機密、秘密、極秘で処理します。未分類データと最高機密データを同時に処理することを許可されたシステムはありませんでした[548]。  
5：–カスケード問題図が示すように、このポリシーが破られるような方法で2つのB3システムを接続することは簡単です。  
 これにより、スパン制限が無効になります。  
6。  
 1973年にランプソンによって最初に指摘された[1125]秘密チャネルは、通信用には設計されていませんが、悪用されて情報が高から低に伝達されるメカニズムです。  
 最新のマルチコアCPUでは、時刻tiに使用するCPUコアのクロック周波数を上げて、トップシークレットファイルのi番目のビットが1であることを通知し、ビットを0にしたことを通知するように縮小することができます。  
 2018年以降、CPU設計者は、CPUマイクロアーキテクチャーを利用する一連のカバーチャネルに苦労しています。 Meltdown、Spectre、Foreshadowなどの名前で、HighがLowに信号を送るだけでなく、Lowがアクセス制御を回避してHighでメモリを読み取る方法を提供しています。開発者が通常のオペレーティングシステムで機密性保護を一貫して行うことができた最善の方法は、1秒あたり1ビットまたはそれ以上に制限することです。  
）1秒あたり1ビットは、satelliteSecurity Engineering315Ross Anderson9などの大きなTS / SCIファイルを防止する必要がある環境では許容できる場合があります。  
 WHAT GOES WRONGphotographs – TS / SCIユーザーから「シークレット」ユーザーに漏れる。  
 これは、特別な目的のハードウェアで暗号化を行うという軍および銀行の原則の理由の1つです。  
この場合、隠れチャネル帯域幅は毎秒数メガビットであるため、レーダーコードを信頼する必要があります。  
6。  
 彼の最初の実験では、書き込みに8時間しかかからなかったファイルウイルスは、以前はマルチレベルのセキュリティであると考えられていたシステムに侵入することができました[450]。  
悪意のあるコードを使用してアクセス制御を破る方法はたくさんあります。  
 このため、システムアプリケーションが悪意のあるロジックの挿入に対して適切に保護される[548]と定義されている、いわゆるクローズドセキュリティ環境に少し緩いルールが適用され、ベンダーが改ざん防止のインセンティブを生み出しました。 TCB、TPMなどの手法を使用します。  
9。  
5ポリインスタンス化研究コミュニティを行使したもう1つの問題は、ポリインスタンス化です。  
 MLSオペレーティングシステムが彼を禁止している場合、情報が漏えいします。つまり、Highにエージェントと呼ばれるファイルがあるということです。  
多くの場合、低ユーザーと高ユーザーに異なるディレクトリを与えるなどの命名規則によって問題を解決できます。  
 Highユーザーが船に分類された貨物を割り当てるとします。  
ここでは、米国と英国の慣行が分かれています。  
 したがって、基になるデータは図9のようになります。  
セキュリティエンジニアリング316ロスアンダーソン9。  
 WHAT GOES WRONGLevelCargoDestinationSecretMissilesIranRestricted––UnclassifiedEngine SparesCyprus図9。  
 2つの利用可能なビューは、図9のようになります。  
LevelCargoDestinationSecretMissilesIranRestrictedClassifiedClassifiedUnclassified––図9。  
 また、カバーストーリー（e。  
、低ユーザーはキプロスの弾薬のコンテナーを追加しようとします）。  
（実際には、秘密の使命の存在を必要以上に宣伝しないようにするために、カバーストーリーは引き続き使用されます。  
6。  
 コストと混乱には多くの原因があります。  
 それらは少量で構築され、多くの場合、物理的な堅牢性の高い基準に基づいて、軍事購買官僚が推進する精巧な文書、テスト、およびその他の品質管理手段を使用しています。  
 MLSシステムには、特異な管理ツールと手順があります。  
3。  
4。  
 新しいファイルはデフォルトで、可能な入力に属する最高のラベルになります。  
 システムコンポーネントが見たすべてのラベルを累積して、ラベルの爆発につながる特定の問題があります。セキュリティエンジニアリング317ロスアンダーソン9。  
 何が問題なのかというと、単一のプリンシパルがそれらにアクセスできなくなるようなコレクションを取得しています。  
 この「TCB膨張」は、評価のコストを常に押し上げ、保証を減らします。  
 データの分類は複雑になる可能性があります。•競合の前段階で、食品などの「無害な」店舗の場所は戦術的な意図を明らかにする可能性があるため、突然格上げされる可能性があります。•分類は常に単調であるとは限りません。  
インテリジェンス分析は、TS / SCIで分類された衛星写真を撮り、「秘密」でフィールドの指揮官のための評価に貼り付ける必要があります。  
 1つのオプションは、ドキュメントをビットマップに変換し、追跡のためにログに記録する「印刷とFAX」メカニズムです。  
 たとえば、衛星写真を1つでも機密解除してもかまいませんが、コレクション全体を機密解除すると、監視機能と機密情報の優先順位の履歴が明らかになります。  
2。  
6。  
したがって、軍事環境であっても、その利益には疑問の余地があります。  
 もちろん、その代償はスノーデンの開示でした。  
 最後に、強迫的な政府の秘密は慢性的な負担です。  
 たとえば、教皇がトルーマンにヴェノナの暗号解読を知らされたことはありませんでした。  
シークレットは組織の資産になり、他の組織の資産と引き換えに共有されることはありません。6。  
これは、苛立たしいイギリスの一般人からの皮肉を思い起こさせます：「ジュラシックパークと国防省の違いは何ですか？ 1つは恐竜でいっぱいのテーマパークで、もう1つは映画です！」内部の戦略的批評は不足していません。  
 生産者と消費者のコミュニティの広く異なるリスク/利益計算を含む多くの興味深い理由があります。分類は、実際のリスクではなく、流通チャネルによって支配されるようになります。  
 それは多くの不可解な結果を指摘した。たとえば、イラクの捕食者の画像は分類されておらず、暗号がNSA官僚の鍵管理に関与し、戦闘を抑制することを軍が恐れていたため、しばらくの間は不明瞭でした。  
とにかく、この本の第2版以降の大きな変更点の1つは、MLSに関する巨大なDoD研究プログラムがなくなり、MLS機器が政府系システム市場であまり積極的に宣伝されなくなったことです。システムは10年間かなり静止しています。  
 上記のセクションで説明した困難に加えて、ハードウェアのコストの低下と仮想化の到来により、同じマシンで異なるレベルを使用するインセンティブが損なわれました。  
 実際の分離は、未分類のネットワーク、暗号の背後にある基本的に標準的な機器を使用して秘密データを処理する秘密インターネットプロトコルルーターネットワーク（SIPRNet）、および最高機密資料を処理する共同世界規模の情報通信システム（JWICS）の間のネットワークレベルにあります。システムはSecure Compartmentalized InformationFacilities（SCIF）に保管されます。部屋は電子的な盗聴を防ぐためにシールドされています。これについては、後でサイドチャネルの章で説明します。  
 このような醜いハッキングは、悪用される可能性が明確です。せいぜい、正直な人々を不注意な間違いから守るのに役立ちます。  
7。  
7SummaryMandatoryアクセスコントロールは当初、軍事用に開発されましたが、特殊なファイアウォール（ガードおよびデータダイオード）でも使用されています。  
MACメカニズムは1970年代中頃からコンピューターセキュリティ研究の主要な主題であり、軍事的マルチレベルのセキュリティにそれらを使用しようとすることで学んだ教訓は、セキュリティ評価に使用されるスキームの多くの根底にあります。  
解決するには、「ヘッジホッグ」ではなく「フォックス」である必要がある多くの問題があります。  
研究上の問題NSAがSELinuxを発表した後、2001年にEarl Boebertによってスケッチされた現在の課題は、必須のアクセス制御メカニズムを安全が重要なシステムに適応させることです（この章の冒頭の引用と[270]を参照）。  
 モノのインターネットで広く使用されていると思いますか？車や配電などのアプリケーションでのBibaタイプのメカニズムについて説明しました。 SELinux、Windows、Androidなどの製品のMACメカニズムにより、設計者は情報フローをロックダウンし、予期しない相互作用の可能性を減らすことができますか？ 。  
 現代のオペレーティングシステムの固有の複雑さに加えて、電話には大量のサイドチャネルがあり、そのアプリは多くの場合、クラウドサービスとの通信にのみ役立ちます。  
実際の軍事作戦を取り巻く別の一連の研究問題があり、現実は政策にはるかに及ばない。  
 英国海軍は2009年に電話を禁止しようとしましたが、あまりにも多くの船員が去りました。  
 規律は、船員が地雷の処分を急いで見られる場合など、即時の操業上の脅威に焦点を合わせる傾向があります。問題は、鉱山の近くで無線機を使用するリスクです。異なる海軍には、セキュリティエンジニアリング320ロスアンダーソン9があります。  
 概要異議のあったこと：ノルウェー人には船員のための独自の特別なネットワークがあり、米国はMLS機能を備えた電話を試みています。  
 そしてイスラエル人でさえ、兵士たちがWestBankとGolan Heightsで携帯電話を使用することに問題を抱えています。  
 ウォーカースパイリングに関するレポートは、壮大な障害の詳細な説明であり、毎年300万人がいつでもクリアランスを取得し、毎年100万件のアプリケーションが処理されているシステムを実行することの非常に複雑さをもたらします[876]。技術面では、Dieter GollmannのComputer Se-curity [779]などの教科書がMLSシステムの概要を説明していますが、実際のMLSシステムに関する多くの出版論文は、2つの会議の議事録に掲載されています。セキュリティとプライバシーに関するIEEEシンポジウム（以前は開催されていた場所で「オークランド」として知られています）、NSAサプライヤーコミュニティの未分類のbashは、（オークランドのように）公開されているコンピュータセキュリティアプリケーション会議（ACSAC）です。 IEEE。  
 この分野の古典的な初期の論文の多くは、NISTアーカイブ[1395]にあります。NISTは、1999年までマルチレベルセキュリティに関する会議シリーズを実施していました。  
セキュリティエンジニアリング321ロスアンダーソン