滑走路には、核兵器とコックピットに外国人パイロットが搭乗したドイツ（またはトルコ）の緊急対応警報機が立っていました。  
 Uの唯一の証拠。  
 コントロールは、カービン銃で武装し、ターマックの上に立っている孤独な18歳の歩哨でした。  
S  
–ジェローム・ヴィースナー、キューバ危機後の核兵器の指揮統制についてケネディ大統領に報告した15。  
核兵器管理は国際外交の中心です：北朝鮮が現在爆弾を持っている間、南アフリカとリビアはそれを放棄するように説得されました、イランとシリアは彼らの大量破壊兵器プログラムを持っている間イランのプログラムは（外交的およびサイバー手段によって）停止されました強制終了。  
 実際には、これが望ましいと考えられていたとしても、どれだけ秘密にしておくことができるかには限界があります。  
1。  
。  
）そのため、民間の文脈で核物質の管理を維持する。  
 これは、国際原子力機関（IAEA）が施行した核不拡散条約や核物質の物理的保護に関する条約[949]などの国際協定に裏付けられています。  
 したがって、政府間だけでなく、ますます懐疑的な国民からも国際的な信頼を呼び起こす方法で、要塞を守らなければなりません1。  
米国エネルギー省の武器研究所-サンディア、ローレンスリヴァーモア、ロスアラモス-は、核兵器と核物質をできる限り安全にするために2世代にわたって取り組んできました。  
 保護対象のデバイスに光ファイバーを巻きつけ、干渉効果を使用して1ミクロン未満の長さの変化を検出するトリックも、それらの1つです–弾頭の弾頭をループでループし、それらのいずれかが移動されます。  
 たとえば、虹彩認証は、個人の生体認証で知られている最も正確なシステムで、現在はインドのアーダーアイデンティティシステムで使用されています。米国エネルギー省の資金を使用してプルトニウムストアへの入店を制御するために開発されました。改ざん防止および改ざん検知技術の専門知識は、盗まれた武器や制御装置の乱用を防ぐために元々進化してきました。  
 2003年3月のイラク侵攻、その原因はイラクが大量破壊兵器を所有しているとの主張であった2。  
 パキスタンの核計画の上級科学者であるアブドゥル・カディール・カーンが2004年に発表した、シリア、リビア、イラン、北朝鮮を含む他の国々が武器技術の保有と彼のネットワークの解体を支援した4 。  
セキュリティエンジニアリング486ロスアンダーソン15。  
 はじめに5。  
すべての成功が成功したわけではありませんが、明白な例としては、北朝鮮が石油の輸送と引き換えに兵器の開発を中止し、民間の原子力エネルギーの開発を支援するために1994年に米国との条約に署名しました。  
 この歴史のおかげで、トランプ政権が2018年にイランとの合意を放棄したことによる長期的な影響（イランはこれに同意していたにもかかわらず）を多くの人々が理解しています。  
核規制は、弾頭とその建設に必要な核分裂性物質以外にも適用されます。  
したがって、2007年にGAOの調査官は偽の会社を設立し、核規制当局から同位体の購入を許可する免許を取得しました。  
 テロへの恐怖のおかげで、核物質の規制は厳しくなり、経済により広く広がった。  
たとえば、発生させたくない特定のアクションの確率が人為的エラーによって発生する確率が10分の1である場合、5人の異なる人に確認してもらうことで、確率を1に減らすことができます。 100,000。  
 それでも2007年10月、ノースダコタ州のマイノット空軍基地からルイジアナ州のバークスデールまで巡航ミサイルを運んでいた飛行機が6個のミサイルを弾頭で武装させた後、36時間、6つの米水素爆弾が行方不明になった。  
 飛行機はルイジアナに着陸し、着陸し、滑走路に着陸し、地上の乗組員が到着する9時間前にミサイルを降ろし、ミサイルが生きていることを発見しました[187、549]。  
 人々は他者に頼り、ゆるやかにする–医療安全の世界でも知られている教訓。2。  
 では、このように失敗しないシステムをどのように設計できるでしょうか？この章では、原子力安全環境と、他の場所でアプリケーション（または脅威）を発見する可能性のあるいくつかのトリックについて説明します。  
15。  
 その安全性はやや即興でした。  
 しかし、重装荷されたB-29の多くは、彼らが使用していた基地であるテニアンからのタケオで墜落した。  
 捜査の前日、彼はプライマーの取り外しと再取り付けの練習をしました-パンの塊の大きさほどの火薬の装填–代わりに、武装後にそれを取り付けることができました。  
 それは進化の過程を経てきました。  
コンビネーションロックへの移行がありました。パイロットは、ワイヤードシールのふたが付いた特別なキーパッドに6桁のコードを入力して、爆弾を武装しました。  
しかし、1950年代の技術的制御と手続き的制御はどちらも原始的なものでした。  
2。  
ソビエトB-59はフォックストロット級のディーゼル電気潜水艦で、1962年10月27日に空母USSランドルフと11隻の駆逐艦からなる米軍戦闘グループが近くに爆撃を仕掛け始めました。  
 しかし、これは、船上にいる3人の上級役員が同意し、ラッキーなことにヴァシリーアルキポフが拒否した場合にのみ実行できます。  
これは、世界大戦が偶然にアメリカの政策立案者に顕著になるリスクをもたらし、ケネディ大統領は彼の科学顧問ジェローム・ヴィースナーに調査するよう命じました。  
 これらの武器は、米国の拘留されたトークンによって保護されていたため、武器が安全であるという物理的な理由はありませんでした。セキュリティエンジニアリング488ロスアンダーソン15。  
 コマンドとコントロールの進化は、危機的状況に陥る可能性はありません。  
’[1825]で、この章の冒頭に引用されている箇所を見つけました。  
 160 [217]。  
 このポリシーは米国の核兵器を外国人から保護するものとして議会に売却されましたが、クレイジーな「Dr Strangelove」（または現実のキャプテンサヴィツキー）に関する懸念は、実際にはヴィースナーのリストのトップにありました。  
基本的な原則は、武器が発動する前に環境のユニークな側面を感知しなければならないということでした。  
 例外が1つありました：原子爆弾。  
 偶発的または悪意のある爆発を防止する独自の環境センサーの範囲はないようです。  
主なエンジニアリング問題はメンテナンスでした。  
 したがって、すべての武器に同じコードを含めることは許容されません。  
ケネディのメモに続いて、すべての核爆弾はコードロックを使用して保護されるべきであり、大統領または彼の後継者だけが与えることができる「ユニバーサルロック解除」アクションメッセージがあるべきであると提案されました。  
問題は、教義が大規模な報復から「測定された対応」に変わった1960年代と1970年代に悪化しました。  
 これにより、特にメンテナンスの目的で武装解除コードも必要であることに気づいた場合や、武器の安全性と有効なコマンドの間のトレードオフをナビゲートするいくつかの手段など、複雑なシステムにつながり始めています。  
2。  
 アメリカで出現したのは、「オーソラリゼーション、環境、意図」のルールでした。  
許可：問題の武器の使用は許可されている必要がありますセキュリティエンジニアリング489ロスアンダーソン15。  
 国家司令当局による無条件の安全認証（i。  
、大統領と彼の合法的な後継者）。  
 （原子爆弾の場合、この要件は特別なコンテナを使用することで置き換えられます。  
初期のシステムでは、「認証」は4桁の認証コードをデバイスに入力することを意味していました。  
 航空機は通常、6桁の武装または「使用制御」コードを使用します。  
 実装が何であれ、それはユニークなシグナルでなければなりません。 6桁のコードから導出された22ビットは、ユーザビリティから偶発的な武装のリスクを最小限に抑えることまでの多くの要因の間の適切なトレードオフであると考えられています[1349]。  
3無条件に安全なAuthenticationNuclearコマンドと制御により、ワンタイム認証コードの理論が開発されました。  
 キーは1回しか使用されないため、認証コードは無条件に安全にすることができます。これにより、キーが与える保護は、攻撃者が利用できる計算リソースとは無関係になります。  
推測が成功する確率を制限するには、コード長を選択する必要があることを思い出してください。これは、相手が有効なメッセージを最初から推測しようとしたか（偽装）、既存の有効なメッセージを変更して別のメッセージを取得しようとしたか（置換）によって異なります。例でこれを明確にする必要があります。  
 指示には、「ロシアを攻撃する」と「中国を攻撃する」の2つの値があります。  
 メッセージの信憑性は、337で除算したときの残りを、鍵の2番目の部分である秘密番号に等しくすることによって保証されます。  
3。  
したがって、「攻撃ロシア」は「686」（または「12」）であり、「攻撃中国」は「349」です。  
ただし、有効なメッセージ（「Attack Russia」の「12」など）が表示されたら、337を追加することで簡単に別のメッセージに変更できるため、（指揮官の意図を理解していれば）他の国にミサイルを送ることができます。 。  
計算上安全な認証と同様に、無条件の多様性はメッセージの秘密性を提供するかどうかを決めることができます。それはブロック暗号のように、またはプレーンテキストメッセージのaMACのように機能します。  
 複数の仲裁人が必要な場合もあるため、個別に信頼する必要はありません。  
たとえば、機密性のない無条件のコードでは、従来の暗号化システムを使用してメッセージとオーセンティケーターを単純に暗号化することで、計算上安全な機密性を追加できます。  
 エラー訂正コードの設計者が特定のエラー回復機能に対して最短のコード長を望んでいるのと同じように、認証コードの設計者は、詐欺確率の特定の限界を達成するために必要なキー長を最小限に抑えたいと考えています。  
 キーを非武装化せずに人による武装解除または解体に抵抗する方法で、弾頭にキー制御メカニズムを構築する方法を考え出す必要があります。  
 攻撃者がソーシャルエンジニアのメンテナンス状況を常に把握し、これを防ぐために何をすべきかを考える必要があります。  
 バッテリーを交換するために爆弾の武装解除を行うメンテナンス担当者がユニバーサルロック解除コードを知らないように、一方向性の要素をどのように導入しますか？この1つの特定のデバイスのロックを解除するには、ユニバーサルロック解除からコードを導出できる必要がありますが、その逆はできません。  
 現在、米国のシステムでは、公開鍵暗号を使用してこの一方向性を実装していますが、一方向関数を使用することもできます。  
認証研究からの興味深いスピンオフの1つは、「暗号化」の章で説明されている、ブロック暗号のGCM操作モードでした。これは、最近の暗号スイートで最も一般的な操作モードになっています。  
4。  
4共有統制スキーム1970年代後半から、核の指揮統制ビジネスは懸念とともにさらに複雑になり、ソ連のアメリカ国軍司令部に対する斬首ストライキで兵器庫は無傷のままでは無益になる可能性がある。  
解決策は、秘密の共有と呼ばれる暗号数学の別のブランチで発見されました。  
さもなければ、多数の兵器の詳細な集中管理を維持するという問題は、おそらく解決できなくなります。  
 これらは、最初のストライキであなたの国を破壊した国に復讐するために、2番目のストライキ機能を提供するために存在します。  
 したがって、イギリスのアプローチでは、武装材料をボートの兵士の管理下にある金庫に保管し、武器が使用される状況に関する首相からの手紙を添えています。  
これはどのように一般化できますか？ええと、認証キーの半分を2人のユーザーそれぞれに与えるだけでも、キーの2倍の長さが必要です。ただし、どちらかが発行されたとしても、元のセキュリティパラメータを適用する必要があると仮定します。  
 これは、現金自動預け払い機のキーを管理する方法です2。  
 したがって、より一般的なアプローチは、1979年にBlakleyとShamirによって独立して発明されました[256、1703]。  
1）。  
 これを実装するには、z軸上の点Cを武器に提供する必要があるロック解除コードとします。  
 これで、それらの2つを組み合わせて、ラインの座標を計算し、z軸と交わる点Cを見つけることができます。  
 これで、3人の将軍、または2人の将軍と大臣が飛行機を再構築して、発砲コードCを再構築できます。  
ただし、無条件にセキュリティで保護された認証コードのコンテキストでは、追加は問題ない場合があります。  
4。  
1：–線や面ではなく、幾何一般代数構造を使用して制御を共有します。この手法により、武器、指揮官、オプションを、使用可能な帯域幅によってのみ制限される複雑さでリンクできます。これは、第5章「暗号化」で説明されているしきい値署名スキームの開発に影響を与え、「取引所の任意の2人の副社長がコールドビットコインウォレットをアクティブにする可能性がある」などのルールを適用する製品で使用できます。  
 多くの細部に注意が必要です。  
 銀行はほとんど同じです。大規模な支払いを解除するには2つのトークンが必要になる場合があります。委任規則では、両方のキーが1つのペアの手に落ちないように注意する必要があります。  
 典型的な例は有料テレビで、海賊が数十の加入者カードを購入し、その秘密のためにそれらをリバースエンジニアリングする場合があります。  
この裏切り者追跡問題については、著作権の章で詳しく説明します。  
5。  
5改ざん防止とPAL現代の兵器では、ソレノイド安全ロックは、ほとんどの米国の核装置を保護するために使用されるPermissiveactionリンク（PAL）に取って代わりました。  
 PALの開発は1961年頃に始まりましたが、展開に時間がかかりました。  
 より複雑なアーミングオプションが導入されたため、コードは4桁から6桁に、最終的には12桁に増加しました。  
PALシステムは、さまざまなコード化されたスイッチシステムと運用手順によって補足されます。また、PALがアクセス不能になるほど大きくて複雑ではない原子爆弾のような武器の場合、武器は、 PAPS（規定の行動保護システム）と呼ばれるタンパーセンシングコンテナー。  
どのようなシステムの組み合わせが使用されても、盗まれた武器から泥棒が核収量を獲得する能力を否定するペナルティメカニズムがあります。  
この自己破壊の手順は、敵の捕獲が脅かされている場合、収量なしで永久にそれらを動作不能にします。  
 爆弾の輸送を盗むために「テロリスト」を配備する準備をした反逆政府は、爆弾の一部（および一部の技術要員）を犠牲にして単一の使用可能な兵器を入手する準備ができていると想定されます。  
 さまざまなロック解除コードを保持しているデバイス（サービスおよび発射用）は、武器と同様に保護されています。  
このような野心的な目標を達成するには、非常に大きな努力が必要です。  
 他の人は、これは使用制御コードにすぎないと言いました。  
6。  
 成形された電荷は、8000m / sの速度でプラズマジェットを生成する可能性があり、理論的には改ざん検出回路を無効にするために使用できます。  
この注意は、実装と操作の多くの詳細に及ぶ必要があります。  
 イヴェンテン、可能な対戦相手によるアクセスを防ぐためにすべての実際的な対策が取られています。  
改ざん防止については、銀行カードや電話などのアプリケーションで広く使用されているため、改造については別の章で詳しく説明します。  
 さらに微妙なシステムのレッスンもあります。  
6条約の検証核不拡散条約の遵守を監視するために、さまざまな検証システムが使用されています。  
興味深い例は、包括的テスト禁止条約[1747]を監視するように設計された耐タンパー性地震センサーデバイスから来ています。  
 ここでの改ざん検知はかなり単純です。地震センサーは鋼管に取り付けられ、コンクリートで埋め戻されたドリル穴に挿入されます。  
 この物理的な保護は、ランダムチャレンジ検査によって強化されています。  
双方が信頼するサードパーティはなく、送信される地震データの量は1日あたり108ビット程度であるため、ワンタイム認証タグの代わりにデジタル署名スキーム（RSA）が使用されました。  
 ある当事者は、署名されたメッセージを生成する責任を負う担当者が不在であったため、署名されたメッセージを常に否認する可能性があるため、署名が偽造されました。  
7。  
 また、一方が機器を構築する場合、もう一方は非表示の機能があると疑います。  
 これらの問題の多くは、その後、電子商取引で再浮上しています。  
）15。  
15。  
1原子力事故主なリスクは単なる事故かもしれません。  
 世界最大の備蓄である160トンのプルトニウムを貯蔵する、セラフィールドのイギリスの主な廃棄物再処理工場は、何十年にもわたってスキャンダルに悩まされてきました。  
 すべてを一掃する作業には1世紀かかり、1,000億ドル以上の費用がかかる可能性があります。その間、それは守られなければなりません[1867]。  
 ロシアの状況はさらに悪化しているようです。  
15。2サイバー戦争との相互作用2番目の、そして増大している懸念は、サイバー攻撃の可能性によって原子力の安全性が損なわれる可能性があることです。  
7。  
 もう1つの重要な質問は、指揮官が画面に表示されるものを信じられるかどうかです。  
モスクワのバンカーの司令官であるスタニスラフペトロフ中佐は、ミサイルを5発だけ発射するのは非論理的であると考え、誤警報であると判断し、衛星が誤報であることを確認するまで発砲しました。  
 AIがあらゆる種類の場所でコマンドチェーンに侵入し、それを実現することなく、はるかに複雑なシステムができた今日、そのようなシステム障害はどのように起こりますか？そして、失敗を気にしないでください。ミサイル発射を監視し、核爆発を検出し、命令を渡す衛星を含む、情報、監視、偵察（ISR）機能への攻撃についてはどうでしょうか。核脅威イニシアチブからの2018年のレポートでは、懸念が詳細に説明されています。 1833]。  
 主なリスクは、誤った警告または誤算による使用です。ネットワークから電力網まで、外部の依存関係もあります。  
 このような問題は、トランプ政権の2018年核姿勢レビューで認められています。  
また、サイバー作戦における対戦相手の能力が、自分の抑止力の有効性を低下させたり、自分の能力がライバルへの攻撃の危険性を低下させたりするかもしれないという自信過剰につながる恐れもある。  
 これが実際に真実であったかどうかに関係なく、そのような感情は権力の回廊で表明された場合、抑止力を弱め、核紛争をより起こりやすくする可能性があります。  
S  
そしてそれは宣言された核保有国だけではありません。  
 これらの国のうち、15か国にはサイバーセキュリティ法さえありません。エネルギー会社は、規制当局から指示がない限り、一般にサイバーセキュリティに投資しませんが、一部の企業（および国）には実際の能力はありません。  
 2009年に濃縮ウランの生産量は30％減少し、2010年にはウイルスが発見されました。  
7。  
 米国政府の関与は2012年に最終的に認められました[1028]。  
7。  
 1つの例は、核数学削減条約で発見された可能性のある攻撃であり、暗号数学の新しい分野（サブリミナルチャネルの研究）の開発につながり、著作権マーキングとステガノグラフィーに関する後の研究に関連しています。  
カーター政権下で、アメリカはソ連との協定を提案し、両国は大陸間弾道ミサイルの数を検証するために互いに協力することになった。  
 したがって、ソビエトは1,000サイロすべてを破壊しなければならなかったでしょう。  
 問題は、この1ビットの情報しか送信できないことでした。ロシア人がメッセージにこれ以上情報を密輸できる場合、彼らは完全なサイロを見つけることができます。フィールドで単一のサイロを指定するのに10ビットのアドレス情報しか必要としないためです。  
）サブリミナルチャネルがどのように機能するかを確認するには、暗号化の章で説明されているデジタル署名アルゴリズムを検討してください。  
 メッセージMの署名はr、sで、r =（gk（mod p））（mod q）であり、kはランダムセッションキーです。  
これにより、セキュリティプロトコルに致命的な障害が発生した可能性があります。  
 最終的に中距離弾道ミサイル条約（MRBM）は統計的手法を使用しました。  
 冷戦の終結とともに、衛星ではなく、両側からオブザーバーがいる有人航空機の検査飛行において、検査ははるかに親密になった。  
 虐待の悪用の方法には、HIVステータスまたは重罪の有罪判決の事実をデジタルパスポートまたはIDカードに入れることが含まれます。  
8。  
15。  
1930年代には、多くの国の物理学者が爆弾の科学的アイデアを自由に共有していましたが、「原子スパイ」（フックス、ローゼンバーグなど）が広島と長崎のデバイスの設計をソビエト連邦に漏らした後、もう一方の極端。  
 つまり、あなたが米国の管轄権の範囲内にあり、核兵器に関連する考えを持っている場合は、セキュリティクリアランスを持っているか、核産業で働いていたかに関係なく、秘密にしておかなければなりませんでした。その後、保護の問題が詳細に検討されたため、事態は大幅に緩和されました。  
 「どのレベルで分類する必要がありますか？誰が盗むのですか？ロシア人、彼らは彼らのためにそのデータを手に入れました。  
 ガダ？彼はそれで何をするのでしょうか？」このような問題が解決されたので、多くの技術は、少なくとも概略的には、機密解除されて公開されました。  
施設の50の建物のうちどれに警報対応部隊が含まれているかなど、妨害行為を助長する可能性のある情報を含め、多くの実装の詳細は秘密に保たれています。  
 偶発的な戦争の可能性を減らすことの利益は、秘密の可能な利益を上回ると考えられていました。  
 これは、システムのセキュリティがそのキーに依存しなければならない、システムのセキュリティがその曖昧なままではないという104世紀の格言であるケルホースの教義の現代の生まれ変わりです[1042]。  
 9/11以降、多くの政府が生物兵器を使用したテロリストの可能性について話し合い、細菌学、ウイルス学、毒物学、そして実際の医学における研究と教育に規制を課しました。  
 「炭疽菌について心配するべきではありません」と英国のトップウイルス学者の一人が私に言った。  
 これらのポリシーにより、次にウイルスが感染したときにハルツームに有能な公衆衛生関係者がいない場合、セキュリティエンジニアリング499ロスアンダーソン15。  
 概要ナイル、申し訳ありません。  
15。  
コストに関係なく、武器と核分裂性物質をほとんど保護しなければならないという合理的な決定により、他の場所で応用されている多くの数学と科学の発展が促進されました。  
 この本の残りの部分には、アラームからアイリスバイオメトリクス、不正開封防止の電子機器からシールまで、他の例が散在しています。  
 サイバー攻撃が国の諜報能力、監視能力、偵察能力を狙って抑止力への信頼を損なう可能性がある場合でも、深刻な不安定化が続く可能性があります。  
 また、1945年以来、米国の大統領が核の脅威を十数回使用していることを考えると（キューバ、ベトナム、イラクは、より明白な例に過ぎません）、各世代にいくつかのそのような危機が予想されるでしょう。  
』第2版では、ブロック暗号のガロアカウンターモードの動作が標準化され、現在では普及しています。  
2009-10年のイランのウラン濃縮計画に対する米国/イスラエルの攻撃は、核の世界で使用されているサイバー攻撃の例を世界に与えました。  
9。  
 核兵器に関する公開情報の最も優れた情報源の1つは、アメリカの科学者連盟であり、爆弾の設計から多くの核兵器技術の分類解除の根拠まですべてについて話し合っています[672]。  
ガスシモンズはサッカーをデザインしたサンディアの男でした。彼は認証コード、共有制御スキーム、サブリミナルチャネルのパイオニアでした。  
 認証と秘密分散の両方のより簡潔な紹介は、Doug Stinsonの教科書[1829]にあります。  
 ロシアのインストールに関する問題は[953]で議論されています。原子力規制委員会[1455]による米国の原子力の安全性。英国の設備の欠点は、Healthand Safety Executiveが投稿した四半期レポート[874]に記載されています。  
 「シリコンとプルトニウムの間の」相互作用については、チャタムハウスからの主題に関する最近の報告があります[27]。