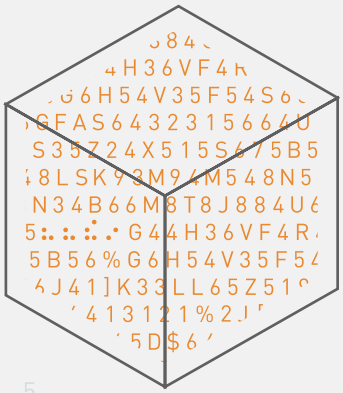


ホワイトボックス暗号方式とは何か

WHITEPAPER

従来の暗号方式では、内在する脆弱性を悪用しようとする多様な攻撃シナリオに十分対応できる防御ソリューションは提供できません。

序論

これまでの暗号方式は、機微な（機密、極秘、または個人の）情報をメッセージの受信者以外が理解できないようにして通信する手段を提供してきました。古代聖書の時代に使われていた暗号方式では、元の内容を隠す手段としてメッセージ内の文字列を手動で置き換える手法が使われていました。長い年月を経て第二次世界大戦に至り、暗号方式は電気機械式暗号機（悪名高いエニグマ暗号機など）が広く使われるようになりました。近年、暗号方式は強固な数学的基礎に支えられたコンピュータに大きく依存し、かつてないほど普及しています。

暗号方式は、その名が示すように、さまざまな手法を使用して文字列の一部を悪意に満ちた目から隠そうとします。理論的には、そのコンセプトは理想的に思えますが、現実には暗号鍵の強度に悪影響を与える多数の要因や環境が関わることが示されています。従来の手法では、暗号方式に内在する脆弱性を悪用しようとする多様な攻撃シナリオに十分に対応できる防御ソリューションは提供できません。

コンピュータシステムやネットワークの信用性と信頼性の分野に携わる Peter G. Neumann 教授は、次のように述べています。「暗号方式が問題に対する答えであると考えている人は、問題が何であるかを分かっていない」[1]

本書では、ホワイトボックス暗号方式の実装に焦点を合わせながら、従来の手法について解説します。

1. Peter G. Neumann、『New York Times』（2001 年 2 月 20 日）に記載

暗号方式の詳細

一般的な DRM（Digital Rights Management：デジタル著作権管理）の実装では、暗号アルゴリズムは既知の強力なアルゴリズムを採用したセキュリティソリューションの一部となっており、暗号鍵の機密性に依存しています。多くの場合、これは極めて不適切です。こうしたアプリケーションの大多数が実行されるプラットフォームは、潜在的に敵対的なエンドユーザーの制御下にあるからです。

暗号方式の従来の前提は、攻撃者は暗号鍵にアクセスできず、暗号インプット（平文）を制御することと結果のアウトプット（暗号文）にアクセスすることだけできると仮定しているブラックボックスでした。長い間、スマートカードなどのハードウェアデバイスについても、これが真であると仮定されてきましたが、ブラックボックスから「流出する」情報を悪用する悪意ある攻撃（Differential Power Analysis（差分電力解析）攻撃など—DPA としても知られる）が開発され、ハッカーはブラックボックス内で使用される秘密鍵を導き出せるようになってしまいました。この手法は、ハッカーがブラックボックスを無効化する攻撃を事実上可能にし、結果としてこれらの実装をブラックではなく「グレー」に変えます。[2]

2. Amitabh Saxena、Brecht Wyseur、および Bart Preneel、『Towards Security Notions for White-Box Cryptography』

AES などの有名な業界標準の暗号は、実行の観察が可能な環境で使用される前提で設計されていませんでした。事実、標準の暗号モデルは、たとえばエンドポイント、PC、ハードウェア保護トークンが信頼できるものであると仮定しています。

ホワイトボックス暗号方式の必要性

AES などの有名な業界標準の暗号は、実行の観察が可能な環境で使用される前提で設計されていませんでした。事実、標準の暗号モデルは、たとえばエンドポイント、PC、ハードウェア保護トークンなどが信頼できるものであると仮定しています。もし、そのエンドポイントが潜在的に敵対的な環境に置かれていた場合、アプリケーションを監視している攻撃者は暗号鍵を直接目にすることができ、アプリケーションによって生成または埋め込まれた鍵をメモリから抽出しようと試みる可能性があります。これは、DRM を施行しようとする PC、IPTV セットトップボックス、その他のデータ消費デバイス上で実行するソフトウェアベースのアプリケーションにとって共通の問題です。標準の暗号 API またはメモリダンプを積極的に監視することで、ハッカーは使用される鍵をいつでも抽出できてしまいます。メモリベースの鍵抽出攻撃が成功した例としては、BackupHDDDVD ツールによって、保護された DVD のコンテンツをコピーして Windows 保護メディアコンテンツから DRM を削除できたことが挙げられます。

ホワイトボックスのジレンマ

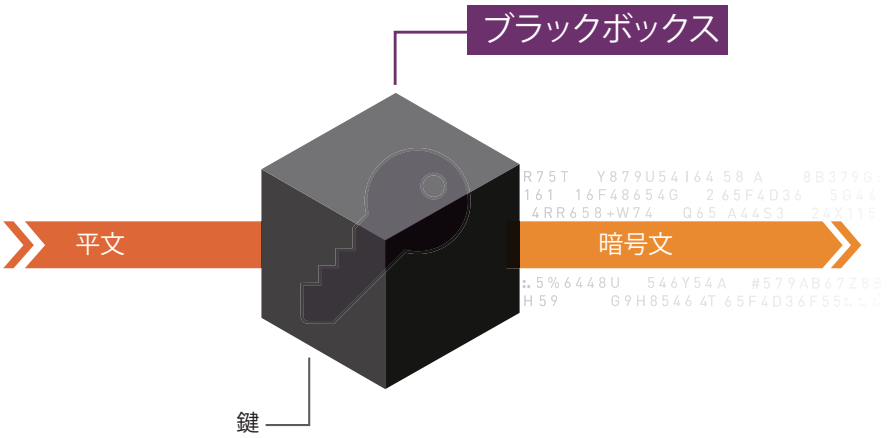
ライセンシングやその他の企業秘密などの貴重な情報を隠したままの状態で、完全に透過的な環境で操作を実行するという概念は、さまざまなジレンマを引き起こします。

- 鍵やデータのいかなる部分も直接公開することなく、どのようにしてコンテンツを暗号化したり復号化したりするのか？
- ハッカーがコードを実行時に観察または改変できる可能性があることを前提にしながら、どのようにして強力な暗号メカニズムを実行するのか？

さまざまな暗号モデル

ブラックボックス（従来の）暗号方式

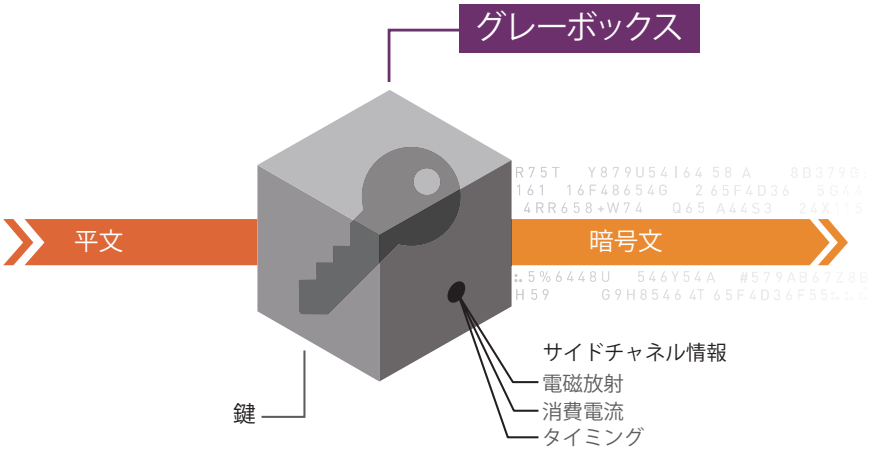
従来のモデルであるブラックボックスのシナリオでは、攻撃者が鍵（暗号化または復号化を実行するアルゴリズム）や内部の仕組みに物理アクセスできず、外部情報や動作しか観察できないことを仮定しています。この情報は、システムの平文（インプット）または暗号文（アウトプット）のいずれかで構成され、コード実行および動的な暗号化操作に対する可視性がゼロであると仮定しています。



グレーボックス暗号方式

グレーボックスのシナリオでは、攻撃者が鍵に部分的に物理アクセスできる、またはいわゆるサイドチャネル情報が「流出している」ことを仮定します。サイドチャネル解析（SCA）攻撃は、暗号システムの物理的実装から流出した情報を悪用します。流出は、タイミング情報、電力消費、電磁放射などを介して受動的に観察されます。サイドチャネル攻撃は低コストですばやく実行できてしまうため、この攻撃に対する防御は重要です。公表されているサイドチャネル情報によって、ハッカーは鍵の一部を事実上明らかにすることが可能になり、結果としてその効果は激減し、セキュリティ全体が低下します。[3]

グレーボックス暗号方式は、実際は従来のブラックボックス実装の副産物です。内部の暗号方式を実行して強力なセキュリティを提供できると認識されているスマートカードでさえ、実際には外部に情報を流出していることが証明されています。ブラックボックスであると思われているシナリオが実際にはグレーでしかないということは明らかです。



ホワイトボックス暗号方式のコンセプト

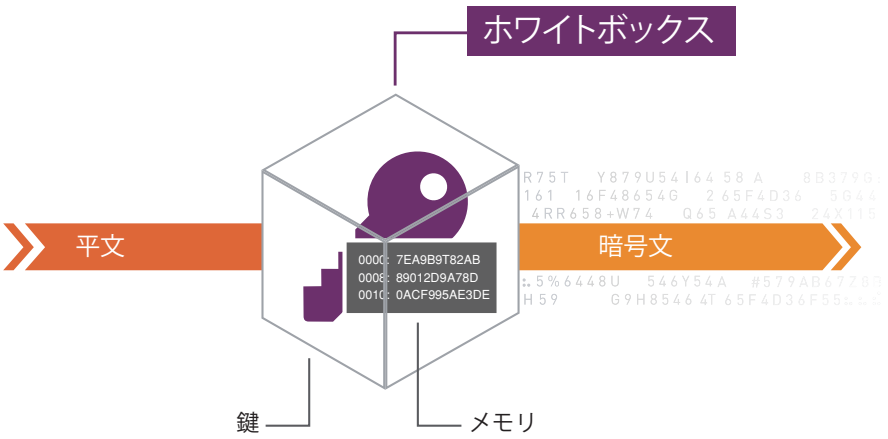
ホワイトボックス暗号方式は、上記の従来のセキュリティモデルに真っ向から対処しました。攻撃者にブラックボックス、すなわちインプットとアウトプットへのアクセスと暗号アルゴリズムへのアクセスしか与えず、内部の仕組みに対する可視性がゼロであると仮定された以前の実装とは対照的に、ホワイトボックスは完全な可視性を提供しました。

ホワイトボックス暗号方式は、暗号化を実行するマシンを攻撃者が自由に制御できる場合でも、暗号アルゴリズムのソフトウェア実装を鍵回復から保護することを目的としており、特に DRM の分野で役立ちます。

ホワイトボックス暗号方式

ホワイトボックスのシナリオは、上記の従来の方式とは対照的に、攻撃者が完全な可視性を持って操作全体を制御できると仮定し、はるかに重大な脅威に対処します。ハッカーは、動的なコード実行（インスタンス作成された暗号鍵を含む）を自由に観察でき、内部アルゴリズムの詳細は完全に目に見える状態で、自由に改変できます。このように完全に透過的な方式であるにもかかわらず、ホワイトボックス暗号方式は、鍵を公開しないように暗号文を統合する方法で構築されています。

3. S. Chow、P. Eisen、H. Johnson、P.C. van Oorschot、『A White-Box DES Implementation for DRM Applications』



ブラックボックスやグレーボックス用のアルゴリズムは、信頼できないホスト上で動作する際に実効力がないことが明らかです。当然のことながら、ハッカーはブラックボックスとグレーボックスのシナリオで可能な手段のみを使用して暗号を解読しようとするのではなく、保護されていない鍵が使用されるときの実行を監視して、鍵を直接盗もうとします。

そのため、最も適切で最もセキュアな暗号モデルを選択することが、悪意のある脅威に対する唯一の防衛線です。これこそが、まさにホワイトボックス暗号方式が達成しようとしていることです。

ホワイトボックス実装の方法論

攻撃者がありとあらゆる命令を完全に監視して改変できると仮定して、どのように実行コード内の鍵を安全に「隠す」ことができるでしょうか？

抽象的に言うと、これは数学的な操作を用いて実装固有のデータと秘密鍵の効果を組み合わせることで達成されます。この数学的な操作により、逆をたどることが実質的に不可能となります。[4]

例として、RSA の本来の強度は、大きな数への単純な乗算によって決まります。これは、その結果を素因数分解することが数学的に難しいことに基づいています。

また、同じく重要なこととして、ホワイトボックス暗号アルゴリズムの実装が、単に暗号化または復号化のいずれかを実行できるだけということがあります。

アルゴリズムの実装は、前述のとおり、逆をたどることが極めて困難な数学的な操作に基づいています。この事実により、完全な公開鍵 / 秘密鍵スキームと同じように機能するシステムを構築することが可能となりますが、実行レベルでは標準の対称暗号にはるかに近いものとなります。

復号化機能は分散アプリケーションの内部に実装できますが、鍵を抽出することも、暗号操作を実行するために復号化の逆をたどることも不可能です。攻撃者には、目的の値に復号化できるような正しい暗号化データを作成する手段はありません。

この特別な手法は特に、ハードウェア保護トークンなどのハードウェアデバイスで保護された通信チャネルの安全性を確保するために役立ちます。攻撃者は、セキュアな通信チャネルに使用される鍵を抽出できないため、チャネルを通過するデータを復号化できず、データを正しく暗号化する手段もないため、チャネルにデータを注入することもできません。

4. Amitabh Saxena、Brecht Wyseur、および Bart Preneel、『Towards Security Notions for White-Box Cryptography』

設計の一環としてのジレンマ

最初にジレンマとして記述しましたが、ホワイトボックス暗号方式は、すべてのカードをシャッフルし、完全に透過的な環境で動作しつつ暗号化を実行する高度にセキュアな手法を提供します。完全に透過的ですが、暗号化操作と復号化操作のどちらも、鍵またはデータ自体のいかなる部分も公開することなく機密データを維持できるようにします。またホワイトボックスは、強力な暗号化メカニズムの実行（他の手法と連動）を許可し、一方で実行時のコードを悪意に満ちた目が観察する可能性があることを前提にしています。

SafeNet のセキュリティ対策に不可欠な要素

SafeNet の Sentinel 製品で提供されるセキュアな通信チャネルは、保護されたアプリケーションとハードウェアトークン間の通信が暗号化され、再現が確実に不可能であるようにします。暗号鍵を隠そうとする以前の実装とは異なり、新しい実装はホワイトボックス暗号方式に基づいています。ここでは、攻撃者が暗号鍵を求めて、保護されたアプリケーションやランタイムを追跡できると仮定されています。設計の一環としてこのような仮定をすることにより、アルゴリズムと暗号鍵は、同じ暗号化を実装するベンダ固有の特別なライブラリに置換されますが、暗号鍵はメモリ内に決して存在しないようにする方法でアルゴリズムの一部として組み込まれます。そのため、暗号鍵を抽出することはできません。ベンダ固有のライブラリの生成は、いくつかの企業秘密を実装しながら SafeNet のサーバー上で実行されます。また各アプリケーションライブラリは個別に生成され、特定のソフトウェアベンダ向けに難読化されます。これにより、一般的なハッカー行為は実質的に不可能になります。

真に革新的なソリューション

SafeNet は、ソフトウェアライセンシングソリューションの Sentinel ポートフォリオに不可欠な要素としてホワイトボックス暗号方式を提供する世界初の唯一のベンダです。この新技術により、暗号鍵を分割して一度に一部を公開するのではなく、常に暗号鍵を保護することが可能になります。セキュリティの観点からも、保護された鍵が確実にハッカーの目から隠されたままの状態になるため、潜在的な攻撃プロセス時における再構成の影響を受けません。

ホワイトボックス暗号方式は、開発者がリバースエンジニアリングや改ざん、自動化された攻撃からアプリケーションを保護できるようにするため不可欠な新たな要素です。SafeNet のホワイトボックス暗号方式は、ソースコードレベルで直接追加の保護層を埋め込めるよう、ソフトウェア設計プロセスに統合されており、ソフトウェア保護に極めて効果的で調整可能なアプローチを提供します。

最後に

保護されたアプリケーションのセキュリティ全体が、その実装自体に大きく依存しています。単に強力な暗号アルゴリズムを採用するだけでは、設計の前提にない使われ方をした場合、セキュリティが効力を失います。ホワイトボックス設定のホワイトボックスアルゴリズムを使用しないというのは、致命的です。これまで最も一般的な攻撃は、暗号アルゴリズムの弱点ではなく、ソフトウェアのセキュリティフロー（欠陥）を悪用しようとするものでした。しかし最近では、攻撃者はオープンな PC 環境の従来型暗号方式の脆弱性を認識しています。

ソフトウェア保護は、製品のライフサイクルや新バージョンのリリースの一環として微調整されるだけでなく、設計段階と実装段階の全体にわたって注目すべきであることが暗黙の前提となっています。ホワイトボックス暗号方式に加え、さらなる補助的なセキュリティ対策を取ることにより、保護スキーム全体を一層強化する必要があります。

セキュリティはコストがかかる上に、直接的な結果として完璧にすることはできません。したがって、アプリケーション自体によって決まる必要なセキュリティレベル、すなわち保護すべきものの価値と、潜在的なリスクを無視することで被る損失を正しく評価することが極めて重要です。

リンクサイト：

Sentinel Online
safenet-inc.com/sentinel

Twitter
twitter.com/LicensingLive

LinkedIn
http://bit.ly/LinkedInLicensingLive

YouTube
youtube.com/user/LicensingLive

LicensingLive
licensinglive.com

BrightTalk
brighttalk.com

参考資料

追加情報や詳細な技術公表文献は、下記のリンクでご覧になれます。

1. Towards Security Notions for White box Cryptography
   http://www.cosic.esat.kuleuven.be/publications/article-1260.pdf
2. White box Cryptography: Formal Notions and (Im)possibility Results
   http://eprint.iacr.org/2008/273.pdf
3. White box (software engineering) on Wikipedia
   http://en.wikipedia.org/wiki/White_box_(software_engineering)
4. What is a white-box implementation of a cryptographic algorithm?
   http://crypto.stackexchange.com/questions/241/what-is-a-white-box-implementation-of-a-cryptographic-algorithm
5. Portable Executable Automatic Protection, Wikipedia
   http://en.wikipedia.org/wiki/Portable_Executable_Automatic_Protection

SafeNet Sentinel ソフトウェア収益化ソリューション

SafeNet は、世界中のソフトウェアベンダとテクノロジーベンダに、革新的で信頼できるソフトウェアライセンシングおよびエンタイトルメント管理ソリューションを 25 年以上も提供してきました。

統合しやすく使いやすい、革新的な機能重視の Sentinel® ソフトウェア収益化ソリューションは、規模や技術要件、組織構造を問わず、どんな組織に対しても固有のライセンス有効化、施行、管理要件を満たすように設計されています。全体の収益性を向上させ、社内業務を改善し、競争力を維持し、顧客やエンドユーザーとの関係を深めつつ、著作権侵害対策、IP 保護、ライセンス有効化、ライセンス管理の課題、あらゆるソフトウェア収益向上に関する課題に SafeNet はお客さまとともに取組んでいます。SafeNet には、進化し続けるマーケットに対応するため、新たな要件に適応し新たなテクノロジーを取り入れてきた実績があります。世界中の 25,000 以上のお客様が、Sentinel を選択することが、今日、明日、そしてその先のビジネスのやり方を発展させていく自由を手に入れることだと考えています。

SafeNet について

SafeNet は、1983 年に設立された、情報セキュリティ業界における世界的なリーダー企業です。SafeNet は、お客様の貴重な資産である ID や、トランザクション、通信、データ、ソフトウェアライセンスを IT セキュリティの視点から、情報ライフサイクル全般にわたり保護しています。SafeNet のお客様は、100 カ国以上、2 万 5 千を超える企業や政府機関に及び、その情報セキュリティの保護を SafeNet に委ねています。

日本セーフネットについて

日本セーフネット株式会社（http://jp.safenet-inc.com 代表取締役社長：酒匂 潔、本社：東京都港区）は、米国 SafeNet, Inc. の日本法人で、2001 年の設立以来、ネットワークやアプリケーションのセキュリティ製品の日本国内での販売、マーケティング、サポートを提供しています。

本ホワイトペーパーの内容、製品・ソリューションについてのお問合せは下記までお願いいたします。

日本セーフネット株式会社

SRM ソリューション事業部

東京都港区新橋 6-17-17

御成門センタービル 8F

Tel: 03-5776-2751

Email: SalesRM-Japan@safenet-inc.com