Super Security Solutions

6_ 最近よく論議されるSSLの弱点
弊社情報セキュリティー技術で解消

デファクトスタンダードになったSSL、最近では常時接続/鍵長さも、安全性向上の為4096bitと長くなる傾向にある。
しかし、下記の問題点が指摘されています
1. 鍵長さが長くなればなるほど、スピードの問題がクローズアップされてきた
2. SSLで有ることを逆手にとって、標的型攻撃で内部のネットワークに侵入し機密情報をサーバーに通信する際SSLを悪用して、問題の無いトラフィックに偽装、検知されない問題が報告されている
3. 従来からのSSLの脆弱性

弊社の技術Pointは3点：新しい安全なプラットホームの構築

1.ID/Pass wordに依存しない認証技術

2.共通鍵8192bitを用いた、高強度乱数化VPN

3.たとえ漏洩しても、解読不可能な秘密分散/平文の1.5倍（通常技術は3倍程度）

支える技術は超小型/超高速/超安全な暗号技術

2016年9月08日
株式会社スーパーセキュリティーソリューションズ

INOVERITA®

SSLスピード問題

1. スマートフォンの急激な普及に伴い、Free Wi-Fiの問題点が表面化し、常時SSL接続が顕在化してきた。Googleもwebサイトにおいて、SSLを優遇する方向を打ち出している。通常の80番ポートを遮断443ポートのみにするという動きがあるようだ。

2. SSLの安全性の強度を高めるために、鍵の長さを4096bit長さまで長くする動きもある

3. もともと、SSLはブロック暗号であり、パケット単位で複雑な計算を行なうことにより安全性を担保している。

上記の現象から容易に推測できることは、

1. スマートフォンの急激な増加による、トラフィックの増加にシステムが追いついていない

2. 鍵長さを長くすることにより、暗号の計算に必要とする時間も長くなっている

⇒結果、SSLのスピード問題が表面がしている

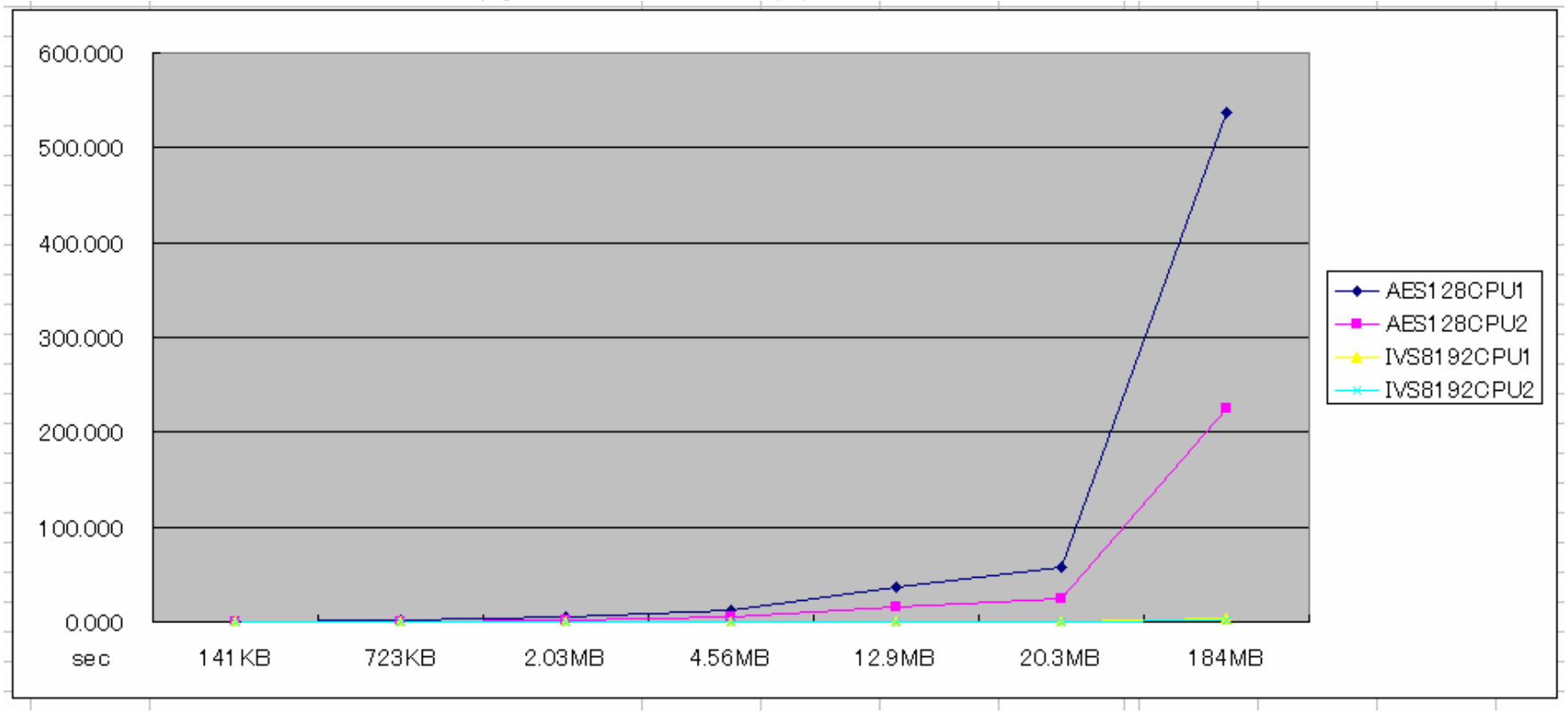
NIST(米連邦情報技術局)のPublication 800-131によって、1024 ビットから2048 ビットへのSSL 鍵長の移行に拍車がかかっていますが、その影響は衝撃的です。NSS Labs のアナリストは、2048ビットのSSLで暗号化されたトラフィックの復号化によって、7 つの主要な次世代ファイアウォールで「平均81% のパフォーマンス低下が発生した」ことを明らかにしました。ファイアウォールをSSL復号化のためにも利用しようとする組織は、ファイアウォールへのパフォーマンスの影響を考慮しなければなりません。

出所:A10ホワイトペーパー

次ページに弊社の独自暗号技術と、SSLに使用される暗号技術である、AESの暗号化の時間を測定したグラフを掲載する。あくまでも弊社調べであることを御理解ください。

Super Security Solutions

弊社独自暗号技術のスピード



IVS8192・・・弊社暗号技術で、鍵長さは8192bit

AES128・・・AES暗号方式で、鍵長さは128bit

【条件】

1. CPUは

①一世代前の CPU:1.6Ghz Dual core/4GB Memory②現状機種の CPU:3.3Ghz Core i7 12 core 相当/24GB Memory

2. 同じ容量の7種類のFileでそれぞれの暗号方式で、暗号化のスピードを計測

INOVERITA®

Super Security Solutions

SSL悪用、成りすまし問題

SSLはデファクトスタンダードであるがゆえに、安全神話がまかり通る、みんな安心してしまう。
SSLパケットが素通りする(IPS/IDSで脅威を発見できない)ことを利用する攻撃が増加している。

対処の方法として、

1. SSL暗号化検査プラットフォームなるものが製品化されているようである
送受信される全てのSSL化されたパケットを復号化して、安全であるかどうかを判断し、検知する方法のようである。

いささか本末転倒の世に思う。安全の為にSSLを使用することを推奨しているにもかかわらず、SSL化された情報が、安全であるかを調べる機構を提供しているわけである。

それで無くとも、SSLのスピード問題を抱えている状況において、検査プラットフォームが実際に使い勝手がいいのか疑問である。

弊社の暗号技術は、全ての送受信のポートに対して強固な認証技術を割り当てる方法であり、いくらID/Passwordの成りすましを行なっても、通信を素通りさせることは無い。

集中型のFirewallではなく、分散型つまりClientベースのFirewallを提供するものである。

今回開発した、弊社独自VPNは

1. スピード問題

2. 暗号成りすまし問題

2点を解消することが可能である。

INOVERITA®

従来からのSSL脆弱性

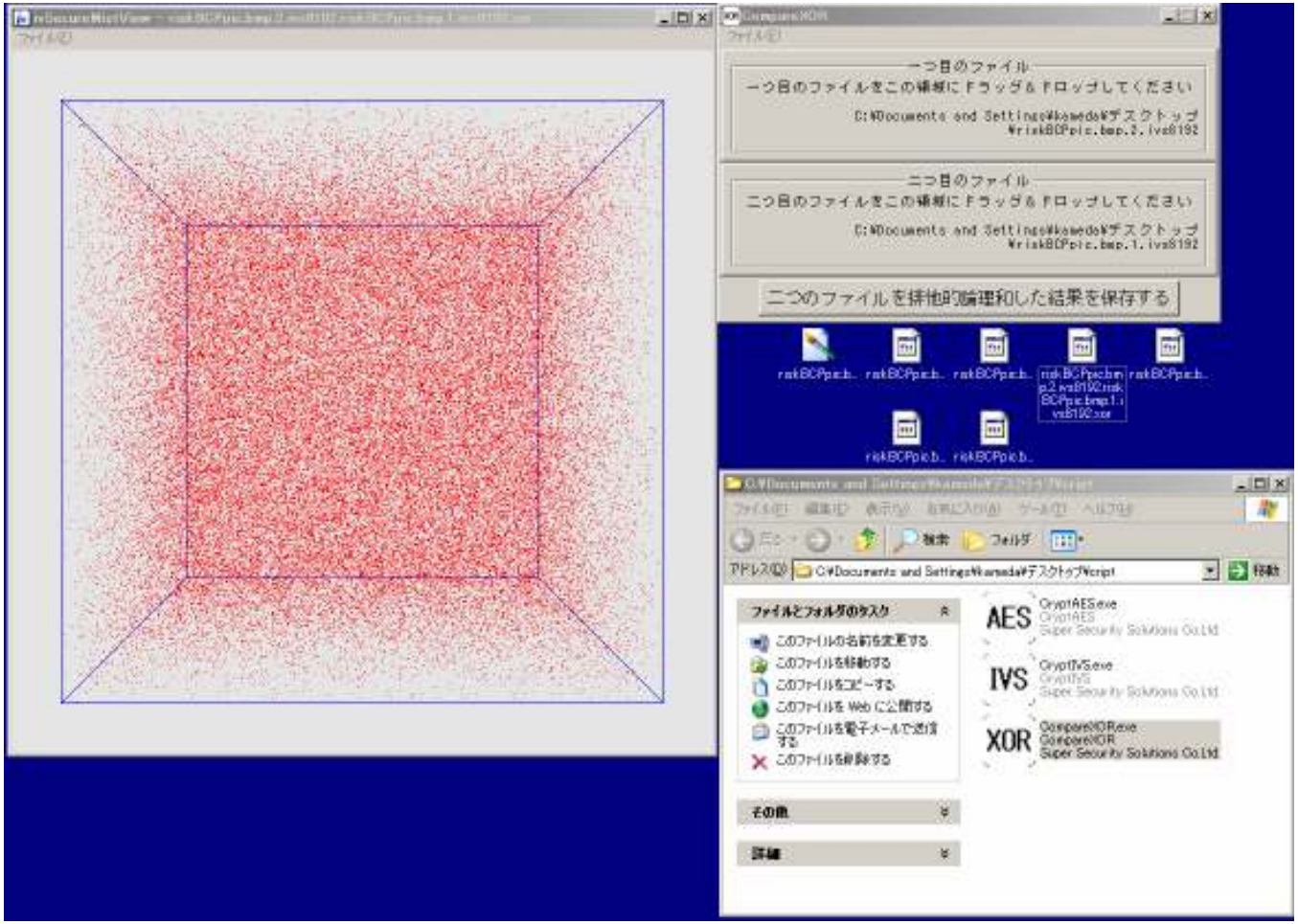
【概要】
SSLは長い歴史があり、その長い歴史の中で脆弱性が発見され現在ではSSL3.0においても脆弱性が発見されている。長い歴史の中でSSLはその脆弱性を担保する為にバージョンの更新を長年行ってきており、システム設計者は脆弱性を改善するためのパッチを常にウオッチする必要性が指摘されている。その脆弱性のSSLを否定するわけでは決して無いが、より安全性の高い暗号技術への移行を考慮すべきでは、と考える。

SSL 1.0	リリース前に脆弱性が発見され公開されず
SSL 2.0	1994年リリース
SSL 3.0	1995年リリース
TLS 1.0	1999年リリース
TLS 1.1	2006年リリース
TLS 1.2	2008年リリース
TLS 1.3	ドラフト策定中

GlobalSignブログより抜粋

Super Security Solutions

参考/弊社暗号技術・・・暗号後のbit単位分布図



弊社の暗号技術でRGBを暗号化後、R/G/B8bitをそれぞれ、X/Y/Zにプロット

偏り、傾向性が無い分布を表しています。

INOVERITA®

弊社のポリシー

前述したように、鍵の長さを長くする対策のみでは、色々な問題が指摘されている。

やはり、現状のインターネットと言うインフラを変更することなく、新しい安全なプラットフォームの構築が急務と考える。

既存技術は長い歴史があり、脆弱性が発見されると、その技術を継承して対策を講じる必要がある。
或いは既存技術の寄せ集めによる対策、インシデントが発生してからの対策のみではやはり無理があるのではないだろうか。

弊社は過去の技術を根本から見直し、プライバシーとセキュリティーの確実な保護のために、情報セキュリティーはいかにあるべきかを根本から考え、安全なプラットホーム実現のために、技術研究・開発をおこないます。

【誤解無きように】既存SSL技術を否定するものではなく、より強固/高速にする必要性を解説しているものと理解ください。

一般的にはVPNはSSL暗号化通信が使用される。しかしその暗号技術を固定するものではなく、新たな暗号技術の追加も可能である。