MicroVation

Where InnoVation happens every MicroSecond

SSL & TLS

Mythos und Wahrheit

Markus Hutter

Senior SharePoint Architect

Enterprise Solution Architect

Agenda

- Was ist SSL und TLS ?
- Aktuelle und kürzliche Bedrohungen
- Live Demo
- SSL-TLS und SharePoint
- Zusammenfassung

Agenda

- Was ist SSL und TLS ?
- Aktuelle und kürzliche Bedrohungen
- Live Demo
- SSL-TLS und SharePoint
- Zusammenfassung

SSL-TLS Basics

Die Geschichte von SSL und TLS ist eine Geschichte voller Missverständnisse und Verständnisfehler.

Beides sind Protokolle mit dem Ziel einer sicheren, verschlüsselten Kommunikation zwischen Client und Server.

Beide Protokolle sind für ihre Funktion von sog. Zertifikaten abhängig.

Die Sicherheit der benötigten Zertifikate ist ihrerseits wiederum abhängig von der genutzten Schlüssellänge sowie dem genutzten Crypto API (z.B. OpenSSL im Falle von Heartbleed)

SSL-TLS Basics

Das SSL-Protokoll existiert in den Versionen 1.0, 2.0 und 3.0, wobei die Version 1.0 nicht veröffentlicht wurde.

TLS 1.0 ist die direkte von Weiterentwicklung SSL 3.0

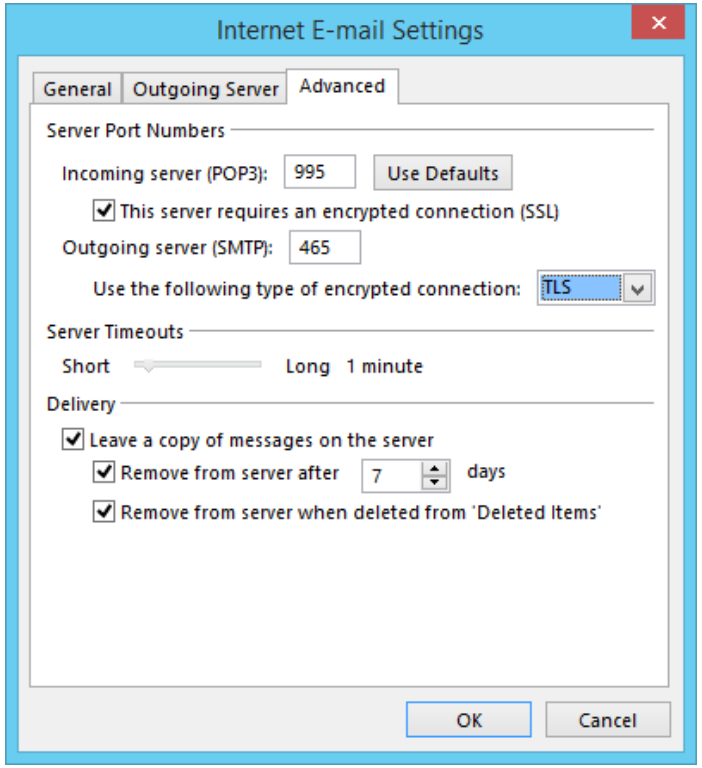
Des weiteren gibt es das TLS-Protokoll in den Versionen 1.1 und 1.2

Damit ist TLS 1.0 der Nachfolger von SSL 3.0 und wird fälschlicherweise auch häufig als SSL 3.1 bezeichnet. Fakt ist jedoch dass SSL als Protokoll tot und nicht mehr einzusetzen ist.

SSL-TLS Mythos

Besonders Email Programme und Dienste vermitteln ein falsches Verständnis von SSL und TLS

- Es wird suggeriert das eine völlig andere Technologie zwischen SSL und TLS zum Einsatz kommt.
- Die sog. Standard Ports sind übrigens nur Standard weil man es so festgelegt hat, technisch wären alle Ports möglich.



Agenda

- Was ist SSL und TLS ?
- **Aktuelle und kürzliche Bedrohungen**
- Live Demo
- SSL-TLS und SharePoint
- Zusammenfassung

You got POODLEd !!

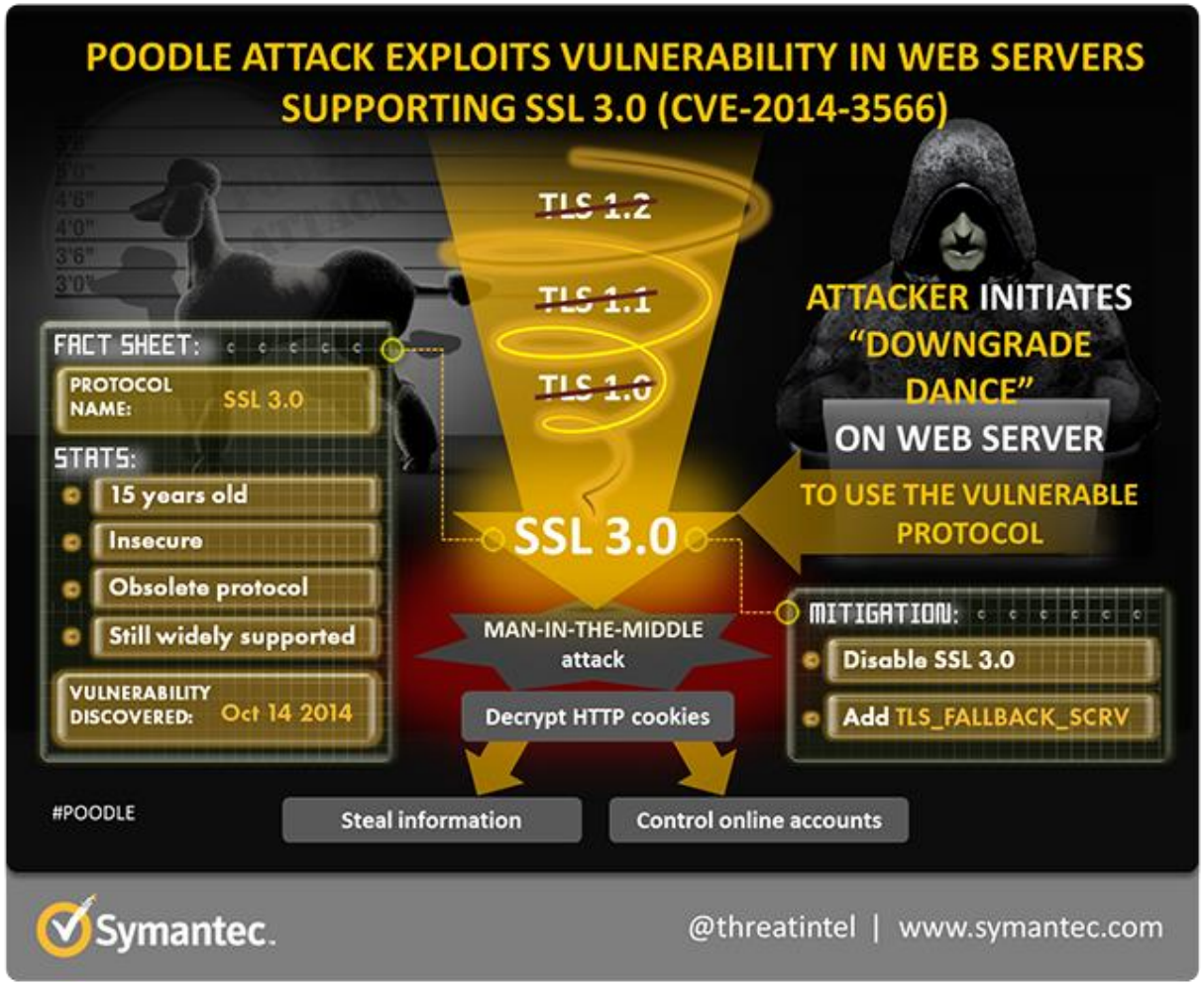
SSL 3.0

Der POODLE ist der "Man In The Middle"

Was macht diesen POODLE zum Killer ?

- Jedes System das SSL 3.0 aktiv nutzt ist betroffen!
- Einzige Gegenmaßnahme ist die Deaktivierung von SSL 3.0 und die Nutzung von TLS 1.0 und höher.
- Problemquelle ist nicht ein Linux, Microsoft oder Apple Betriebssystem, sondern die Nutzung eines 15 Jahre (!!) alten Protokolls und Entwickler und Administratoren.

You got POODLEd !!



MicroVation

Where InnoVation happens every MicroSecond

Offenes Herzbluten

Open ist nicht per se besser

Zertifikate basierend auf dem Microsoft Crypto API waren im übrigen zu keiner Zeit betroffen!

- Der Fehler befindet sich in der OpenSSL-Implementierung der Heartbeat-Erweiterung.
- Bei der fehlerhaften Implementierung dieser Funktion wird nicht überprüft, ob die angegebene Länge der Daten mit der tatsächlichen Länge der mitgelieferten Daten übereinstimmt.
- Aufgrund der fehlenden Überprüfung kann ein Angreifer mit einer Anfrage bis zu 64 KByte des Arbeitsspeichers der Gegenstelle auslesen. Der Angriff kann mehrmals hintereinander durchgeführt werden, um mehr Speicher auszulesen.

Live Demo

SSL Server Test	Server Härtung	Browser Härtung

Agenda

- Was ist SSL und TLS ?
- Aktuelle und kürzliche Bedrohungen
- Live Demo
- **SSL-TLS und SharePoint**
- Zusammenfassung

SSL-TLS und SharePoint

Ist SharePoint betroffen?

Ja!

Wann?

Immer wenn die betroffene SSL oder TLS Version zur Sicherung der Kommunikation genutzt wird.

Warum?

Weil es eine Webanwendung ist die häufig mit SSL oder TLS genutzt wird.

Das zugrunde liegende Problem ist jedoch auch hier weder die Anwendung SharePoint, noch das verwendete Microsoft Betriebssystem. Es ist das SSL 3.0 Protokoll, welches nicht unter der Kontrolle von Microsoft steht.

Agenda

- Was ist SSL und TLS ?
- Aktuelle und kürzliche Bedrohungen
- Live Demo
- SSL-TLS und SharePoint
- **Zusammenfassung**

MicroVation

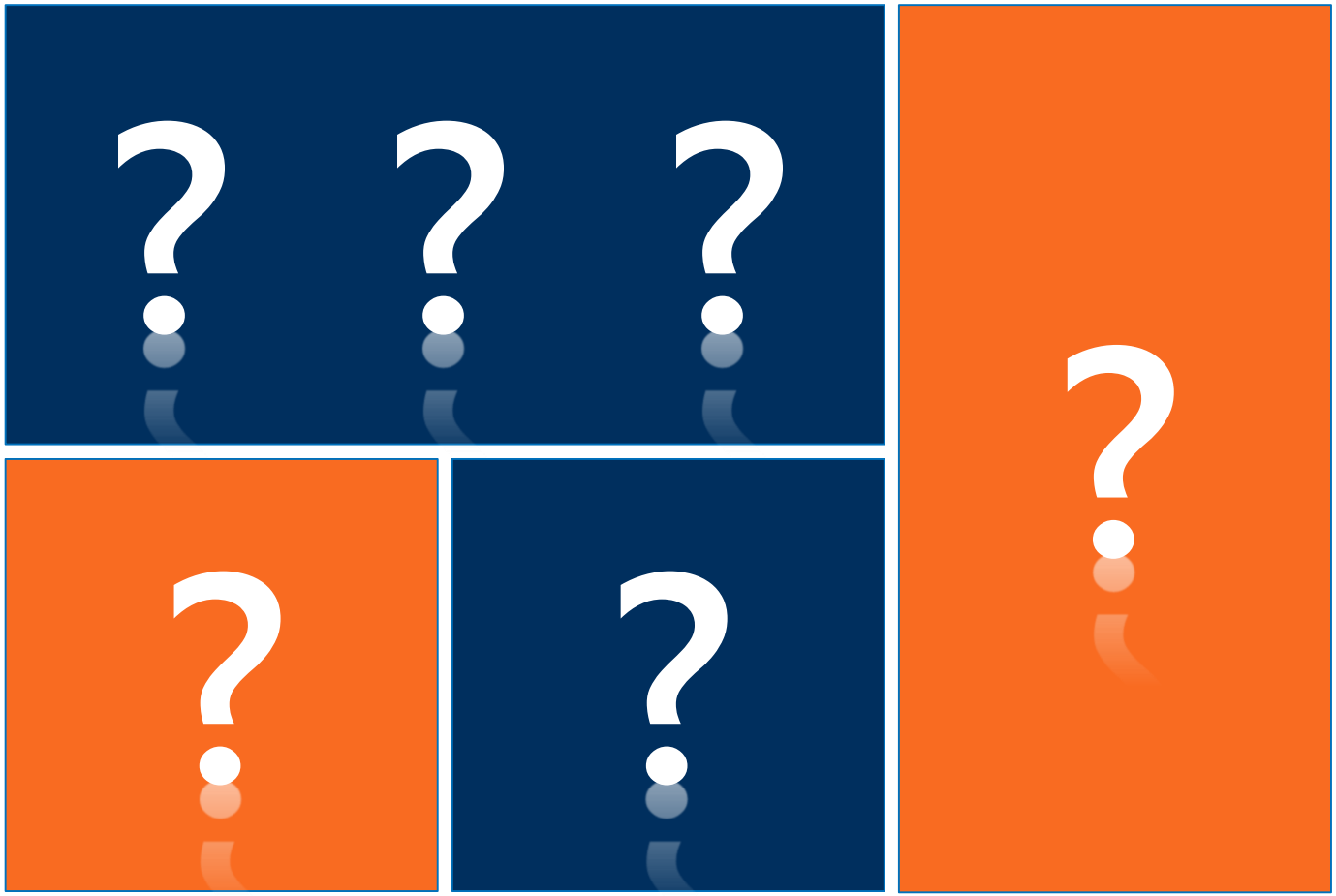
Where InnoVation happens every MicroSecond

Zusammenfassung

Die Sicherheit von Systemen ist maßgeblich von der Kompetenz und Durchsetzungskraft ihrer Administratoren abhängig.

Zertifikate sind eine tragende Säule in der modernen Verschlüsselung, aber immer nur so sicher wie das zugrunde liegende Crypto API.

SSL und TLS sind lediglich alte und neue Protokolle für den selben Zweck.



Quellen und Referenzen

- SSL Server Test
  https://www.ssllabs.com/ssltest
- Cipher Suites in Schannel
  http://msdn.microsoft.com/en-us/library/windows/desktop/aa374757.aspx
- How to restrict the use of certain cryptographic algorithms and protocols in Schannel.dll
  http://support.microsoft.com/kb/245030
- Hardening Windows Server 2008/2012 and Azure SSL/TLS configuration
  http://www.dotnetnoob.com/2013/10/hardening-windows-server-20082012-and.html

TLS 1.0
RFC2246

TLS 1.1
RFC4346

TLS 1.2
RFC5246

Vielen Dank für Ihre Aufmerksamkeit!