



Bundesverband



TeleTrust – Bundesverband IT-Sicherheit e.V.

Allianz für Sicherheit der Wirtschaft e.V. - ASW Bundesverband

TeleTrust/ASW-Workshop "IT-Sicherheit in der Wirtschaft"

Berlin, 23.09.2015

Security oder Insecurity by Design – Standardisierung und IT-Sicherheit

Tobias Kaufmann, BMWi

1. Hintergründe
2. Standards – Mit Absicht unsicher
3. Implementierungen – Mit Absicht unsicher
4. Ausblick

1. Hintergründe (1)

- IT-Sicherheit wird heutzutage über standardisierte Verfahren und Methoden ermöglicht.
- Insbesondere kryptographische Verfahren werden breit eingesetzt, um vor unbefugten Zugriffen zu schützen.
- Alltagsszenario: Online-Banking über SSL, VPN, Festplattenverschlüsselung

1. Hintergründe (2)

- 2013: Snowden
 - NYTimes: *“Simultaneously, the N.S.A. has been deliberately weakening the international encryption standards adopted by developers. One goal in the agency’s 2013 budget request was to **“influence policies, standards and specifications for commercial public key technologies,”** the most common encryption method.”*
- Die NSA schwächte gezielt internationale Krypto-Standards
- In Zusammenarbeit mit dem NIST wurden entsprechen „beeinflusste“ Standards zur Nutzung empfohlen

The New York Times



Quelle:

http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0

1. Hintergründe (3)

■ RSA Security

- WallStreetJournal: *„RSA Security, a division of EMC, privately told customers Thursday to ditch an encryption algorithm that reportedly contains a flaw engineered by the National Security Agency. It marks one of the first instances of a security company acknowledging the U.S. government may have been involved in propping open a backdoor into a product.”*
- *“The type of encryption – a particular random number generator endorsed by the U.S. government – previously has been shown to be vulnerable to hacks. But documents recently leaked by former NSA contractor Edward Snowden suggested the U.S. intelligence agency had played a role in creating a backdoor in the standard.”*



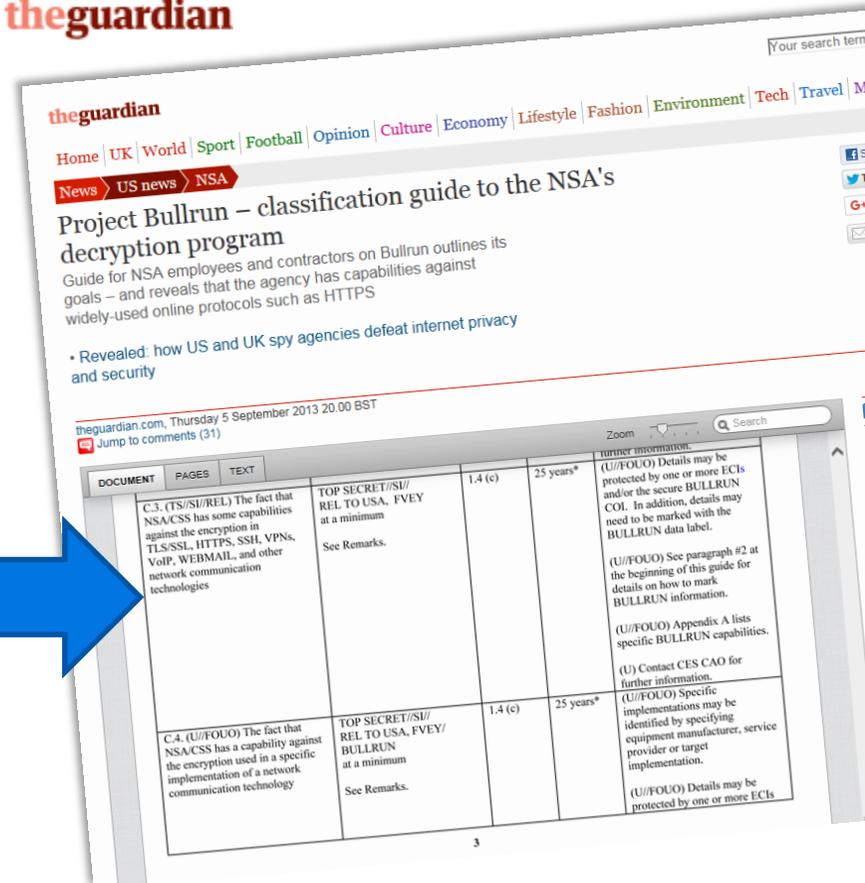

Quelle:

<http://blogs.wsj.com/digits/2013/09/19/rsa-dont-use-encryption-influenced-by-nsa/>

1. Hintergründe (4)

- NSA Project Bullrun
- The Guardian: *“Guide for NSA employees and contractors on Bullrun outlines its goals – and reveals that the agency has capabilities against widely-used online protocols such as HTTPS”*
- Aus dem Inhalt:
*“The fact that NSA/CSS has some capabilities against the encryption in **TLS/SLL, HTTPS, SSH, VPNs, VoIP, WEBMAIL, and other network communication technologies**”*

theguardian



theguardian.com, Thursday 5 September 2013 20.00 BST

Jump to comments (31)

DOCUMENT	PAGES	TEXT
C.3. (TS//SI//REL) The fact that NSA/CSS has some capabilities against the encryption in TLS/SSL, HTTPS, SSH, VPNs, VoIP, WEBMAIL, and other network communication technologies	TOP SECRET//SI//REL TO USA, FVEY at a minimum See Remarks.	1.4 (c) 25 years* (U//FOUO) Details may be protected by one or more ECI's and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.
C.4. (U//FOUO) The fact that NSA/CSS has a capability against the encryption used in a specific implementation of a network communication technology	TOP SECRET//SI//REL TO USA, FVEY/ BULLRUN at a minimum See Remarks.	1.4 (c) 25 years* (U//FOUO) Specific implementations may be identified by specifying equipment manufacturer, service provider or target implementation. (U//FOUO) Details may be protected by one or more ECI's

Quelle:
<http://www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide>

- Gezielte Schwächungen von IT-Sicherheitsstandards besteht aus zwei Teilen:
 1. Standards der Kryptoalgorithmen
 2. Standards der Kommunikationssicherheitsprotokolle

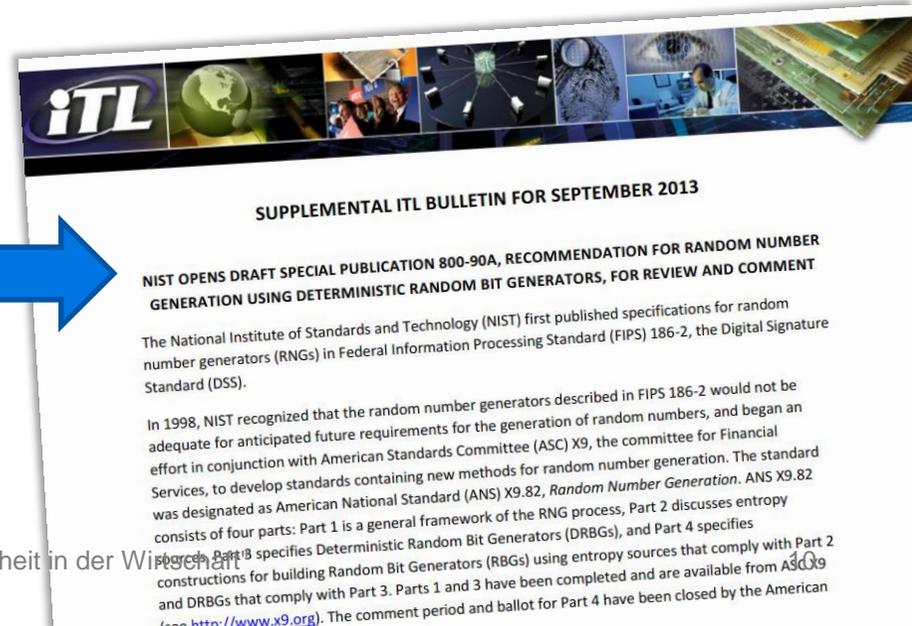
- Gezielte Schwächungen von IT-Sicherheitsstandards besteht aus zwei Teilen:
 1. Standards der Kryptoalgorithmen
 2. Standards der Kommunikationssicherheitsprotokolle

- Gezielte Schwächungen von Kryptoalgorithmen (Methodik):
 - Kryptoalgorithmen bilden die Basis der IT-Sicherheit
 - Ist der Algorithmus fehlerhaft/gezielt geschwächt, steht das System an sich vor Sicherheitsproblemen
 - Kryptoalgorithmen \neq IT-Sicherheit
 - Falls der Algorithmus keine gezielten Schwächen hat, kann das System an sich trotzdem IT-Sicherheitsprobleme beherbergen (z.B. Fehler im Kommunikationsprotokoll)
 - Verwundbarkeiten u.a.
 - Schlüssellänge
 - Zufallszahlengeneratoren

- Gezielte Schwächungen von Kryptoalgorithmen (Beispiel: Vorhersagbare Zufallszahlen)
- NIST Special Publication 800-90:2006 (siehe Snowden)
 - Dual Elliptic Curve Deterministic Random Bit Generation (Dual_EC_DRBG) durch NIST in 800-90:2006 spezifiziert
 - Dual_EC_DRBG danach in ANS X9.82 und ISO/IEC18031 überführt
 - Mögliche „Hintertür“ existiert:
 - NIST warnt vor der Verwendung des Dual_EC_DRBG

Quelle:

http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf



- Gezielte Schwächungen von Kommunikationssicherheitsprotokollen (Methodik):
 - Protokolle nutzen Kryptoalgorithmen um Informationen in bestimmten Umgebungen zu schützen
 - Werden sichere Kryptoalgorithmen innerhalb des Protokolls absichtlich falsch verwendet, ist das System an sich trotzdem gebrochen
 - Protokoll-Spezifikationen sollten eindeutig und mathematisch überprüfbar sein
 - Verwundbarkeiten u.a.
 - Nicht korrekte Verwendung eines Kryptoalgorithmus
 - Protokoll teilweise unsicher
 - Unsichere Schlüsselgenerierung

- Gezielte Schwächungen von Kommunikationssicherheitsprotokollen (Beispiel RADIUS):
 - Dial-in user service (RADIUS) nach IETF RFC2865
 - Das Protokoll soll einen sicheren Kanal herstellen
 - Verwendung von PAP und CHAP
 - Bruce Schneier, The Guardian:

*“The NSA deals with any encrypted data it encounters more by subverting the underlying cryptography than by leveraging any secret mathematical breakthroughs. First, there's a lot of bad cryptography out there. If it finds an internet connection protected by **MS-CHAP**, for example, **that's easy to break and recover the key**. It exploits poorly chosen user passwords, using the same dictionary attacks hackers use in the unclassified world.”* (Quelle: <http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance>)

3. Implementierungen

Mit Absicht unsicher (1)

- Gezielte Schwächungen von IT-Sicherheit durch Schwächung der Implementierung besteht aus zwei Teilen:
 1. Schwächung im Source Code
 2. Schwächung der Hardware und des Systems

3. Implementierungen

Mit Absicht unsicher (2)

- Gezielte Schwächungen durch die Implementierung (Methodik Source Code):
 - Source Code ist die Quelle von IT-Sicherheit:
 - Source Code wird erdacht und gesteuert durch Menschen
 - Source Code soll die Konzepte Standard-konform exakt wiedergeben
 - Closed-Source Code:
 - Source Code Sicherheit hängt von Managemententscheidungen ab
 - Schwachstellen können in Closed Source länger unentdeckt bleiben
 - Open-Source Code:
 - Source Code Sicherheit hängt von den Fähigkeiten der mitarbeitenden Community ab
 - Macht den Anschein, alles wäre offensichtlich
 - Schwachstellen u.a.:
 - Design
 - Konkrete Implementierungen

- Gezielte Schwächungen durch die Implementierung (Beispiel Source Code: IPSec in OpenBSD):
- Heise: „Der OpenBSD-Gründer Theo de Raadt weist in einer Mail auf eine **mögliche Hintertür in der Implementierung des IPSec-Stacks** zum Aufbau von VPNs hin. Da weitere Open-Source-Projekte den Code übernommen haben, könnte die Hintertür dort ebenfalls enthalten sein. Die Hintertür soll in den Jahren 2000 bis 2001 Eingang in den Code gefunden haben, als OpenBSD-Entwickler im Auftrag der US-Regierung den Code manipuliert haben sollen.“

(Quelle: <http://www.heise.de/security/meldung/FBI-Backdoor-in-IPSec-Implementierung-von-OpenBSD-1153180.html>)



heise Security News Hintergrund Tools Foren

Security > News > 7-Tage-News > 2010 > KW 50 > FBI-Backdoor in IPSec-Implementierung von OpenBSD?

« Vorige | Nächste »

FBI-Backdoor in IPSec-Implementierung von OpenBSD?

15.12.2010 11:19 Uhr - Daniel Bachfeld vorlesen

Der OpenBSD-Gründer Theo de Raadt [weist](#) in einer Mail auf eine mögliche Hintertür in der Implementierung des IPSec-Stacks zum Aufbau von VPNs hin. Da weitere Open-Source-Projekte den Code übernommen haben, könnte die Hintertür dort ebenfalls enthalten sein. Die Hintertür soll in den Jahren 2000 bis 2001 Eingang in den Code gefunden haben, als OpenBSD-Entwickler im Auftrag der US-Regierung den Code manipuliert haben sollen.

In einer von de Raadt beigefügten Mail des Softwareentwicklers und nach eigenen Angaben ehemaligen OpenBSD-Contributors Gregory Perry wird namentlich der Entwickler Jason Wright als Beteiligter erwähnt. Wright ist beziehungsweise war einer der führenden Köpfe von OpenBSD.

Die Vorwürfe wiegen schwer, de Raadt hatte nach eigenen Angaben seit über zehn Jahren keinen Kontakt mehr mit Perry und stellt deshalb die Mail von Perry öffentlich zur Diskussion – auch um nach eigener Aussage nicht Teil dieser Verschwörungstheorie zu werden. De Raadt weist auch darauf hin, dass in den vergangenen zehn Jahren der betroffene Code mehrfach gepatcht, überarbeitet und neu geschrieben wurde. Daher ließe sich schwer einschätzen, ob die Hintertür überhaupt noch vorhanden sei.

Perry hat sich nach eigener Aussage erst jetzt an den OpenBSD-Gründer gewandt, weil seine Verschwiegenheitsvereinbarung mit dem FBI nach zehn Jahren ausgelaufen sei. Als Mitarbeiter des Unternehmens Netsec haben er damals eine FBI-Abteilung [beraten](#), die sich unter anderem mit dem Einbau von Hintertüren und Key-Recovery (Key Escrow) in Smartcards beschäftigt habe. Daher wisse er, dass das FBI seinerzeit erfolgreich mehrere Hintertürchen und Möglichkeiten für Seitenkanal-Angriffe im OpenBSD Crypto Framework (OCF) platziert habe.

3. Implementierungen Mit Absicht unsicher (4)

- Gezielte Schwächungen durch die Implementierung (Methodik Hardware und System):
 - Schwachstellen
 - Unbekanntes Modul oder Kanal in der Hardware
 - Stärke der Sicherheitsfunktionen der Hardware zu niedrig
 - Interaktion von Hardware und Software

3. Implementierungen

Mit Absicht unsicher (5)

- Gezielte Schwächungen durch die Implementierung (Beispiel Hardware und System: TPM in Windows 8):
 - Die Nutzung eines TPM 2.0 Hardwaremoduls in Zusammenspiel mit dem Einsatz von Microsoft Windows 8 kann die Sicherheits grds. erhöhen
 - „Aus Sicht des BSI geht der Einsatz von Windows 8 in Kombination mit einem TPM 2.0 mit einem Verlust an Kontrolle über das verwendete Betriebssystem und die eingesetzte Hardware einher.“
 - Vertraulichkeit und Integrität sind hierdurch nicht mehr gewährleistet

Quelle:

https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Windows_TPM_PI_21082013.html

- Mögliche Konsequenzen für die Erarbeitung und Implementierung von IT-Sicherheitsstandards:
 1. Hohe Transparenz während der Erarbeitung
 2. Offenheit der Standards
 3. Falls möglich: Referenzimplementierungen als Open Source
 4. Zertifizierungen und Audits im Nachgang

Kontakt

Bundesministerium für Wirtschaft und Energie

Tobias Kaufmann

Standardisierung in der IKT und sichere Internetarchitekturen

Telefon: +49 30 18 615 6697

E-Mail: Tobias.Kaufmann@bmwi.bund.de