

Object moved to [here](#).

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop | RSS | Mobile | Newsletter | Sign in | Register | [Search](#)

SPIEGEL ONLINE INTERNATIONAL

Front Page World Europe Germany Business Zeitgeist Newsletter

English Site > World > NSA Spying Scandal > NSA-Documents: Attacks on VPN, SSL, TLS, SSH, Tor

NSA Documents: Attacks on VPN, SSL, TLS, SSH, Tor

December 28, 2014 – 08:04 PM | Share | Recommend 62 | Tweet 651 | g+1

[Print](#) | [E-Mail](#) | [Feedback](#)

NSA Spying Scandal

Get Mobile with Our New App



Download It Today: 'DER SPIEGEL' in English! Now Available for iPhone

European Partners

 PressEurop

 Politiken

 Corriere della Sera

Photos of Kidnapped Boy with IS Fighters

Malala and the school massacre Her father: "It's beyond human imagination"

Newsletter



Sign up for SPIEGEL Online's daily newsletter – and get the best of Der SPIEGEL's and SPIEGEL Online's international coverage in your In-Box everyday.

Facebook

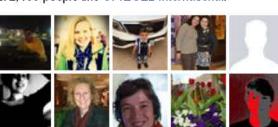
Find us on Facebook



272,456 people like SPIEGEL International.

 SPIEGEL International Like

272,456 people like SPIEGEL International.



Einzelne Social Plugins

Attacks against Crypto

Guide for Analysts on how to use the PRISM Skype Collection

GCHQ Briefing on the BULLRUN Program

GCHQ Presentation on the BULLRUN Programs Decryption Capabilities

NSA LONGHAUL program for end-to-end attack orchestration and key recovery service

BLUESNORT program on "Net Defense" from Encrypted Communications

Presentation from the SIGDEV Conference 2012 explaining which encryption protocols and techniques can be attacked and which not

NSA program SCARLETFEVER explaining how attacks on encrypted connections are orchestrated

Description of VOIP Telephony Encryption methods and cryptanalytic and other ways to attack

Attacks on SSL/TLS

NSA Experiment for massive SSL/TLS Decryption

Canadian Document from CES on TLS Trends

Details on how NSA uses the SCARLETFEVER program to attack Scure Sockets Layer (SSL)/Transport Layer Security (TLS)

Analysis from SSL/TLS Connections through GCHQ in the flying pig database

Attacks on VPN

NSA High Level Description on TURMOIL / APEX Programs on Attacking VPN

Explanation of the GALLANTWAVE that decrypts VPN Traffic within LONGHAUL

Intro to the VPN Exploitation Process mentioning the protocols attacked - PPTP, IPSEC, SSL, SSH)

Analytic Challenges from Active-Passive Integration when NSA attacks IPSEC VPNs

Overview of the capabilities of the VALIANTSURF program

MALIBU Architecture Overview to exploit VPN Communication

POISENNUT Virtual Private Network Attack Orchestrator (VAO)

NSA Presentation on the development of Attacks on VPN

NSA Presentation on the Analysis and Contextualisation of data from VPN

Description of existing projects on VPN decryption

Explanation of the Transform Engine Emulator when attacking VPN

Explanation of the POISENNUT Product and its role when attacking VPN

Explanation of the TURMOIL GALLANTWAVE Program and its role when attacking VPN

Processing of data from exploited VPN in the TURMOIL program

Decryption of VPN Connections within the VALIANTSURF program

Description on the processing of VPN data packets within the TURMOIL program

Explanation on the SPIN9 program on end-to-end attacks on VPN

Deanonymizing

Explanation of a potential technique to deanonymise users of the TOR network

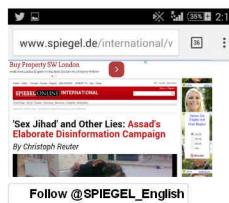
Object moved to [here](#).

Twitter

 NedOukrainka
@Vallitsa

Nazis in Ukraine - "Kremlin propaganda" And @SPIEGEL_English said ISIS atrocities - "Assad propaganda" @rusockey
pic.twitter.com/AxPsNCSPuM

Retweeted by Михаил Преображенский



47m

Analytics on security of TOR hidden services

Overview on Internet Anonymization Services on how they work

TOR deanonymisation research

TOR Overview of Existing Techniques

A potential technique to deanonymise users of the TOR network

Cryptanalytic

General Description how NSA handles encrypted traffic

Intercept with PGP encrypted message

Classification Guide for Cryptanalysis

Procedural GCHQ Document on how analysts are to handle encrypted traffic

NSA / GCHQ Crypt Discovery Joint Collaboration Activity

NSA Cryptographic Modernization (CryptoMod) Classification Guide

"National Information Assurance Research Laboratory (NIARL)":
Newsletter, Keyword TUNDRA

What Your Mother Never Told You About the development of Signal
Intelligence

Intercept with OTR encrypted chat

Article...

[Print](#) | [E-Mail](#)

[Feedback](#)

Share **Recommend** 62 people recommend this. [Sign Up](#) to see what your friends recommend.



[Tweet](#) 651 [8+1](#) +10 Recommend this

[Post to other social networks](#)

Das könnte Sie auch interessieren



BVB auf Abstiegsplatz Borussia Dortmund verpflichtet Kampl

Der BVB steckt in der Krise. Nun hat der Klub reagiert - und auf dem Transfermarkt zugeschlagen: Der slowenische Nationalspieler Kevin Kampl wechselt von RB Salzburg nach Dortmund. Ein anderer Profi hat die Borussia verlassen. [mehr...](#)



Bundesliga-Goalgetter Alex Meier Stehen, warten - Tor

Der beste Bundesliga-Torjäger spielt nicht bei Bayern München oder beim VfL Wolfsburg, sondern bei Eintracht Frankfurt: Alexander Meier trifft, wie er will. Viel laufen muss er dafür nicht mehr. [mehr...](#)

ANZEIGE

Das neue Lumia 535

Smartes Phone, smarter Preis. Jetzt für nur 119 € UVP. [mehr...](#)



Borussia Dortmund Langerak bis zur Winterpause im BVB-Tor

Weltmeister Roman Weidenfeller auf der Bank, Ersatzkeeper Mitchell Langerak im Tor: Das wird bei Borussia Dortmund erst einmal so bleiben. Trainer Jürgen Klopp legte sich auf den Australier als Nummer eins für den Rest der Hinrunde fest. [mehr...](#)



Spyware Falsche Mobilfunkstationen im norwegischen Regierungsviertel entdeckt

Norwegens Politiker werden offenbar von Unbekannten ausspioniert. Rund um zentrale Regierungsgebäude in Oslo hat eine Zeitung Überwachungsgeräte entdeckt. Der Geheimdienst ist beunruhigt. [mehr...](#)

powered by veeseo

ADVERTISEMENT

Explore Your Genealogy

 [familylink.com/AncestorSearch](#)

Billions of Names at FamilyLink. Begin Your 7-day Free Trial Now!

[Learn German online free](#)
[Antenna Deal of the Day](#)
[Watch Live Tv Streams](#)
[Scary News Round-Up 2006](#)
[Free Calculator Toolbar](#)
[Start Download](#)
[Start Download](#)
[Listen To It Online](#)
[Stream TV Online Free](#)

Keep track of the news

Stay informed with our free news services:

[Twitter](#) | [RSS](#)All news from [SPIEGEL International](#)[RSS](#)All news from [World section](#)

© SPIEGEL ONLINE 2014
All Rights Reserved
Reproduction only allowed with the permission of SPIEGELnet GmbH

MORE FROM SPIEGEL INTERNATIONAL**GERMAN POLITICS****Merkel's Moves:** Power Struggles in Berlin**WORLD WAR II****Truth and Reconciliation:** Why the War Still Haunts Europe**ENERGY****Green Power:** The Future of Energy**EUROPEAN UNION****United Europe:** A Continental Project**CLIMATE CHANGE****Global Warming:** Curbing Carbon Before It's Too Late[OVERVIEW INTERNATIONAL ▶](#)[▲ TOP](#)[Home](#) [Politik](#) [Wirtschaft](#) [Panorama](#) [Sport](#) [Kultur](#) [Netzwerk](#) [Wissenschaft](#) [Gesundheit](#) [einestages](#) [Uni](#) [Reise](#) [Auto](#) [Stil](#) [Wetter](#)**DIENSTE**[Schlagzeilen](#)
[Nachrichtenarchiv](#)
[RSS](#)
[Newsletter](#)
[Mobil](#)**VIDEO**[Nachrichten Videos](#)
[SPIEGEL TV Magazin](#)
[SPIEGEL TV Programm](#)
[SPIEGEL Geschichte](#)
[SPIEGEL TV Wissen](#)**MEDIA**[SPIEGEL QC](#)
[Mediadaten](#)
[Selbstbuchungstool](#)
[weitere Zeitschriften](#)**MAGAZINE**[DER SPIEGEL](#)
[Dein SPIEGEL](#)
[SPIEGEL GESCHICHTE](#)
[SPIEGEL WISSEN](#)
[KulturSPIEGEL](#)
[UniSPIEGEL](#)**SPIEGEL GRUPPE**[Abo](#)
[Shop](#)
[SPIEGEL TV](#)
[manager magazin](#)
[Harvard Business Man.](#)
[buchreport](#)
[buch aktuell](#)
[Der Audio Verlag](#)
[SPIEGEL-Gruppe](#)**WEITERE**[Hilfe](#)
[Kontakt](#)
[Nutzungsrechte](#)
[Datenschutz](#)
[Impressum](#)[▲ TOP](#)