Curriculum Vitæ

Personal Information

Name	**Axel Benjamin Rengstorf**
Date of birth	**13.06.1977, Bremen, Germany**
Address	**Kaiser-Wilhelm-Ring 70**
	55118 Mainz
	Germany
Telephone	**(01 76)53 46 61 03**
E-mail	**ar@bluebox-security.de**

School education

1998-2009 **Diploma in computer science, Karlsruhe Institute of Technology (KIT)**, *Specialization in "Cryptography", "Telematics" and "Electronic Engineering", all marks good*, diploma final mark 2.7.

1997 **Abitur (A-level equivalent)**, *KGS Brinkum, Germany*, main subjects mathematics, physics.

Certifications

November 26th 2018 **Offensive Security Certified Professional (OSCP)**, *Identify and exploit XSS, SQL injection, and file inclusion vulnerabilities in web applications.*, Analyze, correct, modify, cross-compile, and port public exploit code., Successfully conduct both remote and client side attacks..
Write basic scripts and tools to aid in the penetration testing process. Use multiple information gathering techniques to identify and enumerate targets running various operating systems and services.

October 27th 2017 **Offensive Security Certified Expert (OSCE)**, *Identify hard-to-find security vulnerabilities.*, Conduct intelligent fuzz-testing., Analyze, correct, modify, and port x86 exploit code.. Hand-craft binaries to evade anti-virus software.

Dec 2017 **Splunk Certified User**.

Dec 2017 **Splunk Certified Power User**.

Exploit Advisories

BBS-2019-01 **Mitel 6869i SIP Deskphone 4.2.2032: Unauthenticated Bash Command Injection Vulnerability with Root Priviledges in webuploadconfig script**.

CVE-2010-3281 **Alcatel-Lucent - arbitrary code execution at OmniVista 4760**.

CVE-2010-3279
CVE-2010-3280 **Alcatel-Lucent - unauthenticated administrative access to CTI CCA Server**.

CVE-2010-3281 **Alcatel-Lucent - arbitrary code execution at OmniVista 4760**.

Experiences

since June 2004 **Consultancy work as IT Security freelancer**.

2004-2005 **Maintainer of a Siemens PBX-system with 800 extensions**.

1999-2001 **Chief of network security at HadiNet**, *including penetration testing and maintaining a Certification Authority and security advisory.*

Noticeable assignments

Oct2019 **Java Source Code Review of a web-based online Casio Game.** , *Security Code Review of 100k lines of Java Code*, Analysis of the REST-API and gaming functions.

March2019 **Source Code Audit of Java based Webapplication-Backend Code of an IOT device.** , *Analysis of Authentication Functionalities*, Review of code implementing REST-API functionalities and REST-API based calls.

June2019 **Webapplication Pentest of REST-API components and Frontend of an Application for a german insurance company.** , *BlackBox Analysis of a Spring/AngularJS based application*.

March2019 **Source Code Audit of Java based Webapplication-Backend Code of an IOT device.** , *Review of 100mb of Source Code*, Analysis of the Authentication Mechanisms, Web hooks and Recipie Management, Man-in-the Middle Attacks used to inject malicious data into commununication.

March2019 **Configuration and Infrastructure review of a a complete Avaya based VoIP Infrastructure for a major german fair**, *Assessment of the available Documentation.*, Review of Security Settings, Firewall Configuration Review.
Analysis of Configuration Files

July2018 **Vulnerability Assessment of a complete Cisco based VoIP Infrastructure for a major Business Consultancy Agency**, *Security Analysis from the perspective of an internal employee*, Configuration Review of all major components.

June2018 **BlackBox and Source Code Audit of an Android based Mobile Banking Application for a major german Bank**, *Assesment of the Source Code in C and Java*, Analysis of the Code responsible for webservice communication.

Feb2018 **Several BlackBox Web Application Security Assessments for a major german Consultancy Agency**.

Jul2016-Sep2018 **Work as Vulnerability Assessment Specialist at Deutsche Bank**, *Development of a SSL Vulnerability Scanner in Python Programming Language*, Managing and performing corporate/global wide SSL Vulnerability Scans using Nessus, Managing and performing coperate wide Vulnerability Scans.

March-Mai 2016 **Security Assessment of the major IT components of a german car for a major german car manufactor**, *Internal CAN-Bus Analysis*, USB Attacks of the Radio, Attacks over DAB of the Radio.

February 2016 **Web Application Pentest of the Web Backend Services of a kitchen cooking machine**.

January 2016 **Development of a Digital Audio Broadcast (DAB) Radio Protocoll Fuzzer for a major german car manufactor**, *Protocol Fuzzer implemented in C++ using GnuRadio*.

December 2015 **Security Analaysis of a Huawei LTE Small Cell**, *Analysis of data that can be gathered from a stolen device*, Reverse Engineering of VxWorks based ARM and PPC Binaries, Black Box Analysis of administrative Web Interface.

May 2015 **Assesment of a windows software for a swiss medical device**, *SSL Man-in-the-Middle Attacks*, Finding implementation flaws.

March 2015 **Security Analaysis of a Nokia and Alcatel LTE Small Cell**, *Reverse Engineering of ARM and PPC Binaries*, Black Box Analysis of proprietary Networking Protocols.

Oct 2014 - Feb 2015 **2nd Level Global Security Incident Manager at Vodafones Global Security Operations Center**, *Set-up, execution and maintenance of the security incident management and coordination process in conjunction with operator and customer / partner incident management capabilities.*, Acting as functional lead for managed incident handling as well as underlying processes and tools. , Set-up of analytics framework and tools..
Teaming up with Security Analysts and Engineers of other departments and customers for problem and incident resolution.

Sept 2015 **Documentation and Implementation of IBM AppScan Enterprise into Vodafones Infrastructure**, *Installation of IBM AppScan Enterprise used for automatic Web Application Assessments, Configuration of parameters for periodic security scans, Manual verification of found security issues*, Documentation for users in english language.

Feb-August 2015 **Security support for SAP in the HANA Database project**, *Analysis of the C++ based Core Components*.

Kaiser-Wilhelm-Ring 70 • 55118 Mainz Germany
☎ (01 76) 53 46 61 03 • ✉ ar@bluebox-security.de

2014 **Security Assessment of the Android and iPhone SAP FIORI Client Applications**, *SAP developed an in-App Browser to cache access to FIORI URLs. Implemented by usage of PhoneGap API.*, Source Code Audit in Objective-C and JAVA language, Blackbox Mobile Client Security Assessment.

2014 **Configuration Audit of HiPath 4000 PBX**, *Analysis of IP Phone Configurations, Remote Management Ports, DECT Configuration*.

2014 **Configuration Audit of a Windows 8.1 operating system for a german super market chain**, *Security improvements for a corporate wide used Windows 8.1 workstation configuration*.

Feb-August 2014 **Security support for SAP in the HANA Database project:**, *Design of API to prevent SQL injection in HANA for DDL Procedures, Analysis of Threats when HANA used in a Multi Database Scenario, C++ Source Code Review of SQL Procedures*, Audit of administrative XSEngine Applications.
Source Code Audit of SQLScript builtin procedures

2014 **Blackbox Penetrationtest of a banking Webapplication and its infrastructure for a major german supermarket chain**, *Testing for OWASP-Top10 Web Security Vulnerabilites, Vulnerability Analysis of used network components*.

2013 **Penetration test of a HiPath 4000 PBX for a german airline**, *Main focus: eavesdropping of internal calls*, Analysis of the configuration of end-user devices.

2013 **BlackBox Testing of Windows WebDAV client components for the European Central Bank (ECB)**.

2013 **3 months of Security support for SAP in the HANA project:**, *Performing C++ Source Code audits, Analysis of AFL applications*, Analysis of Clickjacking Attacks against SAP HANA XSEngine applications, Assesment of SAML and O-Data implementation.
Designanalysis of Javascript and SQLSCript Debugging mechanisms

2013 **Source Code Audit of a DECT basestation in C language for a german company producing DECT phones**, *Analysis of security flaws in Radio Protol and Management Interfaces*.

2012 **Blackbox Penetration testing of Alcatel 4400 based DECT components (basestation and headsets) for the German Federal Bank**, *Analysis of Authentication and Encryption mechanisms of Handsets*, BlackBox Assessment of the DECT Mac-Layer, Man-in-the-Middle attacks.

2012 **Source Code Audit of an iOS and Blackerry Java mobile payment application for a major UK bank**.

2012 **Writing security guidelines for a HiPath PBX Enviroment**, *Guidelines for Security Parameters for a secure integration of a HiPath PBX into a middle-class company's network*.

2012 **Penetrationtest of Avaya PBX's SIP components for a german tax consultancy company**, *Fuzzing of SIP-Stack implementations of Callserver, Softphone and Phone.*, Threat Analysis of Avavay PBX environment.

2012 **3 months of Security support for SAP in the HANA projekt**, *performing penetration tests of (HTML5/JS) web-components*, C++/C/Objective-C/Javascript source code review, writing secure programming guidelines and threat analysis in Germany and USA.

2012 **Security assesment of an iOS application's file encryption functionalities for SAP**, *Source code review of application's code in Objective-C*, BlackBox penetration tests of application and backend components.

2012 **Source code audit of an iOS application with HANA as backend server for SAP: Assesemnet of client side coding for security flaws**.

2012 **Source code review of an IOS and Blackberry Travel Expenses application for SAP: Analysis of code for security bugs**.

2011 **C/C++ Source Code Audit of 1and1ś developped Apache Webdav Modules at 1and1**, *Analysis of the customn developped Code for Injection Bugs*.

2011 **Java Source Code Audit of an Androip App for a major german bank**.

2011 **PHP Source Code Audit of 1and1s DIY homepage product at 1and1 in Karlsruhe**, *Review of 100k lines of object orientated PHP code*, Review of Code with administrative access toa virtual machine running the product.

Kaiser-Wilhelm-Ring 70 • 55118 Mainz Germany
☎ (01 76) 53 46 61 03 • ✉ ar@bluebox-security.de

2011 **Penetration test of a Tandberg based video conference system for the German Federal Bank**.

2010 **Threat Analysis of a VoIP and Video infrastructure for a major german bank**.

2010 **Reverse Engineering of ARM based Executables of AVM FritzBox 6360 for KabelBW**, *Main focus: possibilites to increase available bandwith*.

2010 **Security assesment of the IQImpact Broker-PBX manufactured by IPC for the German Federal Bank**, *included Blackbox Analysis and Reverse Engineering of propertary signalling algorithms*.

2010 **7 months of Webapplication Testing for T-Systems's key systems during their Security Checkup 2010**.

2009 **Penetration testing of the Alcatel based call-center-infrastructure of the German Federal Bank**, *Reverse Engineering of CTI-Server and Client Components*.

2008 **Security review of T-System"s Cisco-based VOIP-Infrastructure**.

2007 **Review of Siemens Security Documentation for their HiPath 8000 PBX-system**.

2007 **Penetration testing of a Siemens OpenStage 40 VoIP-phone at Siemens**, *Blackbox Assessment of the SIP and RTP Stack, Review of the Software Update Mechanism*.

2007 **2 months Web application penetration testing of "T-Systems" key systems**.

2007 **Binary analysis of a software distribution tool at "T-Systems"**.

2006 **Selected as head of security audit and penetration testing of the PBX-environment of German Federal Bank including documentation review, network-operating system- and PBX-configuration audit and ISDN tests**.

2006 **Security assesment of the Alcatel 4400 based PBX-environment of "Deutsche Börse AG"**.

2006 **Penetration testing and audit of an Avaya-PBX-environment at "TechData"**, *Main focus: Analysis of VMB access methods*.

2005 **Security assessment of the complete SIP-environment of "T-Online"**, *OpenSER based VoIP infrastructure with SBC to german telecoms phone network*.

2005 **VoIP-Training for "T-Online" security department**, *1 week course of training, SIP and RTP based VoIP attacks*.

2004 **Audit of a Siemens HiPath PBX-enviroment at "Tengelmann"**.

Whitepapers

Decemeber 2009 **"Security-Improvements for the P2PNS-Nameservice"**, *Diploma Thesis*.

Summer 2007 **"Security properties in GSM Networks - SIM and SMS"**, *Student Thesis*.

Winter 2003 **"Security of the .de-top-level domain through DNS SEC"**, *Federal Office for Information Security (BSI)-Study*, http://www.bsi.de/literat/studien/securedns/Studiesecdns.pdf.

Conferences

November 2008 **"Hacking cordless phones"**, *Bellua Cyber Security Conference Asia*, Disclosing DECT Standard authentication algorithm and 1st analysis.

4.7.2008 **"Introduction into GnuRadio Programming"**, *CCC Gulasch Programmiernacht GPN#7*, http://entropia.de/wiki/images/9/91/Introduction_to_gnuradio_programming.pdf.

Skills

Programming languages: C/C++, Java, Python, Perl, PHP, x86-Assembler, Sparc-Assembler, MIPS-Assembler, ARM-Assembler, 6502-Assembler, VHDL, SQL, XML

Network protocols: TCP/IP, IPV4, IPV6, SIP, SDP, SCTCP, (S)RTP, H.323, H.225, H.254, MGCP, MEGACO, Q.921, Q.931, GSM, SMS, X.25, DECT, SS7, CCITT#5, BGP, OSPF, TLS/SSL, IPSEC, MPLS, DNS, DNS-SEC, IEEE 802.11, KADEMLIA, CHORT

Kaiser-Wilhelm-Ring 70 • 55118 Mainz Germany
☎ (01 76) 53 46 61 03 • ✉ ar@bluebox-security.de

Penetration testing	VMB hacking, ISDN attacks, Wardialing, Fuzzing, Reverse Engineering, Embedded Systems, Buffer-/Heap-/Integer overflow attacks, Web application pentesting, network protocol analysis, proprietary protocol analysis, analysis and attacks on cryptographic protocols, Source code auditing (C,C++,Java,PHP,Android), Threat analysis
Operating systems	Linux, *BSD, Solaris, Windows
PBX	Alcatel, HiPath, Hicom, Avaya

Kaiser-Wilhelm-Ring 70 • 55118 Mainz Germany
☎ (01 76) 53 46 61 03 • ✉ ar@bluebox-security.de

Spoken languages

German	native language
Englisch	fluent in speaking and writing
French	understanding and reading

Security clearances

Since 2006	**German security clearance Level 1 (Ü1)**.

Personal interests

Music	Electronic music, Rock
Literature	Horror, Daily newspaper
Sport	Jogging, Swimming, Rowing, Teamsport

Kaiser-Wilhelm-Ring 70 • 55118 Mainz Germany
☎ (01 76) 53 46 61 03 • ✉ ar@bluebox-security.de