No Hats
IP & DNS Security Specialists

Paul Wouters

Security specialist with a focus on DNS, DNSSEC and IPsec VPNs. He has build DNSSEC appliances, as well as DNSSEC signing solutions for various TLD's. He has written DNSSEC Practise Statements (“DPS”) for some TLDs as well. Paul has worked with ICANN before both as a consultant and volunteer. He is a long time Internet Engineering Task Force (“IETF”) participant and contributor, author of various RFC's and currently the co-chair of the IETF TRANS working group which is responsible for writing the internet standards related to Certificate Transparency.

Extensive experience programming in C, python and UNIX shell-scripting languages. He is a founding member and core developer for the Libreswan (formerly “Openswan”) IPsec and IKE opensource software project.

Education

1992 – 1995	CS undergraduate at Radboud University Nijmegen, the Netherlands
[redacted]	Bachelor of Education (concentration in chemistry) at Noordelijke Hogeschool Leeuwarden, the Netherlands

Positions

2011 – current	President at No Hats, DNSSEC and IPsec consulting	No Hats
2012 – current	Associate (Sr Software Engineer) for Red Hat Enterprise Linux (RHEL)	Red Hat
2011 – current	Core Developer IPsec software	Libreswan Project
2015 – current	Technical Expert Group member for the IETF (Liaison)	ICANN / IETF
2015 – current	Registry Services Technical Evaluation Panel (RSTEP) member	ICANN
2014 – current	Co-Chair TRANS working group	IETF
2015 – 2016	DNS Root Zone KSK rollover Design Team member	ICANN
2012 – 2013	newGTLD Registry Services Technical Evaluation Panel member	ICANN
2003 – 2011	Sr. Software engineer for DNSSEC	Xelerance
2003 – 2011	Release Manager IPsec software	Openswan Project
1995 – 2003	CTO at an ISP	Xtended Internet

Recent Publications

RFC 7929	DNS-Based Authentication of Named Entities (DANE) Bindings for OpenPGP
RFC 7901	CHAIN Query Requests in DNS
RFC 7828	The dns-tcp-kepalive EDNS0 Option
RFC 7670	Generic Raw Public-Key Support for IKEv2
RFC 7619	The NULL Authentication Method in IKEv2
RFC 7250	Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)

Openswan: Building and Integrating Virtual Private Networks
by Paul Wouters & Ken Bantoft
ISBN-13: 978-1904811251 ISBN-10: 1904811256
https://www.amazon.ca/Openswan-Building-Integrating-Networks-developers/dp/1904811256

Draft Publications

draft-ietf-dnsop-maintain-ds	DNS, Registry
draft-ietf-ipsecme-rfc4307bis	IPsec
draft-ietf-regext-dnsoperator-to-rrr-protocol	DNS, Registry
draft-mglt-ipsecme-rfc7321bis	IPsec
draft-pauly-ipsecme-split-dns	IPsec, DNS
draft-wouters-sury-dnsop-algorithm-update	DNS, cryptography
draft-york-dnsop-deploying-dnssec-crypto-algs	DNS, cryptography

Recent presentations:

Linux Security Summit, Toronto, August 2016
“Opportunistic Encryption using IPsec”
http://events.linuxfoundation.org/sites/events/files/slides/LinuxSecuritySummit-2016-OE-16x9.pdf

Linux Con, San Diego, 2012
“DNSSEC: The shiny new cryptographically secured globally distributed database”
https://people.redhat.com/pwouters/LinuxCon2012-DNSSEC.pdf

SecTor, Toronto, 2012
“DNSSEC deployment in Canada” - with Norm Ritchie of CIRA (.ca)
http://sector.ca/sessions/dnssec-deployment-in-canada/