

Ralph Holz

NICTA (National ICT Australia)
13 Garden St
Eveleigh NSW 2015
Sydney, Australia

Office: (2) 9376 2192
Mobile: (435) 349593
Fax: (2) 9376 2300
Email: ralph.holz@nicta.com.au

Personal data

Current position	Researcher
Degree	PhD ('summa cum laude')
Citizenship	German

Research interests

My research interests focus on collecting and utilising large-scale observational data to design intelligent network systems that can reason with this data and make appropriate choices to improve network resilience, efficiency, and security. I pursue empirical approaches to determine factors that are causative for security and allow to analyse and understand the weaknesses of current systems and deployments.

Experience

- 12/2014–ongoing** **Researcher**
Mobile Systems and Software Systems research groups; Security Business Team
NICTA, ATP, Sydney, Australia
Current projects: Research and development of systems to gather empirical data to improve the resilience of network components and the security of systems. Detection of attacks on security-critical infrastructure, in particular DNS, routing, TLS. Leading research efforts to develop and deploy secure deployment pipelines, countering threats at code level.
PhD students: Co-advisor for Mr Jun Young Kim, with Dr. Wen Hu.
[since 03/2015] **Conjoint Lecturer:** University of New South Wales. Co-lecturer of Securing Wireless Networks course (COMP9337), with Dr. Sanjay Jha.
[since 12/2014] **Adjunct Research Associate:** Technische Universität München. Cooperation with NICTA on global Internet scans.
- 08/2014–11/2014** **Post-doctoral Research Associate**
Chair for Network Architectures and Services
Technische Universität München
Projects: Large-scale measurements of DNS with custom-built scanners; development of distributed global scanning infrastructure.
Teaching: Designed, updated, and taught core parts of Network Security. Led tutorials and designed student assignments.
- 05/2014–07/2014** **Visiting Researcher**
NICTA, Sydney, Australia
Project: Inference of network topology from passive measurement data. Developed testbed and inference algorithms; proof-of-concept.
- 01/2014–05/2014** **Guest Scientist**
Chair for Network Architectures and Services
Technische Universität München
Project: Attack detection in BGP using a combined approach based on TLS and SSH measurements together with BGP and RIR data.
- 01/2008–12/2013** **Research Associate and PhD student**
01/2010–12/2013
Chair for Network Architectures and Services
Technische Universität München

01/2008–12/2009 Group previously based at Universität Tübingen

Academic research projects:

since 12/2011 Crossbear: devised, developed and deployed a tool for the automated detection and reporting of Man-in-the-middle attacks on TLS. A notary-based design, Crossbear goes beyond existing mechanisms by carrying out an attempt to locate the attacker, using multiple vantage points in the network. This endeavour won a grant from Counterpart, USA, which allowed me to hire a team of students to implement Crossbear for the Open Observatory of Network Interferences, a Tor subproject.

11/2010–11/2011 ResumeNet: designed and evaluated a concept to increase network resilience. Using an overlay, routers leverage common BGP peering and run a special protocol to determine whether they can reroute traffic via other neighbours when a link to the primary next hop has failed. Funded by the EU's 7th Framework Programme (FP7); nine international partners. (resumenet.eu)

01/2008–12/2009 Spontaneous Virtual Networks: developed and evaluated a cross-layer network measurement component, whose results are shared across a number of application-tailored overlay networks. We demonstrated the feasibility and usefulness by integrating it into a massively multiplayer online game. I was also involved in the design of a security component for the application-tailored networks. (spovnet.de)

Industry research projects:

01/2010–09/2012 With Airbus Group: designed and developed a novel Ethernet-based and IP-capable cabin network to serve multiple purposes. The resulting network uses only commercial off-the-shelf components yet meets the aerospace industry's stringent requirements concerning bandwidth, latency and jitter. Specified the use of Ethernet subprotocols in the proposed architecture. Investigated suitable codecs for high-quality audio transmission. A preliminary security analysis of the design was also part of my responsibilities.

04/2010–08/2010 With Nokia Siemens Networks: carried out an analysis of IETF ALTO and DECADE for network caching and traffic optimisation with the goal of determining their potential use in the company's 4G network technology.

04/2008–10/2008 With Nokia Siemens Networks: developed a privacy-preserving Identity Provisioning solution for 3G/4G networks. The solution allows the telco to act as an Identity Provider towards commercial services and vouch for a user's pseudonym, thus preserving the user's privacy towards the service. Specified the protocol for use with 3G/4G AAA solutions and provided SAML reference specification. Verified the security of the protocol with model checker.

Teaching:

01/2008–12/2013 Co-lecturer and assistant for the courses Network Security, iLab 1 and 2, Communication Networks, P2P Security, seminars. Designed lectures and course work. Advised 25 research students during their theses.

02/2002–04/2002 Academic Visitor

IMPACT Research Group, University of Loughborough, UK. In cooperation with UBC Media, London, UK. Researched novel information design and developed an XML/XSL-based demonstrator to encode audio-visual content in Digital Audio Broadcasting.

Education

01/2008–05/2014 **Doctoral student**

Technische Universität München, Germany
PhD with highest distinction ('summa cum laude')
Advisor and first referee: Prof. Georg Carle, Technische Universität München
Second referee: Prof. Nick Feamster, Princeton University

Dissertation: 'Empirical analysis of Public Key Infrastructures and investigation of improvements'.

Carried out Internet-wide measurements of PKI deployments, in particular SSL/TLS (X.509), SSH, and GPG. Developed scanning framework in Python; data analysis with PostgreSQL, R, Python. Analysed proposals such as Certificate Transparency, TACK and DANE with respect to different attacker models and potential issues with deployment. Developed and deployed Crossbear, a tool for distributed detection and localisation of Men-in-the-middle in TLS.

10/1999–10/2007 **Studies of Computer Science**

Universität Tübingen, Germany
Degree: Diplom-Informatiker (= MSc., grade: 1.0—very good)
Focus areas: networks, security, neural networks
Thesis: 'Secure domain-based Peer-to-Peer networks'

10/2001–10/2004 Parallel studies of Romance Languages
Enrolment to learn Italian and Spanish

10/1998–09/1999 **Studies of Mathematics and Theology**

Universität Tübingen, Germany
Enrolment to become a teacher at secondary schools

Service

TPC member of IFIP SEC 2015 and 2016

Local Arrangements Co-Chair for IFIP Performance 2015

Reviewer for ACM Trans. Information and System Security, ACM SIGCOMM IMC, IEEE ISSRE, IEEE ICC, IEEE N2S, IFIP Networking, IFIP SEC, NetSys

Co-founder of the Munich Security Meetup MUC:SEC

Member of Faculty Board, Universität Tübingen

Scholarships and awards

Counterpart, USA: Technology Grant for Crossbear (USD 20,000)

Scholarship Baden-Württemberg-Stipendium, Germany (studies in Australia)

Scholarship by Istituto Italiano di Cultura, Italy (language training)

Standardisation work

Y. Sheffer, R. Holz, P. Saint-Andre: *RFC 7525: Recommendations for secure use of TLS and DTLS*. May 2015.

Y. Sheffer, R. Holz, P. Saint-Andre: *RFC 7457: Summarizing known attacks on TLS and DTLS*. October 2014.

Publications at conferences and workshops

O. Mehani, R. Holz, S. Ferlin, R. Boreli: *An early look at Multipath TCP deployment in the wild*. Proc. 6th Int. Workshop on Hot Topics in Planet-Scale Measurement (HotPlanet), Paris, France, September 2015.

L. Bass, R. Holz, P. Rimba, A. B. Tran, and L. Zhu: *Securing a deployment pipeline*. Proc. 3rd Int. Workshop on Release Engineering, Florence, Italy, May 2015.

J. Schlamp, R. Holz, O. Gasser, A. Korsten, Q. Jacquemart, G. Carle, and E. W. Biersack: *Investigating the nature of routing anomalies: closing in on subprefix hijacking attacks*. Proc. 7th Int. Workshop on Traffic Monitoring and Analysis, Barcelona, Spain, April 2015. (**best paper award**)

O. Gasser, R. Holz, G. Carle: *A deeper understanding of SSH: results from Internet-wide scans*. Proc. 14th Network Operations and Management Symposium (NOMS), Krakow, Poland, May 2014.

R. Holz, T. Riedmaier, N. Kammenhuber, G. Carle: *X.509 forensics: detecting and localising the SSL/TLS Man-in-the-middle*. Proc. 17th European Symposium on Research in Computer Security (ESORICS), Pisa, Italy, 2012.

R. Holz, L. Braun, N. Kammenhuber, G. Carle: *The SSL Landscape: a thorough investigation of the X.509 PKI using active and passive measurements*. Proc. 11th ACM SIGCOMM Internet Measurement Conference (IMC), Berlin, Germany, 2011.

A. Ulrich, R. Holz, P. Hauck, G. Carle: *Investigating the OpenPGP Web of Trust*. Proc. 16th European Symposium on Research in Computer Security (ESORICS), Leuven, Belgium, 2011.

A. Fessi, N. Evans, H. Niedermayer, R. Holz. *Pr2-P2PSIP: Privacy Preserving P2P Signaling for VoIP and IM*. Proc. 7th Principles, Systems and Applications of IP Telecommunications (IPTComm), Munich, August 2010.

H. Niedermayer, R. Holz, M.-O. Pahl, G. Carle. *On using home networks and cloud computing for a Future Internet of Things*. Proc. 2nd Future Internet Symposium (FIS), Berlin, Germany, September 2009.

D. Haage, R. Holz, H. Niedermayer, P. Laskov. *CLIO—a cross-layer information service for overlay network optimization*. Proc. 16. Kommunikation in Verteilten Systemen (KiVS), Kassel, Germany, March 2009.

R. Holz, H. Niedermayer, P. Hauck, G. Carle. *Trust-rated authentication for domain-structured distributed systems*. Proc. 5th European PKI Workshop: Theory and Practice (EuroPKI), Trondheim, Norway, June 2008.

Publications in journals

H. Kinkelin, R. Holz, H. Niedermayer, S. Mittelberger, G. Carle. *On using TPM for secure identities in future home networks*. Future Internet 3(1):1–13. 2011.

D. Haage, R. Holz. *Towards measurement consolidation for overlay optimization and service placement*. Praxis der Informationsverarbeitung und Kommunikation (PIK), 10:12-15, March 2010.

O. Waldhorst, C. Blankenhorn, D. Haage, R. Holz, G. Koch, B. Koldehofe, F. Lampi, C. Mayer, S. Mies. *Spontaneous virtual networks: on the road towards the Internet's next generation*. it—Information Technology Special Issue on Next Generation Internet, 50(6):367-375, December 2008.

Invited talks and congress presentations

Managing security-relevant data from measurements on Internet scale. Invited talk at Workshop on Human-Centred Technologies, University of Sydney, Australia, June 2015.

The sorry state of our PKIs—using Internet-wide scans to determine and improve the state of TLS and SSH. Invited talk at University of Auckland, New Zealand, June 2014

The sorry state of our PKIs—using Internet-wide scans to determine and improve the state of TLS and SSH. Invited talk at NICTA, Sydney, Australia, June 2014.

One year of Crossbear (now with SSH, too!). Talk at 29th Chaos Computer Congress, Hamburg, Germany, December 2012.

The sorry state of X.509—from certification weaknesses to Man-in-the-middle-detection. Invited talk at University of Luxembourg, November 2012.

The sorry state of X.509—from certification weaknesses to Man-in-the-middle-detection. Invited talk at University of Trento, Italy, September 2012.

The SSL Landscape. Invited talk at University of Applied Sciences Hagenberg, Austria, March 2012.

The SSL Landscape. Invited talk at Hertz-Goertz-Institut, Ruhr-Universität Bochum, Germany, December 2011.

Investigating PKI: the OpenPGP Web of Trust, with a side order of X.509. Invited talk at RWTH Aachen University, Germany, September 2011.

Technical reports

R. Holz, C. P. Mayer, S. Mies, H. Niedermayer, M. A. Tariq. SpoVNet Security Task Force Report. Technical Report TM-2009-3, Universität Karlsruhe, Germany, December 2009.

R. Holz, H. Niedermayer. A protocol for inter-domain authentication with a trust-rating mechanism. Technical Report WSI-2008-02. Universität Tübingen, Germany, April 2008.

Thesis work

R. Holz. *Empirical analysis of Public Key Infrastructures and investigation of improvements.* Dissertation for PhD degree, Technische Universität München, Germany. December 2013.

R. Holz. *Secure domain-based Peer-to-Peer systems.* Thesis for completion of degree of Diplom-Informatiker. Universität Tübingen, Germany. October 2007.

R. Holz. *The Digizone project.* Advanced student research project, carried out at University of Loughborough, UK, summarising the results of my Academic Visitorship. Universität Tübingen, Germany. 2002.

Languages

German	Native tongue
English	Full professional proficiency
Italian	Professional working proficiency
Spanish	Elementary proficiency
French	Elementary proficiency