Ralph Holz

School of IT
Faculty of Engineering and IT
1 Cleveland St
University of Sydney NSW 2006
Sydney, Australia

Office: (2) 9036 9718
Mobile: (435) 349593
Fax: (2) 9351 3838

Email: ralph.holz@sydney.edu.au

Personal data

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

Research interests

My research interests revolve around security and network measurement, employing a decidedly empirical approach. My current focus is on global-scale measurement of the security of Internet services, from classic services such as the Web to modern technology such as blockchains.
My theme is real-world security: security is achieved only by technology that supports its human users. No matter how brilliant the technology, if humans find it hard to operate, it will be insecure. Similarly, technology is always used in a context (at home, in finance, etc.) and this context is important in understanding how a technology must designed. I employ a data-driven approach in designing and building secure systems, where measurement and data collection at both planetary and local scale provide the necessary foundation for solid, measurable, and deployable improvements.

Positions held

01/2016–ongoing **Lecturer in Networks and Security**
School of IT, Faculty of Engineering and IT, University of Sydney

01/2018–ongoing **Theme Leader Security & Communications**
Sydney Nano Institute

01/2016–ongoing **Node Leader Cybersecurity**
Human-Centred Technologies Cluster, Faculty of Engineering and IT

01/2016–ongoing **Contributed Staff**, Data61/CSIRO within USyd/Data61 DUCA program
03/2015–ongoing **Visiting Fellow**, University of New South Wales
12/2014–ongoing **Visiting Academic**, Technical University of Munich

12/2014–01/2016 **Researcher**
Mobile Systems and Software Systems research groups; BaDE Business Team
NICTA, ATP, Sydney, Australia
Projects: Research and development of systems to gather empirical data for the detection of attacks on security. Leading research efforts to develop and deploy secure deployment pipelines.

08/2014–11/2014 **Post-doctoral Research Associate**
Chair for Network Architectures and Services
Technical University of Munich
Projects: Large-scale measurements of DNS; distributed global scanning.

05/2014–07/2014 **Visiting Researcher**
NICTA, Sydney, Australia
Project: Inference of network topology from passive measurement data.

01/2014–05/2014 **Visiting Academic**
Chair for Network Architectures and Services
Technical University of Munich

Project: Attack detection in BGP.

01/2008–12/2013 **Research Associate and PhD student**

01/2010–12/2013 Chair for Network Architectures and Services
Technical University of Munich

01/2008–12/2009 Group previously based at University of Tübingen

Project work:

since 12/2011 **Crossbear**: automated detection and reporting of Man-in-the-middle attacks on TLS. **Won grant from Counterpart, USA**.

11/2010–11/2011 **ResumeNet**: network resilience (EU FP7.

01/2008–12/2009 **Spontaneous Virtual Networks**: overlay network measurement and security.

01/2010–09/2012 **Airbus Group**: design and development of novel cabin network.

04/2010–08/2010 **Nokia Siemens Networks**: analysis of IETF ALTO and DECADE for 4G.

04/2008–10/2008 **Nokia Siemens Networks**: privacy-preserving Identity Management for 3G/4G and formal analysis.

02/2002–04/2002 **Academic Visitor**
IMPACT Research Group, University of Loughborough, UK; UBC Media, London, UK. Hypermedia encoding for Digital Audio Broadcasting.

Education

01/2008–05/2014 **Doctoral student, Technical University of Munich**
PhD with highest distinction ('summa cum laude')
Advisor and first referee: Prof. Georg Carle, Technical University of Munich
Second referee: A/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. Analysed 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**
University of Tübingen, Germany
Degree: Diplom-Informatiker (= MSc., grade: 1.0—very good)
Focal areas: networks, security, neural networks
Thesis: 'Secure domain-based Peer-to-Peer networks'

10/2001–10/2004 Parallel studies of Romance Languages
Non-degree enrolment

10/1998–09/1999 **Studies of Mathematics and Theology**
University of Tübingen, Germany
Enrolment to become a teacher at secondary schools

Research projects

01/2018-12/2020 **Taipan: a block-chain with democratic consensus and validated contracts.**
ARC Discovery DP180104030.

01/2017-06/2018	**Setting the standard for consumer data sharing practices of top-rated health apps** Funded by Sydney Policy Lab.
06/2016-06/2018	**Measurement of dependability and vulnerability in digital ecosystems** Data61 Collaborative Research Project.
01/2017-12/2017	**Policy Scenarios for the Future(s) of Australian Cybersecurity** Funded by Sydney Policy Lab.
01/2017–12/2017	**Global activity analysis of blockchain transactions and smart contracts with the Blockchain Observatory** Funded by Early Career Researcher Grant 2017.
01/2016-12/2016	**Enabling data-driven security and privacy—a cross-disciplinary platform for observation and analysis** Funded by Major Equipment Grant 2016.
01/2016-06/2016	**Cybersecurity knowledge: empirical security analysis and research on data-driven security** Data61 Collaborative Research Project.
12/2011-11/2014	**Integration of Crossbear with OONI** Funded by Counterpart, USA.

Students

ongoing	**University of Sydney** **PhD students:** Mr Christopher Natoli (with Vincent Gramoli). Topic: consensus in blockchains. **Honours students:** Ms Deanna Arora, Ms Eve Martin-Jones. **Research students:** Mr Simon Koch, Ms Yue Han (research interns) Mr Benedikt Brandner (visiting Master by Research student from Technical University of Munich). **Graduations of research students**: 1 PhD, 4 Honours students, 1 Master (Research)
08/2014–11/2014	**Technical University of Munich** Graduations: 25 students at Bachelor and Master (research) level.

Teaching and teaching innovation

01/2016–ongoing	**School of IT, University of Sydney**
S2 2018	**COMP5617** Empirical Security Analysis and Engineering. Lecturer and coordinator.
S1 2018	**INFO3616** Principles of Security and Security Engineering. Lecturer and coordinator.
S1 2018	**FASS3998** Big Data, Algorithms, and Security. Unit developer and lecturer.
S2 2017	**COMP5617** Empirical Security Analysis and Engineering. Lecturer and coordinator.
S2 2017	**COMP5618** Applied Cybersecurity. Unit coordinator.

S2 2017 **COMP9121** Design of network protocols and distributed systems. Lecturer and unit coordinator.

S2 2016 **INFO5010** Empirical Security Analysis and Security Engineering. Lecturer and coordinator.

S2 2016 **COMP9121** Design of network protocols and distributed systems. Lecturer and coordinator.

Teaching Innovation

S1 2018 **FASS3998 Big Data, Algorithms, and Security.** Unit developer. Supported by Strategic Education Grant.

S1 2018 **INFO2222 Integrated IT: Usability and Security**. Unit developer.

S1 2018 **INFO3616 Principles of Security and Security Engineering.** Unit developer.

S2 2016 **INFO5010/COMP5617** Empirical Security Analysis and Engineering.

03/2015–ongoing **University of New South Wales**

every S2 **COMP9337** Securing Wireless Networks. Guest lecturer.

01/2010–11/2014 **Technical University of Munich**

every S2 **IN2101** Network Security: Designed, updated, and taught core parts (30%). Led tutorials; designed assignments.

every semester **IN0014/IN2107/IN4595** Seminar Innovative Internet Technologies and Mobile Communications/Future Internet. Supervisor.

2011 **iLab2** Internet Lab 2. Advisor and guest lecturer.

Service

12/2017–ongoing **Theme Leader Security, Communications, and Computing**, Sydney Nano Hub, University of Sydney.

12/2016-12/2017 **Special Studies Program Coordinator**, School of IT, University of Sydney

12/2016-12/2017 **Talented Students Program Coordinator**, with Faculty of Science, University of Sydney

2017 **Financial Chair**, Passive and Active Measurements 2017 (PAM)

2015 **Local Arrangements Chair** for IFIP Performance 2015

2015-2017 **TPC memberships**
Mobiquitious 2017, PAM 2017, SPBP 2017, LCN 2016-2018, IFIP SEC 2015-2016

Reviewer service

2009-2017 ACM TOPS (TISSEC), ACM SIGCOMM IMC, ACM CCR, Elsevier Computer & Security, IFIP Networking, IEEE N2S, Big Data Research, IEEE ICC, IFIP SEC, NetSys

Grants and awards

Taipan: a block-chain with democratic consensus and validated contracts. Recipients: Vincent Gramoli, Michel Raynal, Alan Fekete, Ralph Holz, Bernhard Scholz. ARC Discovery DP180104030, AUD 367,666. 2017.

Towards Smart Sydney: University-wide IoT Data Collection Platform Recipients: Wei Bao, Athman Bouguettaya, Vincent Gramoli, Ralph Holz, Uwe Roehm, Suranga Seneviratne, Bernhard Scholz, Kanchana Thilakrathna, Bing Zhou, Albert Zomaya. AUD 70,000. 2017.

A Cross-Continental Collaborative Network Security Lab. Recipient: Ralph Holz, Marc-Oliver Pahl. Strategic Education Grant 18052-2018, International Educational Collaborations. AUD 7,000. 2017.

Measurement of Dependability and Vulnerability in Digital Ecosystems. Recipient: Ralph Holz. Data61 Collaborative Research Project. 2017. Data61 commitment: FTE equivalent AUD 36,093. Hardware AUD 33,000 in-kind. 11,720 AUD research funding.

Setting the standard for consumer data sharing practices of top-rated health apps. Recipients: Quinn Grundy, Lisa Bero, Ralph Holz, Fabian Held, Judy Kay, Margaret Allman-Farinelli. Sydney Policy Lab Collaborative Project Award 2017. AUD 30,000.

Policy Scenarios for the Future(s) of Australian Cyber Security. Recipients: Frank Smith, Aim Sinpeng, Simon Atkinson, Ralph Holz, Jonathon Hutchinson, Sarah Logan, Hui Xue. Sydney Policy Lab Collaborative Project Award 2017. AUD 15,000.

Big Data, Algorithms, and Security in the Digital Age. Recipients: Frank Smith, Benedetta Brevini, Joe Dong, Ralph Holz. Strategic Education Grant Scheme 2017. University of Sydney. AUD 12,000.

Global activity analysis of blockchain transactions and smart contracts with the Blockchain Observatory. Recipients: Ralph Holz. Early Career Researcher Scheme 2017, Faculty of Engineering and Information Technologies, University of Sydney. AUD 36,500.

Enabling data-driven security and privacy—a cross-disciplinary platform for observation and analysis. Recipients: Uwe Roehm, Ralph Holz, Sanjay Chawla. Major Equipment Grant MES-2016-12, Faculty of Engineering and Information Technologies, University of Sydney. AUD 45,000. 2016.

Cybersecurity Knowledge: Empirical Security Analysis and Research on Data-Driven Security Engineering. Recipient: Ralph Holz. Collaborative Research Project NICTA/Data61. 2016. NICTA commitment AUD 33,000 hardware and 0.5 FTE in-kind; AUD 114,500 scholarships, AUD 13,869 research and travel funding.

Integration of Crossbear with the Open Observatory of Network Interference. Recipients: Ralph Holz, Georg Carle. Fixed Obligation Grant No. 1011-07, Counterpart International, USA. USD 19,980. 2011.

Peer-reviewed publications at conferences and workshops

Johanna Amann, Oliver Gasser, Quirin Scheitle, Lexi Brent, Georg Carle, Ralph Holz. *Mission accomplished? HTTPS security after DigiNotar*. Proc 17th ACM SIGCOMM Internet Measurement Conference (IMC). London, UK, November 2017. **Community Contribution Award**. Rank: Core A.

Jun Young Kim, Ralph Holz, Wen Hu, and Sanjay Jha. *Automated analysis of secure Internet of Things protocols*. Proc. Annual Computer Security Applications Conference (ACSAC). San Juan, Puerto Rico, USA, December 2017. Rank: Core A.

Ingo Weber, Vincent Gramoli, Alex Ponomarev, Mark Staples, Ralph Holz, An Binh Tran, Paul Rimba. *On availability for blockchain-based systems*. Proc. Symp. Reliable Distributed Systems (SRDS). Hong Kong, China, September 2017. Rank: Core A.

Dario Banfi, Olivier Mehani, Guillaume Jourjon, Lukas Schwaighofer, Ralph Holz. *Endpoint-transparent Multipath Transport with Software-defined Networks*. Proc. Local Computer Networks (LCN). Dubai, UAE, November 2016. Rank: Core A.

Ralph Holz, Johanna Amann, Olivier Mehani, Matthias Wachs, and Mohamed Ali Kafaar: *TLS in the wild-An Internet-wide analysis of TLS-based protocols for electronic communication*. Proc. Network and Distributed System Symposium (NDSS). San Diego, CA, USA, February 2016. Rank: Core A.

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. Rank: Core B.

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

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. Rank: Core A.

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. Rank: Core A.

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. Rank: Core B.

Peer-reviewed publications in journals

J. Schlamp, R. Holz, Q. Jacquemart, G. Carle, and E. W. Biersack. *HEAP: Reliable assessment of BGP Hijacking attacks*. IEEE J. Selected Areas of Communication (JSAC), Special Issue on Measuring and Troubleshooting the Internet: Algorithms, Tools, and Applications. 2016. Rank: A.

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.

Thesis work

R. Holz. *Empirical analysis of Public Key Infrastructures and investigation of improvements*. Dissertation for PhD degree, Technical University of Munich, Germany. December 2013.

R. Holz. *Secure domain-based Peer-to-Peer systems*. Thesis for completion of degree of Diplom-Informatiker. University of 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. University of Tübingen, Germany. 2002.

Technical reports

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

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

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.

Languages

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

References

Dr. Georg Carle, Professor, Department of Informatics, Technical University of Munich, Germany
carle@in.tum.de, +49 89 289 18030

Dr. Nick Feamster, Professor, School of Computer Science, Princeton University, USA
feamster@cs.princeton.edu, +1 609 258 2203

Dr. Alan Fekete, Professor, School of IT, University of Sydney
alan.fekete@sydney.edu.au, +61 9351 4287

Dr. Uwe Roehm, Assoc. Professor, School of IT, University of Sydney
uwe.roehm@sydney.edu.au, +61 9036 5305

Dr. Aruna Seneviratne, Research Director Cyber-Physical Systems, Data61/CSIRO, Australia
aruna.seneviratne@data61.csiro.au, +61 2 9376 2069

Dr. Liming Zhu, Research Director Software and Computational Systems, Data61/CSIRO, Australia
liming.zhu@data61.csiro.au, +61 2 9376 2138

Dr. Sanjay Jha, Professor, School of Computer Science and Engineering, University of New South Wales, Australia
sanjay@cse.unsw.edu.au, +61 2 9385 6471

Dr. Peter Hauck, Professor, Department of Computer Science, Universität Tübingen, Germany
hauck@informatik.uni-tuebingen.de, +49 7071 29 70466

Dr. James Sterbenz, Professor, University of Kansas and Lancaster University, USA/UK
jpgs@ittc.ku.edu

Dr. Sebastian Schinzel, Professor, University of Applied Sciences Münster, Germany
schinzel@fh-muenster.de, +49 2551 9-62188

Stefan Schneele, Airbus Group Innovations, Munich, Germany
Stefan.Schneele@eads.net, +49 89 607 24029