

# CURRICULUM VITAE

**Dr. Karsten Nohl**

nohl@virginia.edu

**RESEARCH INTERESTS:** microchip security, privacy protection, economics of information.

## PROFESSIONAL EXPERIENCE

Security Research Labs, Berlin	– Chief Scientist	since 02/2010
COREtransform, Berlin	– Director	04/2010 – 11/2010
McKinsey & Company, Berlin	– Senior Associate	11/2008 – 01/2010

## EDUCATION

University of Virginia, Charlottesville	01/2005 – 08/2008
PhD in Computer Engineering, GPA: 3.7	
Advisor: Prof. David Evans	
Indian Institute of Technology, Bombay – research assistant	06/2003 – 10/2003
University of Applied Sciences, Heidelberg	10/2001 – 09/2004
Major: Electrical Engineering, German GPA: 1.2 (~3.87)	

## SCHOLARSHIPS

Konrad Adenauer Stiftung	04/2002 – 09/2004
Studienstiftung des deutschen Volkes	11/2002 – 01/2006
e-fellows.net (Deutsche Telekom, McKinsey)	09/2003 – 10/2008
Microsoft Student Partner	12/2003 – 12/2004

## AWARDS

Louis T. Rader Graduate Research Award	04/2008
Dean's Summer Fellowship	05/2006 – 08/2006
Price of the School of Engineering, Heidelberg	10/2004
Diploma <i>summa cum laude</i> (German GPA 1.2)	09/2004
High School valedictorian	05/2001

## RESEARCH GRANTS

- Benton Calhoun, David Evans (PI), John Lach, Karsten Nohl, Abhi Shelat. *Implementable Privacy and Security for Resource-Constrained Devices*. NSF Cybertrust Grant, 2008 – 2012.

## PUBLICATIONS

- Karsten Nohl and David Evans. *Quantifying Information Leakage in Tree-Based Hash Protocols*. 8<sup>th</sup> International Conference on Information and Communications Security (ICICS), December 2006.
- Karsten Nohl. *Privacy through Noise: A Design Space for Private Identification*. Secure Component and System Identification Workshop (SECSI), March 2008

## CURRICULUM VITAE

- Karsten Nohl, Starbug, Henryk Plötz, and David Evans. *Reverse-Engineering a Cryptographic RFID Tag*. USENIX Security, August 2008
- Karsten Nohl and David Evans. *Hiding in Groups: On the Expressiveness of Privacy Distributions*. 23rd International Information Security Conference (SEC), Sep. 2008
- Karsten Nohl and David Evans. *Design Trade-Offs for Realistic Privacy* (Book Chapter). Paris Kitsos and Yan Zhang (Ed.): *RFID Security: Techniques, Protocols and System-On-Chip Design*
- Sean O’Neil, Karsten Nohl. *EnRupt* – a submission to the NIST SHA-3 Hashing Competition, August 2008
- Mate Soos, Karsten Nohl, and Claude Castelluccia. *Extending SAT Solvers to Cryptographic Problems*. Theory and Applications of Satisfiability Testing (SAT), July 2009
- Karsten Nohl, and David Evans. *Privacy through Noise: A Design Space for Private Identification*. Theory Annual Computer Security Applications Conference (ACSAC), December 2009
- Karsten Nohl, Erik Tews, Ralf-Philipp Weinmann. *Cryptanalysis of the DECT Standard Cipher*. International Workshop on Fast Software Encryption (FSE), February 2010
- Henryk Plötz, Karsten Nohl. *Peeling Away Layers of an RFID Security System*. Financial Cryptography, February 2011

### INVITED TALKS

- *RFID Privacy—Old Threats and New Attacks*. 6<sup>th</sup> HOPE Conference, NYC, July 21<sup>st</sup> 06
- *RFID Hacking* (with Henryk Plötz and z0ccor). 23<sup>rd</sup> Chaos Communication Congress (23C3), Berlin, December 28<sup>th</sup> 2006
- *Mifare—Little Security, Despite Obscurity* (with Henryk Plötz). 24<sup>th</sup> Chaos Communication Congress (24C3), Berlin, December 27<sup>th</sup> 2007
- *Why RFID Crypto Must not Rely on Obscurity*. CUSP RFID Security Workshop: From Theory To Practice, Baltimore, January 24<sup>th</sup> 2008
- *From Silicon to C: Reverse-Engineering Cryptographic Hardware*, University of Bochum, March 20<sup>th</sup> 2008
- *RFID Reverse-Engineering* (with Starbug). Easterhegg, Cologne, March 23<sup>rd</sup> 2008
- *Proprietary RFID Systems* (with Starbug). CanSecWest, Vancouver, March 27<sup>th</sup> 2008
- *The (Im)possibility of Hardware Obfuscation*. Univ. of Washington Seattle, March 31<sup>st</sup> 08
- *Exploiting Proprietary Cryptography*. Toorcon Seattle, April 19<sup>th</sup> 2008
- *Hardware Reverse-Engineering Workshop* (with Bunnie). Toorcon, April 20<sup>th</sup> 2008
- *Spotting Weak Cryptography*. Safety in numbers Symposium, Utrecht, June 20<sup>th</sup> 2008
- *The (Im)possibility of Hardware Obfuscation*. Last HOPE Conference, NYC, July 2008
- *Crippling Crypto: The Debian OpenSSL Debacle* (with Jacob Appelbaum, Dino Dai Zovi). The Last HOPE Conference, NYC, July 2008
- *Mifare—Little Security, Despite Obscurity*. BlackHat, Las Vegas, August 2008
- *The Risks of Wireless Technology*. Mobile Banking Security Conf., Vienna, Sep 2008
- *Disclosing Secret Algorithms from Hardware*. BlackHat Japan, Tokyo, Oct 2008
- *Chip Reverse Engineering* (with Starbug). 25<sup>th</sup> Chaos Communication Congress (25C3), Berlin, Dec 2008
- *Analyzing RFID Security* (with Henryk Plötz). 25C3, Berlin, Dec 2008

## CURRICULUM VITAE

- *A Security Expert's Perspective on Micro-Payment*. Workshop on Integrated Transportation Payment Systems, Boston, Feb 2009
- *Reverse-Engineering Silicon Chips*. CodeGate, Seoul, Korea, April 2009
- Three lectures on *GSM security, Microchip security, and Car Key Security*. HAR conference, Netherlands, Aug 2009
- *Silicon Chips: No More Secrets*. Pacsec, Tokyo, Nov 2009
- *Cracking GSM Encryption*. Deepsec, Vienna, Nov 2009
- *GSM – SRSLY? (with Chris Paget)*. 26C3, Berlin, Dec 2009
- *Legic Prime: Obscurity in Depth (with Henryk Plötz)*. 26C3, Berlin, Dec 2009
- *DECT Security Part II (with Erik Tews)*. 26C3, Berlin, Dec 2009
- *Do not trust your phone*. SISCTI, Monterrey, Feb 2010
- *Assessing the security risk of GSM technology*. Telecoms Fraud & Revenue Assurance Summit, London, March 2010
- *The Risks of Wireless Technology; Why NFC is not a Simple Upgrade*. WIMA Global NFC Summit, Monaco, April 2010
- *Hardening Identification Systems*. Secure Component and System Identification Workshop (SECSI), Cologne, April 2010
- *Attacking phone privacy*. BlackHat USA, Las Vegas, Aug 2010
- *Trusted Chips: No More Secrets*. Smart Event, French Riviera, Sep 2010
- *Car Immobilizer Security*. escar, Bremen, Nov 2010
- *GSM Debugging (with Dieter Spaar)*. Deepsec, Vienna, Nov 2010
- *The Hacker Perspective on Smart Cards*. CARTES, Paris, Dec 2010
- *GSM Sniffing (with Sylvain Munaut)*. 27C3, Berlin, Dec 2010
- *The Risks of NFC and GSM in Mobile Payment*. WIMA NFC Summit, Monaco, Apr 2011
- *GSM:SRSLY?*. BIG TECH DAY, Munich, May 2011
- *The Hacker Perspective on Meters*. Teletrust Smart Metering, Berlin, May 2011
- *Reviving smart card analysis (with Chris Tarnovsky)*. Black Hat, Las Vegas, Aug 2011
- *GPRS Intercept: Wardriving phone networks (with Luca Melette)*. Chaos Communication Camp, Finowfurt, Aug 2011
- *Reviving smart card analysis*. Chaos Communication Camp, Finowfurt, Aug 2011
- *GSM attack tools and defense trends*. govcert.nl workshop, Den Haag, Oct 2011

### REFERENCES

- Prof. David Evans, University of Virginia, <evans@cs.virginia.edu>  
David was my advisor at the University of Virginia and continues to be my most important research mentor and challenging partner.
- Prof. Christof Paar, Ruhr-University Bochum, <christof.paar@rub.de>  
Christof is both a role model to me for bridging industry and academia with his highly inspired research group. It is because of Christof that I am back in Germany.
- Dr. Jürgen Laartz, Senior Director at McKinsey, <juergen\_laartz@mckinsey.com>  
Jürgen led our seven-month cross-function project at a German telecommunications incumbent where we designed data quality measures and supported the rollout. He has since become an important career mentor.