Marc Stevens
Curriculum Vitae

Personal details

First name, surname:	Marc Stevens
Date of birth:	april 7, 1981
Nationality:	Netherlands
Telephone:	+31-6-38307119
E-mail:	marc.stevens@cwi.nl
Corresponding address:	Marc Stevens CWI – Centrum Wiskunde & Informatica P.O. Box 94079 1090 GB Amsterdam The Netherlands

Degrees

PhD

Title of thesis:	'Attacks on hash functions and applications'
University:	Mathematical Institute, Leiden University
Advisors:	prof. dr. Ronald Cramer, prof. dr. Arjen Lenstra (EPFL) & dr. Benne de Weger (TU/e)
Date of defense:	June 19, 2012

MSc

Title of thesis:	'On collisions for MD5'
University:	Faculty of Mathematics and Computer Science, Eindhoven University of Technology
Advisors:	prof. dr. Henk van Tilborg, dr. Benne de Weger & Gido Schmitz MSc (NBV, Dutch national communications security agency)
Date of defense:	August 28, 2007

Employment

June 2014 – now	Tenure-Track Researcher, Cryptology Group, Centrum Wiskunde & Informatica (CWI)
June 2012 – May 2014	Post-doctoral Researcher, Cryptology Group, Centrum Wiskunde & Informatica (CWI)
October 2007 – June 2012	PhD student, Cryptology Group, Centrum Wiskunde & Informatica (CWI) and Mathematical Institute, Leiden University
August 2007 – September 2007	Research intern, LACAL, École Polytechnique Fédérale de Lausanne (EPFL), Switzerland
September 2005 – May 2006	Research intern, NBV (Dutch national communications security agency), Voorburg
January 2004 – April 2004	Research intern, CITS, Ruhr-Universität Bochum, Germany

Grants, Honors and Awards

- *NWO (Netherlands Organization for Scientific Research) Veni Grant 2014*, PI, awarded 248k€ (NWO: 'Veni is targeted at outstanding researchers who have recently obtained their PhD')
- *Best Young Researcher Paper Award, 33rd Annual IACR CRYPTO 2013, Santa Barbara, CA, USA* (best paper authored solely by young researcher(s) not having received their PhD before 2011)
- Winner of the *KHMW Martinus van Marum prize 2013* of The Royal Holland Society of Sciences and Humanities (KHMW) for my PhD thesis and other publications (awarded once every 5 years within Astronomy, Computer Science, Mathematics and Physics)
- *NWO Vrije Competitie Grant 2012*, Co-PI, awarded 216k€
- *Best Paper Award, 29th Annual IACR CRYPTO 2009, Santa Barbara, CA, USA*
- *Eindhoven University of Technology – Afstudeerprijs 2008* (best master's thesis university-wide)
- Graduated Applied Mathematics *cum laude* (2007)

Publications

- Marc Stevens, Pierre Karpman, and Thomas Peyrin, *Freestart collision for full SHA-1*, 35th Annual IACR EUROCRYPT (Marc Fischlin and Jean-Sébastien Coron, eds.), Lecture Notes in Computer Science, vol. 9665, pp. 459–483, Springer, May 2016, Vienna, Austria.
- Max Fillinger, and Marc Stevens, *Reverse-engineering of the cryptanalytic attack used in the Flame super-malware*, 21st Annual IACR ASIACRYPT (Tetsu Iwata and Jung Hee Cheon, eds.), Lecture Notes in Computer Science, vol. 9453, pp. 586–611, Springer, December 2015, Auckland, New Zealand.

- Pierre Karpman, Thomas Peyrin, and Marc Stevens, *Practical free-start collision attacks on 76-step SHA-1*, 35th Annual IACR CRYPTO (Rosario Gennaro and Matthew Robshaw, eds.), Lecture Notes in Computer Science, vol. 9215, pp. 623–642, Springer, August 2015, Santa Barbara, CA, USA.
- Marc Stevens, *Counter-Cryptanalysis*, 33rd Annual IACR CRYPTO (Ran Canetti and Juan A. Garay, eds.), Lecture Notes in Computer Science, vol. 8042-I, pp. 129–146, Springer, August 2013, Santa Barbara, CA, USA. **Best young researcher paper award**.
- Marc Stevens, *New Collision Attacks on SHA-1 Based on Optimal Joint Local-Collision Analysis*, 32nd Annual IACR EUROCRYPT (Thomas Johansson and Phong Q. Nguyen, eds.), Lecture Notes in Computer Science, vol. 7881, pp. 245–261, Springer, May 2013, Athens, Greece.
- Marc Stevens, Arjen K. Lenstra, and Benne de Weger, *Chosen-prefix collisions for MD5 and applications*, International Journal of Applied Cryptography, IJACT, vol. 2012-**2**, no. 4, Inderscience 2012, 322–359.
- Marc Stevens, *Advances in Hash Function Cryptanalysis*, Marc Stevens, ERCIM, Vol. 90, July, 2012.
- Marc Stevens, *Single-block collision attack on MD5*, Cryptology ePrint Archive, Report 2012/040. **Winner of Tao Xie and Dengguo Feng's $5,000 challenge**: `http://eprint.iacr.org/2010/643`.
- Marc Stevens, Alexander Sotirov, Jacob Appelbaum, Arjen K. Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger, *Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate*, 29th Annual IACR CRYPTO (Shai Halevi, ed.), Lecture Notes in Computer Science, vol. 5677, pp. 55–69, Springer, August 2009, Santa Barbara, CA, USA. **Best paper award**.
- Marc Stevens, *Breaking the Weakest Link: Becoming a Trusted Authority on the Internet*, ERCIM, Vol. 77 April, 2009.
- Marc Stevens, Arjen K. Lenstra, and Benne de Weger, *Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities*, 26th Annual IACR EUROCRYPT (Moni Naor, ed.), Lecture Notes in Computer Science, vol. 4515, pp. 1–22, Springer, May 2007, Barcelona, Spain.
- Marc Stevens, *Fast Collision Attack on MD5*, Cryptology ePrint Archive, Report 2006/104.
- Tanja Lange and Marc Stevens, *Efficient Doubling on Genus Two Curves over Binary Fields*, 11th Annual Workshop on Selected Areas in Cryptography (Helena Handschuh and M. Anwar Hasan, eds.), Lecture Notes in Computer Science, vol. 3357, pp. 170–181, Springer, August 2004, Waterloo, Ontario, Canada.

Invited Talks (selected)

- Keynote lecture, SHARCS 2012, Washington D.C., USA, March 2012, *Cryptanalysis of MD5 and SHA-1.*
- Keynote lecture, 80th Anniversary of Breaking the Enigma Code - Return to the Roots, Warsaw, Poland, November 2012, *Cryptanalysis of MD5 and SHA-1.*
- Invited lecture, NLUUG Voorjaarsconferentie 2016, Utrecht, The Netherlands, *Bitcoin and the Security of the Blockchain*

- Invited lecture, Security in Times of Surveillance 2015, Eindhoven, The Netherlands, *Need Security Against Digital Signature Forgeries*
- Invited lecture, TCCM-CACR 2013, Tianjin, China, August 2013, *Analysis of Truncated Differential Paths and Local Collisions*
- Invited lecture, ASK 2013, Wei Hai, China, August 2013, *Improving Counter-Cryptanalysis*
- Invited lecture, Real World Crypto 2013, Stanford, January 2013, *Counter-cryptanalysis: analyzing Flame's new collision attack.*
- Invited lecture, Technion, Israel, November 2013, *Improving Counter-Cryptanalysis*
- Invited lecture, Tsinghua University, China, September 2013, *Improving Counter-Cryptanalysis*
- Invited lecture, National Cyber Security Center, March 2013, Netherlands, *Counter-cryptanalysis: analyzing Flame's new collision attack*

Scientific Activities (selected)

- Editorial Board member of IACR Transactions on Symmetric Cryptology
- Program Committee member of CT-RSA 2017, 2016
- Program Committee member of IACR FSE 2017, 2016
- Program Committee member of IACR CRYPTO 2014
- Program Committee member of IACR ASIACRYPT 2014
- Program Subcommittee member of Hash-track ISC'07
- General Chair of IACR PKC 2017
- Scientific co-organizer of the CWI RISC Seminar

Software

- Marc Stevens, *Collision Detection Library*, C Library and command line utility to detect cryptanalytic collision attacks on MD5 & SHA-1, 2013,
  `https://marc-stevens.nl/research/`.
- Marc Stevens, *HashClash project*, an open-source C++ framework for MD5 & SHA-1 differential path construction and chosen-prefix collisions for MD5, 2009–2011,
  `http://code.google.com/p/hashclash`.

Supervision

- Rusydi Makarim, PhD student, Mathematical Institute Leiden & CWI Amsterdam, The Netherlands, 2014–2017.
- Huaifeng Chen, visiting PhD student (3 months), CWI Amsterdam, The Netherlands, 2015.
- Fatemeh Sefi Shahpar, visiting PhD student (5 months), Mathematical Institute Leiden, The Netherlands, 2015.
- Maximillian Fillinger, MSc thesis, University of Amsterdam, 2013.

Media (selected)

Media Articles on the "SHAppening" (selection)

- Ars Technica, *SHA1 algorithm securing e-commerce and software could break by year's end*, Dan Goodin, October 8, 2015.
- SC Magazine, *Researchers say SHA-1 will soon be broken, urge migration to SHA-2*, Teri Robinson, October 10, 2015.
- The Register, *Crypto cadre cloud-cracks SHA-1 with just $75k of compute cost*, Darren Pauli, October 9, 2015.

Media Articles on the Flame discovery (selection)

- BBC News Technology, *Flame malware makers send 'suicide' code*, June 8, 2012.
- EuroTech, *Years of Secret Cryptographic Research Uncovered In 0.02 Seconds*, Max Huijgen, June 20, 2012.
- PC World, *"Flame's Windows Update Hack Required World-class Cryptanalysis, Researchers Say"*, Lucian Constantin, June 8, 2012.
- CWI News, *CWI cryptanalyst discovers new cryptographic attack variant in Flame spy malware*, Marc Stevens, June 2012.
- Techweek Europe, *"Microsoft 'Oversight' Helped Flame Spread"*, Tom Brewster, June 8, 2012.

Media Articles on the Rogue Certification Authority construction (selection)

- Le Monde, *L'algorithme MD5 utilisé par de nombreux sites n'est pas fiable*, Catherine Vincent, January 2, 2009.
- NRC, *De sleutel van de bank ligt voor het grijpen*, Margriet van der Heijden, December 30, 2008.
- The New York Times, *Outdated Security Threatens Web Commerce*, John Markoff, December 30, 2008.
- The Washington Post, *One Weak Link to Rule Them All*, Brian Krebs, December 30, 2008.

Media Articles Other (selection)

- NRC weekblad, *Tien beloftes voor de jaren 10* (ten talents of the tenties), Carola Houtekamer and Jannetje Koelewijn, December 19–23, 2009.
- Science Magazine, *Cryptologists Cook Up Some Hash for New 'Bake-Off'*, Dana Mackenzie, vol. 319, no. 5869, pp. 1480–1481, March, 2008.
- The Economist, Technology Quarterly, *Making a total hash of it*, Bas den Hond, March 6, 2008.

References

- prof. dr. Ronald Cramer, Cryptology Group, Centrum Wiskunde & Informatica (CWI) and Mathematical Institute, Leiden University, e-mail: `ronald.cramer @ cwi.nl`