

# Michael (Mike) K. Just

10 Glencairn Crescent  
Edinburgh, UK  
EH12 5BS

Mobile: +44 (0)796 078 1311  
Email: [justmikejust@gmail.com](mailto:justmikejust@gmail.com)  
Homepage: <http://homepages.inf.ed.ac.uk/mjust/>

## Summary

I have worked for more than 10 years in both the public and private sectors and have significant experience in the following areas:

- Computer security analysis and design

- Government policy and international standards development

- Technology assessments, trends analysis, and architecture development.

Most notably, I designed the Government of Canada's authentication recovery solution that is used to authenticate approximately 6 million Canadian citizens and businesses accessing federal government services.

During this time, I have continued to teach academically, publish scholarly research, participate on conference committees, and supervise students (formally and informally). Specifically, I have

- Taught 6 university-level, semester courses.

- Penned more than 20 publications.

- Delivered more than 25 formal presentations.

- Participated on 8 conference program committees.

My publications and continued research interests include applied cryptography, authentication, computer security, economics of security, human-computer interaction, and privacy. I am one of the world's leading researchers studying the security and usability of challenge question authentication systems.

Throughout my career, I have constantly strived to broaden my knowledge and experience. My work has varied from "hands-on" technical to delivering strategic policy direction. My current research is very interdisciplinary, combining my technical security knowledge with more social aspects related to usability and economics. I possess good communication skills and have experience with managing and motivating diverse teams. My current employment and education credentials are listed below.

My current employment is as follows

- Visiting Research Fellow, University of Edinburgh. October 2008 to present (part-time).

- Senior Advisor, Canadian Federal Government. August 2008 to present (part-time).

My academic qualifications are as follows

- Doctor of Philosophy (Ph.D.), Computer Science, Carleton University. 1998.

## Education

Doctor of Philosophy (Ph.D.) Computer Science. 1999.

School of Computer Science, Carleton University (Ottawa, ON, Canada).

DISSERTATION: On the Temporal Authentication of Digital Data

My dissertation centred on technologies and processes to solve problems related to notarizing and *time associating* digital data. This work resulted in two refereed conference publications. My knowledge and expertise in this area were leveraged greatly during my tenure as a Research Scientist at Entrust, Inc.

*Supervisors:* Dr. Paul Van Oorschot, Dr. Evangelos Kranakis,

*External Examiner* Dr. Aviel Rubin.

Master of Computer Science (M.C.S.). 1994.

School of Computer Science, Carleton University (Ottawa, ON, Canada).

DISSERTATION: Methods of Multi-Party Cryptographic Key Establishment

My dissertation centred on problems related to secure teleconferencing among more than two people. This work resulted in two refereed conference publications.

*Supervisor:* Dr. Evangelos Kranakis

Bachelor of Science (B.Sc.) Computer Science. 1992.

Department of Mathematics and Computer Science, Laurentian University (Sudbury, ON, Canada).

## Grants and Awards

### GRANTS

Engineering and Physical Sciences Research Council (EPSRC) (United Kingdom). Standard Research Grant (EP/G020760/1), entitled *Knowledge-Based Authentication: Evaluating and Improving*, and worth £65,253. Principal Investigator: D. Aspinall. Visiting Fellow: **Mike Just**. October 2008 to September 2009.

### FELLOWSHIPS AND SCHOLARSHIPS

Natural Sciences and Engineering Research Council (NSERC) (Canada). PGS-B Graduate Scholarship. \$17,000 for each of first two years of doctoral studies. September 1994 to August 1996.

Natural Sciences and Engineering Research Council (NSERC) (Canada). PGS-A Graduate Scholarship. \$15,600 for each of two years of Master's studies. September 1992 to August 1994.

Laurentian University Entrance Scholarship (Canada). \$1,000 for first year of undergraduate studies. September 1988 to April 1989.

## Academic Employment Experience

### VISITING RESEARCH FELLOW, UNIVERSITY OF EDINBURGH

October 2008 to present. Part-time (3 days per week).

Laboratory for Foundations in Computer Science (LFCS), School of Informatics, University of Edinburgh

I am working to evaluate and improve methods for knowledge-based authentication that rely upon information *already known* to users, such as challenge questions or shared secrets, as opposed to ‘memorized’ information such as passwords. The work involves leading user experiments to evaluate usability, and developing systematic analysis tools to determine the security of these techniques. I am one of the leading researchers in the world studying this area.

### SESSIONAL LECTURER, SCHOOL OF COMPUTER SCIENCE, CARLETON UNIVERSITY

*Course:* Applied Cryptography. January to April 2008.

*Course:* Applied Cryptography. January to April 2007.

*Course:* Applied Cryptography. January to April 2006.

*Course:* Computer Security and Cryptography. January to April 2002.

*Course:* Computer Security and Cryptography. January to April 2001.

*Course:* Discrete Mathematics. January to April 1995.

*Applied Cryptography* is an advanced course for fourth year undergraduates on the application of cryptographic methods to computer security. It includes traditional topics such as symmetric and public key cryptography, as well as secret sharing, authentication, and key distribution.

*Computer Security and Cryptography* is an advanced course for fourth year undergraduates, as well as Masters and Doctoral graduate students covering network and computer security (e.g., email and web security, firewalls, IPSec), as well as practical applications of cryptography (e.g., public key cryptosystems, key management).

*Discrete Mathematics* is an introductory course for first year undergraduate students covering topics such as propositional and predicate calculus, Boolean algebra, algorithm complexity, mathematical reasoning, counting, recurrences, relations, and graphs.

Responsibilities for all courses included preparing and delivering three hours of lectures over 13 weeks to classes that varied in size from 10 to 120 students, as well as setting assignments, tests and exams.

### TEACHING ASSISTANT, CARLETON UNIVERSITY

School of Computer Science, Carleton University. September 1992 to August 1998.

*Courses:* Various undergraduate Computer Sciences courses including Discrete Mathematics, C Programming, and Algorithms and Complexity.

Responsibilities included marking assignments, projects and exams, in addition to leading laboratory sessions.

## Research Experience in Industry and Government

### APPLIED RESEARCH IN INNOVATION, ARCHITECTURE & STANDARDS - CANADIAN GOVERNMENT

I've held several government positions involving the application of research to areas of innovative technology, architecture and standards development. Positions were held at the Information Technology Services Branch of the Department of Public Works and Government Services Canada, unless otherwise noted.

#### SENIOR TECHNOLOGY ADVISOR, AUGUST 2008 TO PRESENT. Part-time (2 days per week)

I research and analyse emerging and innovative technologies for the Government of Canada's shared services organization. The results of my work contribute to the technology direction for the organization. Recent work involves the study of Virtual Worlds (such as Second Life) as a potential government service offering for cost-effective communication and collaboration.

#### DIRECTOR OF TECHNOLOGY STRATEGY AND INNOVATION, MARCH 2006 TO AUGUST 2008

I led a 15-person team (with an annual budget of more than \$2M) tasked with researching and developing emerging and innovative technology solutions for the Government of Canada's shared services organization. This included the study of relevant trends, development of technology roadmaps, and operation of a state-of-the-art test lab facility. Notable projects include the establishment of a wireless proof-of-concept in support of a study into future work environments, and the establishment of a cross-departmental wiki supporting improved communication and collaboration.

#### MANAGER OF IDENTITY MANAGEMENT RESEARCH, OCTOBER 2005 TO MARCH 2006

I led a team responsible for researching and developing strategies and architectures for delivering identity and role-based management services to Canadian citizens, businesses and federal civil servants. This included leading an interdisciplinary "Outcomes Management" exercise with participation from 16 government organizations in order to develop the strategic vision and tactical plans for our work.

#### SENIOR IT POLICY STRATEGIST, JUNE 2004 TO OCTOBER 2005

I was responsible for researching and developing strategic direction for several key components of the federal government's information technology infrastructure. In particular, I lead a project to research and analyze the policy impacts of our organization moving to a model of offering shared IT services to other government departments, including services for desktop deployment, networks and security.

#### IT SECURITY STANDARDS ANALYST, OCTOBER 2002 TO JUNE 2004

At the *Treasury Board of Canada Secretariat*, I was responsible for developing federal information technology security standards, including co-authoring the government's Management of Information Technology Security standard. I also researched and designed various security technology features for the federal governments 'Government OnLine (GOL)' initiative, including the solution for authenticating citizens. This solution is in operation today as part of the government of Canada's *epass* authentication system.

### RESEARCH SCIENTIST, ENTRUST, INC.

October 1997 to October 2002

I performed numerous duties related to the research and development of Entrust's encryption, authentication and access control products. Specifically, the work from my PhD thesis formed the basis of the design of Entrust's time stamping and notarization products. I also represented the organization on several international standards committees, including the Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C). I was the co-coordinator of the company's patent program, encouraging inventive ideas from co-workers and interacting with patent agents during patent filing.

## Publications

(A '\*' denotes publications for which I gave the corresponding presentation.)

### IN SUBMISSION

**M. Just**, D. Aspinall, *Challenging Challenge Questions: Implications for Testing and Deployment of Authentication Technologies*, in submission to *Policy and Internet Journal*, June 2009. (Invited submission based upon accepted presentation to *Trust 2009* Workshop. University of Oxford, Oxford, UK. April 2009.)

### PAPERS IN REFEREED JOURNALS AND MAGAZINES

**M. Just**, *Designing and Evaluating Challenge Question Systems*, IEEE Security & Privacy 2(5): 32-39 (2004). (L. Faith-Cranor, S. Garfinkel, editors).

### PAPERS IN PROCEEDINGS OF REFEREED CONFERENCES

J. Bonneau, **M. Just**, G. Matthews, "What's in a Name? Evaluating Statistical Attacks Against Personal Knowledge Questions," to appear in *Proceedings of the Fourteenth International Conference on Financial Cryptography and Data Security 2010*, LNCS. (19 of 130 submissions accepted for *full paper* publication: 14.6%)

**M. Just\***, D. Aspinall, "Personal Choice and Challenge Questions: A Security and Usability Assessment," in *Proceedings of the 5th ACM Symposium on Usable Privacy and Security (SOUPS) 2009*. (15 of 49 submissions accepted for publication: 31%)

**M. Just\***, D. Rosmarin, "Meeting the Challenges of Canadas Secure Government Service Delivery," in *Proceedings of 4th Annual PKI Research Workshop*, NISTIR 7224, NIST, August 2005.

C. Adams, **M. Just**, "PKI: Ten Years Later," in *Proceedings of the 3rd Annual PKI Research Workshop*, (K. Sankar, N. Hastings, W. Polk, editors), NISTIR 7122, NIST, August 2004.

**M. Just**, E. Kranakis, T. Wan, "Resisting malicious packet dropping in wireless ad-hoc networks using distributed probing," in *Proceedings of ADHOC-NOW 03*, Lecture Notes in Computer Science (LNCS) 2865, Springer, 2003. (27 of 42 submissions accepted for publication: 64%)

**M. Just\***, P. van Oorschot, "Addressing the problem of undetected signature key compromise," in *Proceedings of the Network and Distributed System Security Symposium, NDSS 1999, San Diego, California, USA*. The Internet Society, 1999.

**M. Just\***, "Some timestamping protocol failures," in *Proceedings of the Network and Distributed System Security Symposium, NDSS '98, San Diego, California, USA*. The Internet Society, 1998. (15 of 45 submissions accepted for publication: 33%)

**M. Just\***, S. Vaudenay, "Authenticated multi-party key agreement," in *Advances in Cryptology: Proceedings of Asiacrypt '96*, Lecture Notes in Computer Science (LNCS) 1163, Springer-Verlag, 1996. (31 of 124 submissions accepted for publication: 25%)

**M. Just\***, E. Kranakis, D. Krizanc, P. van Oorschot, "On key distribution via true broadcasting," in *Proceedings of the 2nd ACM Conference on Computer and Communications Security (ACM CCS '94)*, ACM, 1994. (31 of 70 submissions accepted for publication: 40%)

## BOOK CHAPTERS AND ARTICLES

**M. Just**, *Usable Challenge Question Authentication Systems*, in *Security and Usability: Designing Secure Yet Secure Systems That People Can Use*, O'Reilly, Laurie Faith-Cranor, Simson Garfinkel, editors, 2005.

**M. Just**, “Challenge-response protocol,” in *Encyclopedia of Cryptography and Security*, Kluwer, Henk van Tilborg, editor, 2005.

**M. Just**, “Diffie-Hellman key agreement,” in *Encyclopedia of Cryptography and Security*, Kluwer, Henk van Tilborg, editor, 2005.

**M. Just**, “Key Agreement,” in *Encyclopedia of Cryptography and Security*, Kluwer, Henk van Tilborg, editor, 2005.

**M. Just**, “Needham-Schroeder Protocols,” in *Encyclopedia of Cryptography and Security*, Kluwer, Henk van Tilborg, editor, 2005.

**M. Just**, “Schnorr Identification Protocol,” in *Encyclopedia of Cryptography and Security*, Kluwer, Henk van Tilborg, editor, 2005.

## PAPERS ACCEPTED TO WORKSHOPS WITHOUT PUBLISHED PROCEEDINGS

**M. Just\***, D. Aspinall, “Challenging Challenge Questions,” accepted at *Trust 2009*, University of Oxford, Oxford, UK, April 2009.

**M. Just\***, J. Weigelt, “Deriving Secure Service Profiles from Generic Threat and Risk Assessments,” accepted at *4th International Common Criteria Conference*, Stockholm, Sweden, September 2003.

**M. Just\***, “An Overview of Public Key Certificate Support for Canada’s Government On-Line (GOL) Initiative,” accepted at *2nd Annual PKI Research Workshop*, Gaithersburgh, Maryland, April 2003.

**M. Just\***, “Designing Secure Yet Usable Credential Recovery Systems Using Challenge Questions,” accepted at *Workshop on Human-Computer Interaction and Security Systems (affiliated with CHI 2003)*, Fort Lauderdale, Florida, April 2003.

A. Aarnes, **M. Just**, H. Meijer, S. Lloyd, S. Knapskog, “Selecting revocation solutions for PKI,” accepted at *The Fifth Nordic Workshop on Secure IT Systems (NORDSEC 2000)*, Reykjavik, Iceland, October 2000.

## PATENTS

**M. Just**, “Method and apparatus for providing information security to prevent digital signature forgery,” US Patent Number 7,373,512. Issued May 13, 2008.

**M. Just**, P. van Oorschot, “Apparatus and method for reducing transmission bandwidth and storage requirements in a cryptographic security system,” US Patent Number 6,567,914. Issued May 20, 2003.

*Additional patents pending ...*

## INTERNATIONAL STANDARDS

D. Gustafsson, **M. Just**, M. Nystrom, “SACred (Securely Available Credentials) Credential Server Framework,” Internet Engineering Task Force (IETF) Request for Comments (RFC) 3760, April 2004.

F. Hirsch, **M. Just**, “XML Key Management Requirements,” World Wide Web Consortium (W3C) Note, 5 May 2003.

**M. Just**, K. Leclair, J. Sermershein, M. Smith, “LDAPv3 Result Codes: Definitions and Appropriate Use,” Internet Engineering Task Force (IETF) Internet Draft, April 2000. (The content of this draft was eventually incorporated as an appendix of the LDAP v3 standard.)

## Presentations

### KEYNOTE PRESENTATIONS

“Account Recovery: Authentication’s Dirty Secret?”, Information Security Summit 2009, Prague, Czech Republic, 28 May 2009.

### INVITED TALKS

“Secure and Usable Authentication,” Scottish Networking Event (SCONE), University of Strathclyde, Glasgow, Scotland, 10 September 2009.

“Personal Choice and Challenge Questions: A Security and Usability Assessment,” Digital Security Seminar Series, Carleton University, Ottawa, Canada, 13 July 2009.

“On the Security and Usability of Challenge Questions,” Faculty of Informatics Seminar, Masaryk University, Brno, Czech Republic, 29 May 2009.

“Whither Challenge Question Authentication?”, Security Seminar Series, University of Cambridge, 12 May 2009.

“Challenging Challenge Questions,” Laboratory for Foundations of Computer Science (LFCS) ‘Lab Lunch,’ University of Edinburgh, 10 March 2009.

“Challenge Question Authentication,” Department of Computing Science Seminar Series, University of Glasgow, 25 February 2009.

“Challenge Questions: Authentication’s Weakest Link,” Institute for Communicating and Collaborative Systems (ICCS) Seminar Series, University of Edinburgh, 13 February 2009.

“Open Source in Government,” Open Source Software Symposium, Carleton University, 16 March 2007.

“Password Management for Multiple Accounts: Some Security and Usability Considerations,” DIMACS Workshop on Usable Privacy and Security Software (WUPSS), Rutgers, University, Piscataway, NJ, 7-9 July 2004.

“Jeopardy! IT Security Style,” Government Security Policy (GSP) Conference IT Security Session, Ottawa, ON, 11 February 2004.

“Threat and Risk Assessments: Three Wise Mens Views,” ISSA panel discussion, Ottawa, Canada, 29 May 2003 (with Jacques Adams-Robenhymmer and Hugh Ellis).

“Process Improvements for Large-Scale Threat and Risk Assessments,” Communications Security Establishment (CSE) Symposium, Ottawa, Canada, 15 May 2003.

“Enhanced Password Security,” Seminar on Networks, Ottawa, Canada, March 2002.

“Wireless Security,” ISSA - Minnesota Chapter, Sept 18, 2001 (cancelled due to 9/11).

“An Overview of User Authentication Techniques,” CITO TechTalk Workshop, Toronto, Ontario, March 2001.

“Technology Options for Securely Delivering Government Services to Citizens,” Government Technology (GovTech) Conference, October 1999.

“Techniques for Digital Timestamping,” Canadian Applied Mathematics Society (CAMS ’97), Toronto, Ontario, May 1997.

#### GUEST LECTURES AND TUTORIALS

“Usability and Security,” Guest Lecture, Human Computer Interaction (HCI) course, School of Informatics, University of Edinburgh, 5 November 2009.

“Network Security,” Guest Lecture, Computer Networks course, School of Informatics, University of Edinburgh, 19 & 22 October 2009.

“Security and Usability,” Guest Lecture, Computer Security course, School of Informatics, University of Edinburgh, 9 February 2009.

“Usability and Security,” Guest Lecture, Human Computer Interaction (HCI) course, School of Informatics, University of Edinburgh, 28 October 2008.

“Usable Authentication Techniques,” Guest Lecture, Authentication and Software Security course, School of Computer Science, Carleton University, 27 October 2003.

“Designing Usable Security Solutions,” MITACS 4th Annual Conference: Mathematics of Risk and Security, Student Tutorial (1/2 day), Ottawa, Canada, 11 May 2003.

#### POSTERS

“Transforming How We Authenticate People: Greater Protection and Increased Adoption,” Poster for *Scottish Informatics and Computer Science Alliance (SICSA) DemoFest*, University of Edinburgh, 24 November 2009.

“KBA: Trustworthy and Usable Authentication,” Poster for *Lifting the Lid Technology Showcase for SMEs*, University of Edinburgh, 19 November 2008.

## Professional Activities

### ADJUNCT RESEARCH PROFESSOR

School of Computer Science, Carleton University. July 2003 to June 2006.

My activities included lecturing a course, participating in research activities of the Digital Security Group, and serving on the Ph.D. thesis committee for one student.

### STUDENT SUPERVISION AND REVIEW

Gavin Keighren. Member of Ph.D. Review committee. School of Informatics, University of Edinburgh. Project Title: *Information-Flow Analysis for Security APIs*. Expected completion: September 2010.

Simon Le Parc. Supervision of M.Sc. Informatics. School of Informatics, University of Edinburgh. Project Title: *Next Generation Authentication*. Expected completion: December 2009.

Sharmila Mukherjee. Supervision of M.Sc. Informatics. School of Informatics, University of Edinburgh. Project Title: *Security and Privacy in Pervasive Computing*. Expected completion: December 2009.

Justin Zhan. Member of Ph.D. Review committee. School of Information Technology and Engineering (SITE), University of Ottawa. Completed 2006.

### REFEREEING

I am a frequent reviewer of articles submitted to several journals, including IEEE Transactions on Dependable and Secure Computing and IEEE Transactions on Information Forensics and Security.

### PROGRAM AND ORGANIZING COMMITTEE PARTICIPATION

British Human Computer Interaction (HCI). Review Committee: 2009.

Selected Areas in Cryptography (SAC). Program Committee: 2009.

Financial Cryptography. Program Committee: 2005.

Selected Areas in Cryptography (SAC). Program Committee: 2004.

Workshop on Privacy and Security Aspects of Data Mining. Program Committee: 2004.

Selected Areas in Cryptography (SAC). Organizing Committee: 2003.

ADHOC NetWorks and Wireless (ADHOC-NOW). Program Committee: 2003.

ADHOC NetWorks and Wireless (ADHOC-NOW). Program Committee: 2002.

ACM Conference on Computer and Communications Security (CCS). Program Committee: 1999.

Selected Areas in Cryptography (SAC). Program Committee: 1997 (**co-chair**).

Selected Areas in Cryptography (SAC). Organizing Committee: 1997.

Selected Areas in Cryptography (SAC). Organizing Committee: 1995.

## Miscellaneous

I am a member of the ACM, British Computer Society, IEEE, and IEEE Computer Society.

Languages: Native English speaker. I have an intermediate ability to communicate in French.

Interests: I enjoy walking, hiking and biking. I also have a black belt in Karate.

Music: I play the acoustic guitar and am currently learning to play the piano. I am also member of The Practice Choir in Edinburgh, Scotland and am interested in performing music.