

1 Partridge Drive
Bar Hill
Cambridge CB23 8EN
Born: 1974

Phone: 07889 321 089
dancvrcek@gmail.com
Nationality: Czech

Dr Dan Cvrcek is an experienced information security practitioner with over ten years experience working, researching, and teaching in the field. He has held positions at University of Cambridge, Brno University of Technology, and Masaryk University. He preferred hands-on projects and research with practical applications to purely theoretical ones. He left academia in April 2008 and started working at a security consultancy practice of Deloitte UK. He is able to quickly understand large and complicated systems and as such he profiled himself particularly as an expert on architectures of complex security and cryptographic systems as well as operational issues determining the cost of running such systems.

Work Experience

Deloitte UK, Security Privacy and Resiliency Apr 08 – present
Senior consultant, mainly subject matter expert in cryptography related projects for major UK banks: cryptographic standards, attestations / validations (VISA, Bacstel), cryptographic systems' architectures (Faster Payments, PIN processing systems, SWIFT, CHAPS, PKI based systems), deployment of public key infrastructures.

University of Cambridge, Computer Laboratory, UK Jan 07 – Mar 08
Post doctoral researcher working with Dr Frank Stajano on the project *WINES* (Wired and Wireless Intelligent Networked Systems) *Infrastructure*, responsible for the security analysis of hardware and software platforms for sensor networks. The analysis covered cryptographic mechanisms, routing algorithms, reverse engineering and code quality assesment, and practical issues related to deployment of the networks in London Underground, and at Humber Bridge.

Brno University of Technology, Czech Republic Jan 05 – Dec 06 and Oct 02 – Aug 03
Assistant and then associate professor responsible for various teaching and research activities. He taught courses including Algorithms & Data Structures, Programming Languages, Cryptography, and Information Security. He still holds the position as he is advising PhD students.

University of Cambridge, Computer Laboratory, UK Aug 03 – Dec 04
Post-doctoral research position with Dr Ken Moody and Prof. Jean Bacon in the Opera Group (distributed systems). Reseach into reputation and trust-based systems within EU funded project *SECURE* (*Secure Environments for Collaboration among Ubiquitous and Roaming Entities*). The work focused mainly on dynamics of trust and sensitivity of contextual data.

Armed Forces of the Czech Republic Sep 01 – Sep 02
Compulsory military service undergone at the Military Academy in Brno. Besides military training, most significant duties comprised lecturing *Data Security* course and organising *Security and Protection of Information* conference. Left with the rank of Sergeant.

AEC Ltd., Czech Republic 1998 – 2000
Senior Software Engineer (part-time while studying PhD) working on public key infrastructure (PKI). The work involved design and implementation of an engine for processing cryptographic protocols and messages (PKCS #1, #7, #10, #12, OCSP, CRL, CRMF, X.509, ...).

Selected Projects

Banking Cryptographic Systems 2009

Bottom-up synthesis of existing security architectures of main banking processing systems, including card issuance, card transactions (ATMs as well as point-of-sales), Swift, and Faster Payments. The project produced descriptions of architecture building blocks, data flows, configurations of secure hardware, and end-to-end cryptographic protocols' implementations. The second, top-down, part of the project produced processes for managing the systems, and detailed operational procedures for bank's staff.

Analysis of HSM Chrysalis Luna CA³ 2003

Reconstruction of algorithms and protocols implemented in the device. Project with Mike Bond, Steven Murdoch, and others to provide a thorough security analysis of the HSM implementation. The project demonstrated serious flaws in the design of HSMs. The results led to revisions of several key management systems of digital certificates issuers and banks.

Design of dedicated HW security devices 2002 – 2006

Important role in design of several dedicated hardware devices between 2002 and 2006; specification of technical requirements for hardware designs and development of software (proprietary systems, applications for Linux on embedded platforms, improving VHDL designs). The devices are being used for side-channel analysis of smart-cards and security applications for USB devices.

Future of Identity in the Information Society – FIDIS 2006 – 2008

Responsible for a workpackage on existing technologies enhancing privacy of users, privacy modelling, and ID policies throughout the EU. It laid the cornerstone of FIDIS efforts to investigate the inter-relations of various aspects of identity and user profiling techniques. A large European study on the value of location privacy was carried out as part of this work.

Education

Habilitation (*Brno University of Technology, Czech Republic*) 2006

Theses title: *Contextual Information for Security and Privacy*. The work was built upon research in privacy and reputation systems. It provides insight into mechanisms of reputation-based systems and potential privacy risks.

Doctor of Philosophy (*Brno University of Technology, Czech Republic*) Sep 97 – Jan 01

Thesis title: *Authorization Model for Strongly Distributed Information Systems*. Research concerned access control in systems defining workflow processes. The developed abstract model was based on CCS calculus and allowed composition of processes preserving proved security properties.

Master of Science (*Brno University of Technology, Czech Republic*) 1992 – 1997

Five year engineering study program. Graduation as MSc in Computer Science and Engineering. The final year project was dealing with electronic payment protocols.

Skills

Theoretical

Applied cryptography; cryptographic protocols, ability to analyse; wardriving techniques; penetration testing; operating systems' principles; distributed systems' principles; software design; proficient in working with standards and technical specifications; statistical data processing.

Technical

User/administrator knowledge of different operating systems (daily use of Linux, Win32, OS X); implementation of proofs of concepts (any programming language – most recently used C, PHP, Python, Java, ...); practical experience with embedded systems (ARM, Intel, Atmel); ability to reverse engineer and analyse implementations from functional and security point of view.

Passion for work, analytic approach, creativity, ability to manage projects, listening to opinions, analysis, synthesis of solutions, non-conflicting.

Selected Publications

- D. Cvrcek, G. Danezis: ‘Fighting a Good Internet War’. In: *Security Protocols Workshop – Remodelling the Attacker*, Cambridge, UK, 2008, pp. 1–6.
- D. Cvrcek, M. Kumpost, V. Matyas: ‘Authorizing Card Payments with PINs or Signatures?’. In: *IEEE Computer*, Vo. 41, No 5, 2008, pp. 64–68.
- D. Cvrcek, M. Kumpost, V. Matyas, G. Danezis: ‘A Study on the Value of Location Privacy’. In: *Workshop on Privacy in the Electronic Society (WPES)*, Alexandria, Virginia, USA, 2006.
- D. Cvrcek, K. Moody: ‘Combining Trust and Risk to Reduce the Cost of Attacks’. In: *iTrust 2005*, Paris, France, May 2005. Lecture Notes in Computer Science 3477, Springer, pp. 372–383.
- D. Cvrcek, V. Matyas, A. Patel: ‘Evidence processing and privacy issues in evidence-based reputation systems’. In: *Journal of Computer Standards & Interfaces*, Vol. 27, No. 5, 2005, pp. 533–545.
- D. Cvrcek: ‘Dynamics of Reputation’. In: *NordSec 2004*, Helsinki, Finland, pp.1–7, 2004.
- M. Bond, D. Cvrcek, S. J. Murdoch: ‘Unwrapping the Chrysalis’. *Technical Report UCAM-CL-TR-592*, University of Cambridge, Computer Laboratory, 2004.

References

Available upon request.