Ross J. Anderson

MASARYKOVA UNIVERZITA
DOCTOR HONORIS CAUSA

Ross John Anderson

DOCTOR HONORIS CAUSA V OBORU INFORMATIKA

Masarykova univerzita
21. dubna 2022

ROSS JOHN ANDERSON

Narozen 15. září 1956 ve Wallasey (Velká Británie).

VÝZKUMNÉ ZAMĚŘENÍ

Bezpečnostní inženýrství; bezpečnostní ekonomie; kryptografie; technologická politika.

VZDĚLÁNÍ

1992–1994	University of Cambridge (PhD, informatika)
1974–1978	University of Cambridge (BA, matematika a přírodní vědy)

PRACOVNÍ FUNKCE

Od 2021	profesor bezpečnostního inženýrství, University of Edinburgh, Velká Británie
2011	tvůrčí volno – hostující vědec ve společnosti Google, Mountain View, Kalifornie, USA; hostující profesor na Carnegie Mellon University, Pittsburgh, USA
Od 2003	profesor bezpečnostního inženýrství, Cambridge University, Cambridge, Velká Británie
2001–2002	tvůrčí volno – Massachusetts Institute of Technology, USA; National University of Singapore, Singapur; University of California Berkeley, USA
2000–2003	docent, Cambridge University, Cambridge, Velká Británie
1995–2000	lektor, Cambridge University, Cambridge, Velká Británie
1992–1994	doktorand, Cambridge University, Cambridge, Velká Británie
1981–1991	nezávislý dodavatel a konzultant; například pro Barclays Bank, Standard Chartered Bank a pro distribuci elektrické energie
1974–1975	vývojový inženýr, Ferranti, Edinburgh, Velká Británie

VYBRANÁ OCENĚNÍ

2016	Lovelace medal, British Computer Society, Londýn, Velká Británie
2015	Outstanding Innovation Award, Association for Computing Machinery, Special Interest Group on Security, Audit and Control (SIGSAC), USA
2012	Louis D. Brandeis Privacy Award, Patient Privacy Rights, Washington DC, USA
2009	člen Royal Society, Royal Society of London, Londýn, Velká Británie
2009	člen Royal Academy of Engineering (FREng), Londýn, Velká Británie

VYBRANÉ VYŽÁDANÉ PŘEDNÁŠKY

2018	Usenix Security, Baltimore, Maryland, USA
2018	Information Hiding, Innsbruck, Rakousko
2017	Association for Computing Machinery Computer and Communications Security Asia, Abú Zabí, Spojené arabské emiráty
2016	Association for Computing Machinery Computer and Communications Security (ACM CCS), Vídeň, Rakousko
2016	Royal Institute of Navigation, Nottingham, Velká Británie
2014	Black Hat, Las Vegas, Nevada, USA
2014	Cathie Marsh Lecture, Royal Statistical Society, Londýn, Velká Británie
2014	Annual Privacy Lecture, Berkeley Law School, Berkeley, Kalifornie, USA
2012	Annual Computer Security Applications Conference (ACSAC), Orlando, Florida, USA
2012	Amsterdam Privacy Conference, Amsterdam, Nizozemsko
2012	Payment Systems Economics, Kansas, Missouri, USA
2011	Indocrypt, Chennai, India
2011	European Symposium on Research in Computer Security, Leuven, Belgie
2011	AusCERT Information Security Conference (Australia's pioneer Cyber Emergency Response Team), Gold Coast, Austrálie
2010	Visions of Computer Science (launch of the Academy of Computer Science), Edinburgh, Skotsko
2009	Centenary lecture, India Institute of Science, Bangalore, Indie
2007	Crypto, Santa Barbara, Kalifornie, USA
2005	Body Sensor Networks, London, Velká Británie
2003	Principles of Distributed Computing, Boston, Massachusetts, USA
2001	Symposium on Operating System Principles, Banff, Kanada
1999	Annual Computer Security Applications Conference, Phoenix, Arizona, USA
1997	Association for Computing Machinery Computer and Communications Security, Curych, Švýcarsko
1995	Cryptography Policy and Algorithms Conference, Brisbane, Austrálie

VYBRANÉ VĚDECKÉ AKTIVITY

Od 2009	člen Royal Society, Londýn, Velká Británie
Od 2009	člen Royal Academy of Engineering, Londýn, Velká Británie
Od 2009	člen Institute of Physics, Londýn, Velká Británie
Od 2000	člen Institution of Electrical Engineers (od roku 2006 Institution of Engineering and Technology), Londýn, Velká Británie
Od 1993	člen Institute of Mathematics and its Applications, Southend-on-Sea, Velká Británie

ČLENSTVÍ V REDAKČNÍCH RADÁCH

1993–1997 zakládající redaktor, *Computer and Communications Security Reviews*

VYBRANÉ PUBLIKACE

'Why Cryptosystems Fail' in Communications of the ACM v 37 no 11 (November 1994) pp 32–40

'Robustness principles for public key protocols' (with RM Needham), in Advances in Cryptology – Crypto 95, Springer LNCS v 963 pp 236–247

'Security in Clinical Information Systems', British Medical Association (1996)

'On the Reliability of Electronic Payment Systems', (with SJ Beduidenhoudt) in IEEE Transactions on Software Engineering v 22 no 5 (1996) pp 294–301

'The Eternity Service', in Proceedings of Pragocrypt 96 pp 242–252

'Tamper Resistance – a Cautionary Note' (with MG Kuhn), in Proceedings of the Second Usenix Workshop on Electronic Commerce (Nov 96) pp 1–11

'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption' (with H Abelson, SM Bellovin, J Benaloh, M Blaze, W Diffie, J Gilmore, PG Neumann, RL Rivest, JI Schiller, B Schneier) in World Wide Web Journal v 2 no 3 (Summer 1997) pp 241–257

'On The Limits of Steganography' (with F Petitcolas), IEEE Journal on Selected Areas in Communications v 16 no 4 (1998) pp 474–481

'Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations', (with MG Kuhn) in Proceedings of the Second International Workshop on Information Hiding (Portland, Apr 98), Springer LNCS v 1525 pp 126–143

'The Steganographic File System' (with RM Needham and A Shamir), in Proceedings of the Second International Workshop on Information Hiding (Portland, Apr 98) Springer LNCS v 1525 pp 74–84

'Serpent: A New Block Cipher Proposal' (with E Biham and LR Knudsen), in Fast Software Encryption – proceedings of fifth international workshop (1998), Springer LNCS v 1372 pp 222–238; also submitted to NIST as an AES candidate

'The Eternal Resource Locator: An Alternative Means of Establishing Trust on the World Wide Web' (with FAP Petitcolas and VM Matyas) in Proceedings of the Third USENIX Workshop on Electronic Commerce pp 141–153

'Security Engineering – A Guide to Building Dependable Distributed Systems', Wiley (2001); Second edition, Wiley (2008)

'API-Level Attacks on Embedded Systems' (with Mike Bond), in IEEE Computer v 34 no 10 (October 2001) pp 67–75

'Why Information Security is Hard – An Economic Perspective', in Proceedings of the Seventeenth Computer Security Applications Conference (2001) pp 358–365

'Optical Fault Induction Attacks' (with S Skorogbogatov), in Cryptographic Hardware and Embedded Systems 2002, Springer LNCS vol 2523 pp 2–12

‘The Memorability and Security of Passwords – Some Empirical Results’ (with Jianxin Yan, Alan Blackwell and Alastair Grant), IEEE Security & Privacy, Sep–Oct 2004 pp 25–29

‘The Topology of Covert Conflict’ (with Shishir Nagaraja), Workshop on the Economics of Information Security (June 2006)

‘Protecting Domestic Power-line Communications’ (with Richard Newman, Sherman Gavette and Larry Yonge), in Symposium On Usable Privacy and Security (2006) pp 122–132

‘Children’s Databases – Safety and Privacy’ (with Ian Brown, Richard Clayton, Terri Dowty, Douwe Korff and Eileen Munro), Information Commissioner’s Office, November 2006

‘The snooping dragon: social-malware surveillance of the Tibetan movement’ (with Shishir Nagaraja), University of Cambridge technical report UCAM-CL-TR-746, March 2009

‘Information security: where computer science, economics and psychology meet’ (with Tyler Moore) in Philosophical Transactions of the Royal Society A v 367 no 1898 pp 2717–2727

‘Chip and Pin is Broken’ (with Steven Murdoch, Saar Drimer and Mike Bond), at IEEE Symposium on Security and Privacy (2010) pp 433–444

‘Resilience of the Internet Interconnection Ecosystem’ (with Panagiotis Trimintzios, Chris Hall, Richard Clayton and Evangelos Ouzounis), European Network and Information Security Agency, April 2011

‘Measuring the Cost of Cybercrime’ (with Chris Barton, Rainer Böhme, Richard Clayton, Michel van Eeten, Michael Levi, Tyler Moore and Stefan Savage), at the Workshop on the Economics of Information Security 2012; and in The Economics of Information Security and Privacy (Springer 2013) pp 265–300

‘Chip and Skim: Cloning EMV Cards with the Pre-Play Attack’ (with Mike Bond, Omar Choudary, Steven Murdoch and Sergei Skorobogatov) at IEEE Security and Privacy 2014

‘The collection, linking and use of data in biomedical research and health care: ethical issues’ (with Martin Richards, Stephen Hinde, Jane Kaye, Anneke Lucassen, Paul Matthews, Michael Parker, Margaret Shotter, Geoff Watts, Susan Wallace and John Wise), Nuffield Bioethics Council, Feb 2015

‘Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications’ (with Hal Abelson, Steve Bellovin, Josh Benaloh, Matt Blaze, Whit Diffie, John Gilmore, Matt Green, Susan Landau, Peter Neumann, Ron Rivest, Jeff Schiller, Bruce Schneier, Michael Specter and Danny Weitzner), MIT CSAIL Tech Report 2015-026 (July 6, 2015); also in Journal of Cybersecurity (2015) and Communications of the ACM v 58 no 10 (Oct 2015)

‘Standardisation and Certification of Safety, Security and Privacy in the Internet of Things’ (with Éireann Leverett and Richard Clayton), European Commission (2017)

‘Measuring the Changing Cost of Cybercrime’ (with Chris Barton, Rainer Böhme, Richard Clayton, Carlos Gañán, Tom Grasso, Michael Levi, Tyler Moore and Marie Vasek), Workshop on the Economics of Information Security 2019

LAUDATIO

Jiří Zlatuška

Vážení hosté, dámy a pánové,

dovolte mi představit Rosse Andersona – profesora bezpečnostního inženýrství počítačové laboratoře na Univerzitě v Cambridge a univerzitě Edinburgh a člena Churchillovy koleje.

Profesor Ross Anderson se narodil roku 1956 ve Wallasey v Anglii a po skončení studií na střední škole v Glasgow pokračoval ve studiu na Trinity College v Cambridge. Bakalářské studium ukončil roku 1978, poté přes 10 let pracoval v průmyslu, především na projektech zaměřených na počítačovou bezpečnost. V roce 1992 se vrátil do Cambridge jako doktorský student, aby pracoval pod vedením Rogera Needhama – čestného doktora na sousední Univerzitě obrany v Brně, a započal tak svou vědeckou kariéru. Roku 1995 získal titul PhD a stal se lektorem počítačové laboratoře na Univerzitě v Cambridge. V roce 1998 založil Ross Anderson Nadaci výzkumu informační politiky zabývající se výzkumem a lobby v oblasti informačních technologií. V roce 2000 se stal docentem bezpečnostního inženýrství a v říjnu 2003 pak profesorem na Univerzitě v Cambridge.

Bezpečnostní inženýrství – jak ho definoval profesor Anderson – je o stavbě systémů, které zůstávají spolehlivými i přes chyby, záměrné manipulace nebo náhodné jevy. Jako disciplína se zaměřuje na nástroje, postupy a metody potřebné k návrhu, vývoji a testování ucelených systémů a také k adaptaci stávajících systémů podle změn jejich pracovního prostředí.

Ross Anderson začal svoji vědeckou kariéru v oblasti počítačové bezpečnosti – nebo, jak se dnes často říká, kyberbezpečnosti – zkoumáním jak základních principů kryptografických algoritmů, tak i jejich nasazování. Mimo jiné je spoluautorem blokové šifry „Serpent“ (spolu s Eli Bihamem a Larsem Knudsenem) a jedním z finalistů soutěže „Advanced Encryption Standard“ (AES). Začal s důležitým výzkumem v opomíjených oblastech počítačové bezpečnosti, od bezpečnosti hardwaru až po využití zpracovaného signálu. Profesor Anderson zkoumal v oblasti počítačové bezpečnosti řadu nových zajímavých aplikací, od zařízení pro banky až po lékařské záznamy. Poukazoval na způsoby selhávání těchto aplikací, z nichž se mohli vývojáři poučit. Od roku 2001 rozvíjel bezpečnostní ekonomii jako další platformu pro porozumění počítačové bezpečnosti, protože systémy velmi často selhávají ne kvůli technickým chybám, ale díky nevyváženým ekonomickým pobídkám. V roce 2001 vydal velmi populární knihu „Bezpečnostní inženýrství – průvodce budováním spolehlivých distribuovaných systémů“. Také přispěl k vytvoření několika hojně rozšířených systémů, od peer-to-peer systémů přes zálohovací měřiče spotřeby (se 400 miliony instalací) až po „HomePlug standard“ pro elektronickou komunikaci (hojně využívaný k rozšíření sítě WiFi). Za tuto práci získal v roce 2016 cenu Lovelace Medal, nejvyšší ocenění v IT v Británii.

Během své bohaté vědecké kariéry byl profesor Anderson v roce 2009 zvolen členem jak Královské inženýrské akademie, tak i Královské společnosti. V roce 2015 ocenila Asociace pro výpočetní techniku, konkrétně skupina Bezpečnost, kontrola a řízení, prof. Andersona Cenou za vynikající inovaci.

Ross Anderson je důrazným obhájcem akademické svobody, duševního vlastnictví a zájmů univerzit i mimo Univerzitu v Cambridge a její koleje. V letech 2003–2010 a 2015–2018 byl zvolen členem Akademického senátu univerzity.

Ross Anderson spolupracuje s vědci z Masarykovy univerzity od roku 1996. Od té doby byli na univerzitě v Cambridge tři vědci z Fakulty informatiky MU v rámci postdoktorského výzkumného pobytu nebo tvůrčího volna (někteří opakovaně). Mnoho doktorských studentů také mělo možnost navštívit bezpečnostní skupinu počítačové laboratoře Univerzity v Cambridge nebo se zúčastnit workshopu o bezpečnostních protokolech. Téměř každý rok pokračuje spolupráce mezi doktorskými studenty a akademiky z obou univerzit. A proto není náhodou, že se workshop ze tří let pořádaných mimo domovskou univerzitu v Cambridge konal dvakrát právě v Brně za osobní účasti prof. Andersona, který zde prezentoval své nejnovější vědecké poznatky.

Čestný doktorát, který dnes prof. Anderson získává, není jen oceněním jeho profesionality a vědeckých výsledků, ale také uznáním za rozvoj spolupráce s Masarykovou univerzitou, především s fakultou informatiky.

PROSLOV
Ross Anderson

Vážení hosté, dámy a pánové,

s pokorou přijímám od Masarykovy univerzity čestný doktorát.

Lidé se mě často ptají, co je tajemstvím úspěšného multidisciplinárního výzkumu.

Vedoucí mé diplomové práce, zesnulý Roger Needham, měl motto, že dobrý výzkum vychází ze skutečných problémů. Problémy, jimiž se zabýval, byly technického rázu: souvisely s navrhováním nových počítačových systémů a síťovým vybavením. Já jeho tradici následoval, ovšem v oboru velkých aplikací. Jedním z raných projektů byla elektrifikace milionů domácností v Jižní Africe; inovace spočívala ve využití kryptografie při vývoji, elektřina se prodávala pomocí dvacetimístného kouzelného čísla, které jste si koupili v obchodě nebo v bankomatu a naťukali doma do elektroměru. STS systém, který jsme na to vyvinuli, se nyní využívá ve 400 milionech elektroměrů ve 100 zemích.

Dalším projektem bylo pochopit, co se může pokazit v platebních systémech: když Velkou Británii na počátku devadesátých let zachvátila vlna padělatelství platebních karet, dva tisíce obětí žalovalo 13 bank o dva miliony liber na ztrátách. Měl jsem to štěstí, že jsem byl v pozici znalce na straně stěžovatelů, což mi umožnilo nasbírat velké množství dat. Práce na platebních podvodech inspirovala mne i mé studenty k tomu, abychom se zaměřili na metody hackování chytrých karet i na další způsoby, jak obelstít kryptografické vybavení, které banky používají.

Krátce řečeno: když se začnete dívat nejen na skutečné problémy, ale na problémy skutečně využívaných aplikací, musíte se zabývat matematikou, kovem a vším mezi tím – elektrotechnikou, designem protokolu, softwarem. Mělo toho ale přijít ještě víc.

V roce 2001 jsme si začali uvědomovat, že příčiny bezpečnostních selhání v komplexních systémech reálného světa obvykle vycházejí ze dvou podnětů.

Jestliže Alice zabezpečuje systém, zatímco Bob hradí náklady v případě selhání, můžete očekávat, že vzniknou potíže. Například prevence platebních podvodů vyžaduje snahu na straně obchodníků i bank, které od obchodníků získávají transakce, zatímco náklady v případě selhání padají na držitele karet a na banky, které jim ty karty vydávají. Takto se zrodil obor bezpečnostní ekonomie. Proč existuje tolik nezabezpečeného softwaru? Kdo zaplatí údržbu, když už dnes vkládáme software i do zboží dlouhodobé spotřeby jako například do aut nebo do lékařských přístrojů? Proč policie většinou ignoruje kyberzločiny, přestože v současné době představují více než polovinu všech zjištných trestných činů, a to co do objemu i hodnoty? A proč se za posledních deset let vzorce kyberzločinu příliš nezměnily, i když jsme se přesunuli z notebooků na mobilní telefony a život se přesunul na sociální sítě on-line?

Mým posláním se v pozdějším životě stal vývoj bezpečnostního inženýrství jako disciplíny. Stejně jako student medicíny potřebuje znát anatomii, fyziologii, farmacii, psychologii, chirurgii a spoustu dalších věcí a jako architekt potřebuje znát strukturální mechaniku, osvětlení, akustiku, zákon o územním

plánování, kresbu, dějiny umění a další věci, tak bezpečnostní inženýr potřebuje širokou škálu znalostí, od kryptografie po softwarové zabezpečení a od fyziky přes ekonomii až po psychologii. Stejně jako v lékařství a architektuře je třeba tyto komponenty spojit dohromady v kontextu odborné zkušenosti, kterou můžeme soustředit v případových studiích nebo dále prozkoumávat při průmyslové spolupráci.

Jak technologie mění náš svět, my akademici budeme muset vyvinout mnoho nových disciplín, abychom si s tím poradili. Nejvýrazněji se to projeví v přírodních vědách a inženýrství, ale velké změny prostoupí i do dalších oblastí. Jak podpoříme humanitní vědce, aby prováděli výzkum v záplavě dat, která nám nabízejí sociální sítě? Jak zajistíme bezpečnost a férovost ve světě všudypřítomných chytrých zařízení? Jak budeme radit politickým činitelům ohledně soukromí, cenzury a dalších problémů, které bude veřejnost potřebovat řešit?

Věřím, že tajemstvím úspěšného výzkumu není říct si: „Pojďme udělat nějakou multidisciplinární práci," ale hledat skutečné problémy a pak stavět týmy, které jsou potřeba k jejich řešení. To ale potom také znamená vyvíjet akademické obory, které by takové práce dokázaly vést, a stejně jako u jakéhokoliv jiného hodnotného programu může být třeba je deset nebo dvacet let pěstovat. Znamená to také tvorbu podpůrných struktur. Z mého pohledu by každá dobrá univerzita měla mít ambici udržovat několik takových dlouhodobých programů na rozvoj nových typů myšlení. Proto tu koneckonců jsme.

Přeji vám všem, ať se vám tyto snahy daří!

SLAVNOSTNÍ SLIB

Vážený pane, dříve než Vám udělím hodnost, kterou jsme se rozhodli ocenit Vaše mimořádné vědecké zásluhy a vynikající schopnosti, je třeba zachovat starobylý zvyk, který od těch, jimž má být udělena akademická hodnost, vyžaduje, aby složili slavnostní slib.

Vážený pane, protože jste se zasloužil o rozkvět této univerzity a dal jste ostatním příklad hodný napodobení, žádám Vás pouze o to, abyste slíbil:

Především, že této univerzitě, která nese důstojné jméno Masarykovo, trvale zachováte věrnost a přátelství a že ji podle svých sil budete podporovat.

Dále pak, že budete neustále dbát o rozvoj lidského poznání, aby se šířila pravda a aby její světlo zářilo jasněji.

A konečně, že takový, jakým jste se ukázal být, budete stále. Zavazujete se k tomu a slibujete to na své dobré svědomí?

ZAVAZUJI SE A SLIBUJI.

Poté, co jsem s vděčností přijal tento Váš slib, já, řádně ustanovený promotor, z moci svého úřadu Vás,

ROSSI JOHNE ANDERSONE,
JMENUJI ČESTNÝM DOKTOREM
INFORMATIKY.

Vaše jmenování veřejně vyhlašuji a uděluji Vám všechna práva a výsady, jež jsou s touto hodností spjaty. Na důkaz toho Vám do rukou předávám tento diplom s pečetí Masarykovy univerzity a dekoruji Vás zlatou pamětní medailí této univerzity.

Ross John Anderson

DOCTOR HONORIS CAUSA IN THE FIELD OF INFORMATICS

Masaryk University
21 April 2022

ROSS JOHN ANDERSON

Born on 15 September 1956 in Wallasey (United Kingdom).

MAIN RESEARCH AREAS

Security engineering; security economics; cryptography; technology policy.

EDUCATION

1992–1994	University of Cambridge (PhD, computer science)
1974–1978	University of Cambridge (BA, mathematics and natural science)

POSITIONS HELD

Since 2021	Professor of Security Engineering, School of Informatics, University of Edinburgh, Scotland
2011	Sabbatical – Visiting scientist at Google, Mountain View, California, United States; visiting professor at Carnegie Mellon University, Pittsburgh, United States
Since 2003	Professor of Security Engineering, Cambridge University, Cambridge, United Kingdom
2001–2002	Sabbatical – Massachusetts Institute of Technology, United States; National University of Singapore, Singapore; University of California Berkeley, United States
2000–2003	Reader, Cambridge University, Cambridge, United Kingdom
1995–2000	Lecturer, Cambridge University, Cambridge, United Kingdom
1992–1994	Research student, Cambridge University, Cambridge, United Kingdom
1981–1991	Self-employed contractor and consultant; clients included Barclays Bank, Standard Chartered Bank and the electricity metering industry
1974–1975	Development engineer, Ferranti, Edinburgh, Scotland

AWARDS AND HONORS RECEIVED (SELECTED)

2016	Lovelace medal, British Computer Society, London, United Kingdom
2015	Outstanding Innovation Award, Association for Computing Machinery, Special Interest Group on Security, Audit and Control (SIGSAC), United States of America
2012	Louis D. Brandeis Privacy Award, Patient Privacy Rights, Washington DC, United States of America
2009	Fellow of the Royal Society, Royal Society of London, London, United Kingdom
2009	Fellow of the Royal Academy of Engineering (FREng), London, United Kingdom

INVITED LECTURES (SELECTED)

2018	Usenix Security, Baltimore, Maryland, USA
2018	Information Hiding, Innsbruck, Austria
2017	Association for Computing Machinery Computer and Communications Security Asia, Abu Dhabi, United Arab Emirates
2016	Association for Computing Machinery Computer and Communications Security (ACM CCS), Vienna, Austria
2016	Royal Institute of Navigation, Nottingham, United Kingdom
2014	Black Hat, Las Vegas, Nevada, United States of America
2014	Cathie Marsh Lecture, Royal Statistical Society, London, United Kingdom
2014	Annual Privacy Lecture, Berkeley Law School, Berkeley, California, United States of America
2012	Annual Computer Security Applications Conference (ACSAC), Orlando, Florida, United States of America
2012	Amsterdam Privacy Conference, Amsterdam, Netherlands
2012	Payment Systems Economics, Kansas, Missouri, United States of America
2011	Indocrypt, Chennai, India
2011	European Symposium on Research in Computer Security, Leuven, Belgium
2011	AusCERT Information Security Conference (Australia's pioneer Cyber Emergency Response Team), Gold Coast, Australia
2010	Visions of Computer Science (launch of the Academy of Computer Science), Edinburgh, Scotland
2009	Centenary lecture, India Institute of Science, Bangalore, India
2007	Crypto, Santa Barbara, California, United States of America
2005	Body Sensor Networks, London, United Kingdom
2003	Principles of Distributed Computing, Boston, Massachusetts, United States of America
2001	Symposium on Operating System Principles, Banff, Canada
1999	Annual Computer Security Applications Conference, Phoenix, Arizona, United States of America
1997	Association for Computing Machinery Computer and Communications Security, Zurich, Switzerland
1995	Cryptography Policy and Algorithms Conference, Brisbane, Australia

SCIENTIFIC ACTIVITIES (SELECTED)

Since 2009	Fellow of the Royal Society, London, United Kingdom
Since 2009	Fellow of the Royal Academy of Engineering, London, United Kingdom
Since 2009	Fellow of the Institute of Physics, London, United Kingdom
Since 2000	Fellow of the Institution of Electrical Engineers (became Institution of Engineering and Technology in 2006) London, United Kingdom
Since 1993	Fellow of Institute of Mathematics and its Applications, Southend-on-Sea, United Kingdom

EDITORIAL BOARDS

1993–1997 Founder editor, *Computer and Communications Security Reviews*

ORIGINAL PUBLICATIONS (SELECTED)

'Why Cryptosystems Fail' in Communications of the ACM v 37 no 11 (November 1994) pp 32–40

'Robustness principles for public key protocols' (with RM Needham), in Advances in Cryptology – Crypto 95, Springer LNCS v 963 pp 236–247

'Security in Clinical Information Systems', British Medical Association (1996)

'On the Reliability of Electronic Payment Systems', (with SJ Beduidenhoudt) in IEEE Transactions on Software Engineering v 22 no 5 (1996) pp 294–301

'The Eternity Service', in Proceedings of Pragocrypt 96 pp 242–252

'Tamper Resistance – a Cautionary Note' (with MG Kuhn), in Proceedings of the Second Usenix Workshop on Electronic Commerce (Nov 96) pp 1–11

'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption' (with H Abelson, SM Bellovin, J Benaloh, M Blaze, W Diffie, J Gilmore, PG Neumann, RL Rivest, JI Schiller, B Schneier) in World Wide Web Journal v 2 no 3 (Summer 1997) pp 241–257

'On The Limits of Steganography' (with F Petitcolas), IEEE Journal on Selected Areas in Communications v 16 no 4 (1998) pp 474–481

'Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations', (with MG Kuhn) in Proceedings of the Second International Workshop on Information Hiding (Portland, Apr 98), Springer LNCS v 1525 pp 126–143

'The Steganographic File System' (with RM Needham and A Shamir), in Proceedings of the Second International Workshop on Information Hiding (Portland, Apr 98) Springer LNCS v 1525 pp 74–84

'Serpent: A New Block Cipher Proposal' (with E Biham and LR Knudsen), in Fast Software Encryption – proceedings of fifth international workshop (1998), Springer LNCS v 1372 pp 222–238; also submitted to NIST as an AES candidate

'The Eternal Resource Locator: An Alternative Means of Establishing Trust on the World Wide Web' (with FAP Petitcolas and VM Matyas) in Proceedings of the Third USENIX Workshop on Electronic Commerce pp 141–153

'Security Engineering – A Guide to Building Dependable Distributed Systems', Wiley (2001); Second edition, Wiley (2008)

'API-Level Attacks on Embedded Systems' (with Mike Bond), in IEEE Computer v 34 no 10 (October 2001) pp 67–75

'Why Information Security is Hard – An Economic Perspective', in Proceedings of the Seventeenth Computer Security Applications Conference (2001) pp 358–365

'Optical Fault Induction Attacks' (with S Skorogbogatov), in Cryptographic Hardware and Embedded Systems 2002, Springer LNCS vol 2523 pp 2–12

'The Memorability and Security of Passwords – Some Empirical Results' (with Jianxin Yan, Alan Blackwell and Alastair Grant), IEEE Security & Privacy, Sep–Oct 2004 pp 25–29

'The Topology of Covert Conflict' (with Shishir Nagaraja), Workshop on the Economics of Information Security (June 2006)

'Protecting Domestic Power-line Communications' (with Richard Newman, Sherman Gavette and Larry Yonge), in Symposium On Usable Privacy and Security (2006) pp 122–132

'Children's Databases – Safety and Privacy' (with Ian Brown, Richard Clayton, Terri Dowty, Douwe Korff and Eileen Munro), Information Commissioner's Office, November 2006

'The snooping dragon: social-malware surveillance of the Tibetan movement' (with Shishir Nagaraja), University of Cambridge technical report UCAM-CL-TR-746, March 2009

'Information security: where computer science, economics and psychology meet' (with Tyler Moore) in Philosophical Transactions of the Royal Society A v 367 no 1898 pp 2717–2727

'Chip and Pin is Broken' (with Steven Murdoch, Saar Drimer and Mike Bond), at IEEE Symposium on Security and Privacy (2010) pp 433–444

'Resilience of the Internet Interconnection Ecosystem' (with Panagiotis Trimintzios, Chris Hall, Richard Clayton and Evangelos Ouzounis), European Network and Information Security Agency, April 2011

'Measuring the Cost of Cybercrime' (with Chris Barton, Rainer Böhme, Richard Clayton, Michel van Eeten, Michael Levi, Tyler Moore and Stefan Savage), at the Workshop on the Economics of Information Security 2012; and in The Economics of Information Security and Privacy (Springer 2013) pp 265–300

'Chip and Skim: Cloning EMV Cards with the Pre-Play Attack' (with Mike Bond, Omar Choudary, Steven Murdoch and Sergei Skorobogatov) at IEEE Security and Privacy 2014

'The collection, linking and use of data in biomedical research and health care: ethical issues' (with Martin Richards, Stephen Hinde, Jane Kaye, Anneke Lucassen, Paul Matthews, Michael Parker, Margaret Shotter, Geoff Watts, Susan Wallace and John Wise), Nuffield Bioethics Council, Feb 2015

'Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications' (with Hal Abelson, Steve Bellovin, Josh Benaloh, Matt Blaze, Whit Diffie, John Gilmore, Matt Green, Susan Landau, Peter Neumann, Ron Rivest, Jeff Schiller, Bruce Schneier, Michael Specter and Danny Weitzner), MIT CSAIL Tech Report 2015-026 (July 6, 2015); also in Journal of Cybersecurity (2015) and Communications of the ACM v 58 no 10 (Oct 2015)

'Standardisation and Certification of Safety, Security and Privacy in the Internet of Things' (with Éireann Leverett and Richard Clayton), European Commission (2017)

'Measuring the Changing Cost of Cybercrime' (with Chris Barton, Rainer Böhme, Richard Clayton, Carlos Gañán, Tom Grasso, Michael Levi, Tyler Moore and Marie Vasek), Workshop on the Economics of Information Security 2019

LAUDATIO

Jiří Zlatuška

Dear guests, ladies and gentlemen,

Allow me to introduce Ross Anderson – Professor of Security Engineering at the Computer Laboratory of Cambridge University and University of Edinburgh, and a Fellow of Churchill College.

Professor Ross Anderson was born in 1956 in Wallasey, England, and after his studies at the High School of Glasgow went to study at the Trinity College, Cambridge. He finished his Bachelor studies in 1978, followed by a decade spent in the industry, working mostly on projects related to computer security. He returned to Cambridge as a research student in 1992 to work on his doctorate under the supervision of Roger Needham – Doctor Honoris Causa of the neighbouring University of Defence in Brno – and started his career as an academic researcher. He was awarded his PhD in 1995, and became a Lecturer at the Cambridge University Computer Laboratory in the same year. In 1998, Ross Anderson set up the Foundation for Information Policy Research, a think tank and lobbying group on information technology policy. In 2000, he became a Reader in Security Engineering, and in October 2003 was established as Professor of Security Engineering at the University of Cambridge.

Security Engineering – as Professor Anderson defines it – is about building systems to remain dependable in the face of malice, error or mischance. As a discipline, it focuses on the tools, processes and methods needed to design, implement and test complete systems, and to adapt existing systems as their environment evolves.

Ross Anderson started his research career in the areas of computer security – or as it is widely called nowadays, cybersecurity – investigating both core principles of cryptographic algorithms, as well as their deployment. Among others, he is a co-author (with Eli Biham and Lars Knudsen) of the block cipher Serpent, one of the finalists in the Advanced Encryption Standard (AES) competition. He has started strong research threads in neglected areas of computer security, ranging from hardware security to the uses of signal processing. Professor Anderson investigated many interesting new applications of computer security, from banking machines to medical records, which have failure modes from which engineers can learn. Since 2001, he has developed "security economics" as an alternative framework for understanding the subject of computer security since systems very often fail not because of some technical mistake but because of misaligned incentives. In 2001, he authored a widely used book, Security Engineering – A Guide to Building Dependable Distributed Systems. He has also contributed to the design of a number of widely-deployed systems, from peer-to-peer systems through prepayment utility meters (with 400 million installed) to the HomePlug standard for power-line communications (widely used to extend WiFi networks). This work has been recognised by an award of the Lovelace Medal, the UK's top award in computing, in 2016.

Along this way of highly influential research, Professor Anderson was elected a Fellow of both the Royal Academy of Engineering and of the Royal Society, in 2009. The Association for Computing Machinery, Special Interest Group on Security, Audit and Control, awarded Ross Anderson in 2015 with the Outstanding Innovation Award.

Ross Anderson is an outspoken defender of academic freedoms, intellectual property and other matters of university politics, known well beyond the lawns of the University of Cambridge and its colleges. He was an elected member of Cambridge University's governing body from 2003–2010 and 2015–2018.

Ross Anderson has cooperated with researchers of Masaryk University since 1996. Since then, three researchers of the Faculty of Informatics have stayed in Cambridge for their postdocs or sabbaticals (some repeatedly), and numerous PhD students have visited the Computer Laboratory Security Group or attended the Security Protocols Workshop, where the interactions between both PhD students and academic staff of both Masaryk and Cambridge universities take place almost every year. And it is no accident that this workshop – out of the three years being hosted outside Cambridge – took place in Brno twice, with Professor Anderson presenting his latest research findings.

The honorary doctorate presented today to Professor Anderson is therefore not only a recognition of his professional qualities and scientific achievements, it is also a recognition of his contribution to the development of research and cooperation with Masaryk University, namely its Faculty of Informatics.

SPEECH

Ross Anderson

Dear guests, ladies and gentlemen,

I am humbled to receive a doctorate honoris causa from Masaryk University.

One of the things we often get asked is this. What's the secret of successful multidisciplinary research?

My thesis adviser, the late Roger Needham, had a maxim that good research comes from real problems. The problems he worked on were technical: they were to do with designing new computer systems and networking equipment. I followed this tradition, but working on big applications. An early project was electrifying millions of homes in South Africa; the innovation was using cryptography for development, selling electricity via a 20-digit magic number that you buy from a store or ATM and type into your meter to make the lights come on. The STS system we developed is now used in 400 million meters in 100 countries.

Another project was understanding what goes wrong with payment systems; when the United Kingdom was hit with a wave of ATM card forgery in the early 1990 s, two thousand victims ended up suing 13 banks for £ 2 m of losses. I was lucky enough to be the expert witness for the complainants, which enabled me to collect lots of data. The work on payment fraud inspired my students and me to look at ways of hacking smartcards, and at other ways to deceive the cryptographic equipment banks use.

In short, when you start looking not just at real problems, but at the problems of real-world applications, then you have to deal with the mathematics, the metal, and everything in between – the electrical engineering, the protocol design and the software. But more was to come.

In 2001 we started to realise that the root causes of security failures in complex real-world systems are usually down to incentives.

If Alice guards a system while Bob pays the cost of failure, you can expect trouble. For example, preventing payment fraud needs effort by merchants and by the banks that acquire transactions from them, while the costs of fraud fall on cardholders and on the banks that issue them with cards. Thus was born the subject of security economics. Why is there so much insecure software? Who's going to pay for maintenance now that we're putting software in durable goods such as cars and medical devices? Why do policemen mostly ignore cybercrime, despite the fact that it's now over half of all acquisitive crime, by volume and value? And why have the patterns of cybercrime not changed much in the past ten years, while we all moved from laptops to phones, and life moved to online social networks?

My mission in later life has been to develop security engineering as a discipline. Just as a medic needs to know anatomy, physiology, pharmacy, psychology, surgery and many other things, and an architect needs to know structural mechanics, lighting, acoustics, planning law, drawing, art history and many other things, so also the security engineer needs a broad spectrum of knowledge, from cryptography to software safety and from physics through

economics to psychology. As with medicine and architecture, these components have to be brought together in the context of professional experience which we can focus via case studies and explore with industrial collaboration.

As technology changes our world, we academics will need to develop many new disciplines to cope. This will be most obvious in the sciences and engineering but will be wider than that. How do we empower scholars in the humanities to do research with the torrent of data that social media offer us? How do we assure safety and fairness in a world of pervasive smart devices? How do we advise policymakers about privacy, censorship and the many other issues the public will want them to tackle?

The secret, I believe, is not to say "Let's do some multidisciplinary work" but to find real problems and then build the teams you need to tackle them. That in turn means developing the academics to lead such work, and as any worthwhile programme may have to be sustained for ten or twenty years, it also means creating support structures. Every good university should, in my view, aim to have several such long-term programmes of developing new types of knowledge. That's really why we're here.

I wish you all the best in this endeavour!

SOLEMN OATH

Distinguished sir, before I confer upon you this title
in appreciation of your extraordinary scientific merits
and exceptional competences, we must observe
the ancient custom which requires those about
to be presented with this academic title to take
a solemn oath.

Distinguished sir, because you have contributed
to the development of our university and provided
others with an example worthy of following,
I hereby ask you to swear:

First of all, that you shall forever maintain your
allegiance to this university, which bears the illustrious
name of Masaryk, forever keep your friendship
and continue to support it with all your strength.

Moreover, that you shall continue to cultivate the
development of human knowledge so that its light
shines ever brighter. And finally, that you shall
remain in the future as you are now, unchanging.

Do you swear and promise
to do so to the best of your knowledge and belief?

I SWEAR AND I PROMISE.

Now that I have gratefully received your solemn oath,
I, the duly constituted promoter, by the authority
bestowed upon me, proclaim you,

ROSS JOHN ANDERSON,
HONORARY DOCTOR
IN THE FIELD OF INFORMATICS.

I hereby publicly declare your appointment and grant
you the rights and privileges associated with this title.
As proof, I present you with this diploma, bearing the
seal of Masaryk University, and confer upon you the
Gold Medal of this university.

Vydal: Masarykova univerzita, Rektorát, Odbor výzkumu
Grafická úprava: Milan Katovský
Překlad: Gabriela Fialová
Tisk: Ing. Vladislav Pokorný – LITERA BRNO
1. vydání, 2022
Náklad: 150 ks