Marios Omar Choudary

Addresa	Splaiul Independentei 313, Sector 6, 060042 Bucuresti, Romania
Telefon	+ 40 21 402 9465
E-mail	marios.choudary@upb.ro

Educatie

Universitatea București

- 2018 - 2021 — Master în Teologie, Facultatea de Teologie Ortodoxă, Bucharest, Romania

  Studii finalizate cu lucrarea *Mărturii ale picturii paleologe în Țara Românească – Mănăstirea Chora – Kahrie Djami și Biserica Sfântul Nicolae domnesc din Curtea de Argeș*

Universitatea București

- 2014 - 2018 — Licență în Teologie, Facultatea de Teologie Ortodoxă, Bucharest, Romania

  Studii finalizate cu opera literară "Erminia duhovnicească a Sfântului Ioan Gură de Aur la epistola Sfântului Pavel către Filipeni"

University of Cambridge

- Octombrie 2010 - 2014 — Doctorat in Computer Science, supervizat de Markus Kuhn, Cambridge, UK

  Obiectivul meu principal a fost evaluarea si imbunatatirea tehnicilor 'template attack', care sunt considerate printre cele mai puternice metode pentru a obtine datele manipulate de un microprocesor, atunci cand un adversar poate monitoriza curentul consumat de acesta sau o alta proprietate fizica. Cercetarea mea a implicat design-ul unei placute hardware avand ca scop o evaluare cat mai eficienta a acestor atacuri, obtinerea si procesarea a milioane de semnale de curent, obtinute cu un osciloscop digital, aplicarea si design-ul a numeroase metode statistice si evaluarea acestora pe mai multe seturi de date pentru a verifica eficienta atacurilor 'template' folosind diversi parametri de achizitie de date, si algoritmi de procesare a datelor. O alta directie de cercetare in timpul tezei de doctorat a fost dezvoltarea unui protocol pentru a preveni atacurile de tip 'relay', dezvoltarea de protocoale pentru plati 'peer-to-peer' folosind telefoane mobile si smartcard-uri, cat si analiza si implementarea unei librarii open source pentru sistemul de criptare de disc FileVault 2.

University of Cambridge

- Octombrie 2009 - Iunie 2010 — Master in Advanced Computer Science, Cambridge, UK

  In prima jumtatate a masterului am dezvoltat un router hardware foarte rapid, cu capabilitatea de a face Network Address Translation (NAT) la viteza liniei, folosind platforma NetFPGA. In a doua jumatate, am construit un dispozitiv hardware de dimensiuni mici, care sa fie folosit in protocolul EMV (folosit de cardurile bancare), pentru a intercepta tranzactiile intre un smartcard si un terminal (cititor). Obiectivul principal al proiectului a fost sa implementez o protectie impotriva atacurilor de tip 'relay', prin afisarea detaliilor tranzactiei, astfel incat un atacator sa nu poata trimite catre smartcard informatii



diferite de ceea ce este afisat pe ecran. Dupa ce am terminat de construit dispozitivul, am scris codul pentru o stiva cat mai mai completa a protocolului ISO-7816 si EMV, pe care ulterior am folosit-o pentru a demonstra o bresa de securitate in protocolul EMV.

Universitatea Politehnica Bucuresti

- Octombrie 2003 - Iunie 2008Facultatea de Automatica si Calculatoare, sectia Calculatoare
  Bucuresti, Romania

  In ultimul semestru, am lucrat pentru proiectul de diploma la Institute de Recherche en Informatique de Toulouse (Franta), facand cercetare pe computer vision pe telefoane mobile. Ca rezultat, am dezvoltat o aplicatie de ghid mobil care poate folosi scene 3D ale unui stadion de fotbal si informatii despre locatie, pentru a ghida spectatorii la locurile lor. Impreuna cu cei din Toulouse am reusit sa publicam o parte din aceasta munca la conferinta internationala ACM Multimedia.

Interese de Cercetare: Interesele mele actuale de cercetare se concentrează pe analiza canalelor laterale, cu accent pe optimizarea evaluărilor de securitate și modelarea scurgerilor de date prin canalele laterale fizice ale diferitelor dispozitive, în special Sisteme pe Chip (SoC). De asemenea, sunt interesat de protocoalele de securitate. Am lucrat la explorarea securității protocolului de plată EMV. Mai recent, am fost implicat în proiectarea unui nou schimb de chei autentificat fără utilizarea unei terțe părți de încredere sau a unor chei prestabilite, prin utilizarea mai multor canale publice. În prezent, lucrăm la versiuni de criptare end-to-end ale protocolului.

Selectie top 5 publicatii

- C Ghiban, MO Choudary, *Improved Correlation Power Analysis Attack on the Latest Cortex M4 Kyber Implementation*, CRYPTOGRAPHY 9(1), March 2025.
- A Rădulescu, PG Popescu, MO Choudary, *GE vs GM: Efficient side-channel security evaluations on full cryptographic keys*, Conference on Cryptographic Hardware and Embedded Systems (CHES), IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022(4), pp. 886–905.
- Marios O Choudary, Markus G. Kuhn, *Efficient, portable template attacks*, IEEE Transactions on Information Forensics & Security, 13(2), 2018, pp. 490–501.
- S Costea, MO Choudary, D Gucea, B Tackmann, C Raiciu, *Secure opportunistic multipath key exchange*, Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS), 2018, pp. 2077–2094.
- Marios O Choudary, George Popescu, *Back to Massey: Impressively fast, scalable and tight security evaluation tools*, Conference on Cryptographic Hardware and Embedded Systems (CHES) 2017. Springer LNCS 10529, 2017.



Proiecte Majore de Cercetare

- Director de proiect pentru Proiect Tinere Echipe 2019, cod proiect TE188, *IMPLEMENTĂRI SIGURE CRIPTOGRAFICE PE PLATFORME SYSTEM-ON-CHIP*, durata: 2021-2022 (2 ani). `https://uefiscdi.gov.ro/resource-829086-te2019_rezultate-finale_informatica.pdf`

- Director de proiect pentru Proiect Demonstrativ Experimental 2019, cod proiect 285PED. *CREȘTEREA SECURITĂȚII COMUNICAȚIILOR MOBILE PRIN SCHIMB DE CHEI PE MAI MULTE CANALE*, durata: 2020-2022 (2 ani). `https://uefiscdi.gov.ro/resource-829458-d2_finale.pdf`

- **Evaluarea si Imbunatatirea atacurilor de tip 'Template':** Aceasta a fost munca principala din timpul doctoratului, sub supervizarea Dr. Markus Kuhn, in Computer Laboratory, University of Cambridge. In cadrul acestei cercetari am publicat 3 articole la conferinte internationale de specialitate, cel mai recent urmand sa il prezint la conferinta CARDIS 2014 din Paris, in 5–7 Noiembrie 2014.

- **Analiza sistemului de criptare de disc FileVault 2:** Am facut 'reverse-engineering' la sistemul FileVault 2, descoperind functionalitatea acestuia, si apoi am produs o librarie open source care poate sa citeasca volume de date criptate cu FileVault 2 (cu ajutorul unei chei de criptare cunoscute). Aceasta unealta este folositoare celor din domeniul 'digital forensics'. Rezultatele au fost publicate in *Security Analysis and Decryption of Filevault 2*, in Advances in Digital Forensics IX, 2013, pp 349–363.

- **EMV Security Analysis:** In 2012, impreuna cu colegii din Cambridge, am inceput analiza securitatii numerelor aleatoare folosite in tranzactiile EMV cu ATM-uri si POS-uri, si am descoperit ca in unele cazuri, aceste numere erau previzibile, ceea ce putea fi folosit la ceea ce am numit un '*pre-play* attack'. Aceste rezultate au fost initial publicate pe arxiv.org, si apoi acceptate si prezentate la IEEE Symposium on Security and Privacy 2014, una din conferintele de top in securitate.

  Cu doi ani mai in urma, am dezvoltat dispozitivul *Smart Card Detective*, in timpul masterului din Cambridge, pe care l-am si folosit pentru a demonstra o bresa mare de securitate in sistemul EMV. Detaliile sunt publicate in teza de master *The Smart Card Detective: a hand-held EMV interceptor*, Computer Laboratory Technical Report UCAM-CL-TR-827. Am folosit acest dispositiv apoi si pentru alte cercetari, de exemplu in evaluarea unor aplicatii de peer-to-peer, prezentate in *Might Financial Cryptography Kill Financial Innovation? – The Curious Case of EMV*, la conferinta Financial Cryptography and Data Security 2011.

Premii si Burse

- *Google Europe Doctoral Fellowship in Mobile Security:* Bursa de doctorat, acordata in 2010 pentru o durata de 3 ani (£75000 in total). Obtinuta doar de 15 studenti din toata Europa, in urma unui concurs bazat pe propunere de proiect, aptitudini, supervizor, scoala.

- *EPSRC Studentship:* Bursa acordata in octombrie 2009, pentru un an, ca sa acopere costurile de facultate (approximativ £6000) pentru masterul meu in Cambridge.



- *1st prize at Windows Embedded Student Challenge 2006:* Castigator al concursului Windows Embedded Student Challenge 2006 (acum parte din Imagine Cup), organizat de Microsoft. Premiul final a fost de $8000.

Experienta in predare

- din 2024, țin cursul de Topics in Cryptography, la masterul de Quantum Computing, în cadrul Universitatii Politehnica din Bucuresti.
- din 2020, țin cursul de Applied Cryptography, la masterul de Securizarea Avansată a Sistemelor, în cadrul Universitatii Politehnica din Bucuresti.
- din 2020, țin cursul de Introducere în Criptologie în cadrul Universitatii Politehnica din Bucuresti.
- din 2015, țin cursul de Procesarea Semnalelor în cadrul Universitatii Politehnica din Bucuresti.
- In 2010-2014, la Computer Laboratory in Cambridge, am tinut seminariile pe grupe de 2–3 studenti la materiile: protocoale de securitate, criptografie, si procesarea semnalelor digitale.

Technical Skills

- **Programming languages:** Matlab, C, C++, C#, Java, Verilog.
- **Hardware skills:** FPGA programming (NetFPGA, Xilinx, Proxmark III), PCB design.
- **Reverse engineering skills:** Reversed engineered FileVault 2 in Mac OS X 10.7.

Limbi cunoscute

- Romana, Spaniola - nativ,
- Engleza - fluent scris si vorbit,
- Franceza - conversational.

Alte cunostinte

In 2007-2008, am obtinut certificarile Cisco CCNA si CCNP.
In 2011-2013, am parcurs cateva cursuri online oferite de Coursera, si am completat urmatoarele (cu certificat): *Machine Learning*, *Cryptography I*, *Fundamentals of Electrical Engineering.*
In 2010-2012, am urmarit cursurile oferite la Computer Laboratory in: *Research Skills*, *Security I (cryptography)*, *Security II (security protocols)* si *Digital Signal Processing.*
In 2012, am participat la urmatoarele scoli de vara: *ECRYPT II* (hardware security) in Bochum, Germany, si *Cryptabit* (criptografie) in Bohn, Germany.



Lista de publicatii
A se vedea separat.
Prezentari la Conferinte

- A Rădulescu, PG Popescu, MO Choudary, *GE vs GM: Efficient side-channel security evaluations on full cryptographic keys*, Conference on Cryptographic Hardware and Embedded Systems (CHES), IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022(4), pp. 886–905.
- S Costea, MO Choudary, D Gucea, B Tackmann, C Raiciu, *Secure opportunistic multipath key exchange*, Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 2077–2094.
- Marios O Choudary, George Popescu, *Back to Massey: Impressively fast, scalable and tight security evaluation tools*, Conference on Cryptographic Hardware and Embedded Systems (CHES) 2017. Springer LNCS 10529, 2017.
- **Template Attacks on Different Devices** Prezentarea articolului cu acelasi titlu la conferinta COSADE 2014, in Paris.
- **Template Attacks on Different Devices** Prezentarea articolului cu acelasi titlu la conferinta COSADE 2014, in Paris.
- *Chip and Skim: cloning EMV cards with the pre-play attack* Prezentarea articolului cu acelasi titlu la IEEE Symposium on Security and Privacy, San Jose, CA, 2014.
- **Efficient Template Attacks:** Prezentarea articolului cu acelasi titlu la conferinta CARDIS 2013, in Berlin.
- **Security Analysis and Decryption of FileVault 2:** Prezentarea articolului cu acelasi titlu la conferinta IFIP 2013, in Florida, US.
- **Chip and PIN internals:** Invitat sa prezint cercetarea in EMV (Chip and PIN) la:
  - ISSA conference, Ireland, 2011.
  - Athcon, Greece, 2011.
  - IBM Warwick, UK, 2011.
  - Munster Institute for Computer Science, Germany, 2011.
- **Chip and PIN: exploring the EMV system:** Prezentare la Darwin College, Cambridge, 2011.
- **Make noise and whisper: a solution to relay attacks:** Prezentarea articolului cu acelasi titlu la Security Protocols Workshop, in Cambridge, 2011.
- **Might Financial Cryptography Kill Financial Innovation? The Curious Case of EMV:** Prezentarea articolului cu acelasi titlu la Financial Cryptography 2011, in St. Lucia.



Referinte

- **Markus Kuhn:** Senior Lecturer at the Computer Laboratory, University of Cambridge, UK.
  E-mail: markus.kuhn@cl.cam.ac.uk
  Website: `http://www.cl.cam.ac.uk/~mgk25/`
- **Virgil Gligor:** Director of CyberSecurity Lab, Carnegie Mellon University, USA.
  E-mail: virgil@andrew.cmu.edu
  Website: `https://www.cylab.cmu.edu/directory/bios/gligor-virgil.html`

