Xavier de Carné de Carnavalet

Postdoctoral Fellow

School of Computer Science, Carleton University, 1125 Colonel By Dr, Ottawa, ON K1S 5B6, Canada

Online CV, see website for contact info: `https://ccsl.carleton.ca/~xavier/`

RESEARCH INTERESTS

• Privacy • Network Security • Passwords • Firmware Security • Reverse-engineering • Machine Learning

EDUCATION

Concordia University, Montreal, QC, Canada

Ph.D. in Information & Systems Engineering *May 2014 – July 2019*
- Advisor: Dr. Mohammad Mannan
- Dissertation: "Last-Mile TLS Interception: Analysis and Observation of the Non-Public HTTPS Ecosystem"

M.A.Sc. in Information Systems Security (GPA: 4.3/4.3) *Sep. 2012 – Apr. 2014*
- Advisor: Dr. Mohammad Mannan
- Dissertation: "A Large-scale Evaluation of High-impact Password Strength Meters"

Undergraduate exchange semester (GPA: 3.94/4.3) *Sep. 2011 – Dec. 2011*

École Supérieure d'Informatique Électronique Automatique (ESIEA), Paris, France

Engineering degree (equivalent to a M.Sc. + B.Sc.) *Sep. 2010 – Dec. 2014*
- Distinction: Very Honorable with Committee Praise (GPA: 17.40/20)

Lycée les Eucalyptus, Nice, France

Classe Préparatoire (equivalent to the first two years of a B.Sc.) *Sep. 2008 – June 2010*

EMPLOYMENT

Postdoctoral Fellow *Sep. 2019 – present*
School of Computer Science
Carleton University, Ottawa, ON, Canada
Advisor: Dr. Paul Van Oorschot

Internship *June 2012 – Aug. 2012*
Software and web application developer
Humanlog, Antibes, France

REFEREED PUBLICATIONS

1. Mengyuan Zhang, **Xavier de Carné de Carnavalet**, Lingyu Wang, and Ahmed Ragab, "Large-Scale Empirical Study of Important Features Indicative of Discovered Vulnerabilities to Assess Application Security," *IEEE Transactions on Information Forensics and Security* (TIFS), vol. 14, no. 9, pp. 2315–2330, Sep. 2019 (IF: 5.824)
2. Ahmed Ragab, **Xavier de Carné de Carnavalet**, Soumaya Yacouta, Mohamed-Saleh Oualia, "Face recognition using multi-class Logical Analysis of Data," *Pattern Recognition and Image Analysis*, vol. 27, no. 2, pp. 276–288, Apr. 2017
3. **Xavier de Carné de Carnavalet**, Mohammad Mannan, "Killed by Proxy: Analyzing Client-end TLS Interception Software," *Network and Distributed System Security Symposium* (NDSS'16), San Diego, CA, USA, Feb. 2016 (AR: 15.4%, 60/389)
4. **Xavier de Carné de Carnavalet**, Mohammad Mannan, "A Large-Scale Evaluation of High-Impact Password Strength Meters," *ACM Transactions on Information and System Security* (TISSEC), vol. 18, no. 1, pp. 1–32, May 2015 (IF: 2.591)
5. **Xavier de Carné de Carnavalet**, Mohammad Mannan, "Challenges and Implications of Verifiable Builds for Security-Critical Open-Source Software," *Annual Computer Security Applications Conference* (ACSAC'14), New Orleans, LA, USA, Dec. 2014 (AR: 19.9%)
6. **Xavier de Carné de Carnavalet**, Mohammad Mannan, "From Very Weak to Very Strong: Analyzing Password-Strength Meters," *Network and Distributed System Security Symposium* (NDSS'14), San Diego, CA, USA, Feb. 2014 (AR: 18.6%, 55/295)

NON-REFEREED PUBLICATIONS

7. **Xavier de Carné de Carnavalet**, Mohammad Mannan. "Privacy and Security Risks of 'Not-a-Virus' Bundled Adware: The Wajam Case," arXiv:1905.05224 [cs.CR] (May 2019)
8. **Xavier de Carné de Carnavalet**. "Root Agency dummy root certificate trusted by Net Nanny and Untangle NG Firewall," appeared in Bulletproof TLS Newsletter #48 (Jan. 2019)
9. **Xavier de Carné de Carnavalet**. "How I compiled TrueCrypt 7.1a for Win32 and matched the official binaries," online article visited 45,000 times within first two days, relayed on several news websites (Oct. 2013)
10. **Xavier de Carné de Carnavalet**. "Windows 7/8 admin account installation password stored in the clear in LSA Secrets," vulnerability/bug disclosed in the Bugtraq mailing list (July 2013)
11. **Xavier de Carné de Carnavalet**, Robert Erra. "Algorithmic complexity attacks and their complexity," *Rencontres des Solutions de Sécurité et d'Informatique Libre* (RSSIL'12), Maubeuge, France, June 2012

HONORS AND AWARDS

1. Tri-Council Vanier Canada Graduate Scholarship (Vanier CGS, NSERC), 2015–2018 (**$150,000**)
   - Ranked 10/179 of pre-selected applications (50 awarded)
   - First recipient within Concordia's Engineering and Computer Science faculty
2. Quebec Merit Scholarship for Foreign Students (PBEEE, FQRNT), 2015 (declined) (**$75,000**)
   - Ranked 4/28
3. Concordia University Graduate Fellowship, 2014–2017 (**$32,400**)
4. Concordia's Accelerator Award, 2019 (**$5,000**)
5. Concordia's Conference and Exposition Award, 2016 (**$1,000**)
6. Concordia's Conference and Exposition Award, 2014 (**$1,000**)
7. Concordia's Graduation Bonus Award, 2014 (**$1,000**)
8. Concordia's Conference and Exposition Award, 2013 (**$750**)
9. Concordia's Faculty of Engineering and Computer Science Graduate Scholarship, 2013 (**$3,000**)
10. ESIEA Excellency Scholarship, 2010–2013

TEACHING

Experience

- Information Systems Security (SOEN 321, Undergraduate course), Concordia University
  - Teaching Assistant (Fall 2015, Winter 2019)
- Crypto Protocols and Network Security (INSE 6120, Graduate course), Concordia University
  - Teaching Assistant (Fall 2016, Winter 2017, Winter 2019)
  - Guest Lectures on TLS Interception (Fall 2016, Winter 2017, Winter 2019)
  - Guest Lectures on Password Security (Winter 2015, Fall 2015)
- Malware Defenses and Application Security (INSE 6140, Graduate course), Concordia University
  - Teaching Assistant (Winter 2014, Winter 2015)
- Operating Systems Security (INSE 6130, Graduate course), Concordia University
  - Teaching Assistant (Fall 2013, Winter 2014)

Trainings Attended

- Graduate Seminar in University Teaching, Concordia's Graduate & Professional Skills
  - A 32-hour seminar on exploring various approaches to teaching, designing lessons, developing a course syllabus (Dec. 2017)
- Innovating Beyond the Textbook: Conference on Learning to Teach for Graduate Students & Post-Docs, McGill's Teaching and Learning Services
  - Intensive one-day multi-session conference and workshops (Nov. 2013)

TALKS

1. "How to create a strong password," Concordia's X-Explained YouTube series, Jan. 2019
2. "Killed by Proxy: Analyzing Client-end TLS Interception Software," Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, Feb. 2016
3. "Is your 'strong' password all that strong?" **CTV News Montreal live interview**, Mar. 2015
4. "Challenges and Implications of Verifiable Builds for Security-Critical Open-Source Software," Annual Computer Security Applications Conference (ACSAC), New Orleans, CA, USA, Dec. 2014

5. "From Very Weak to Very Strong: Analyzing Password-Strength Meters," Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, Feb. 2014
6. Triannual presentations at CIISE Security Privacy and Forensics Seminar, 2013–2019
7. "Analyzing Password-Strength Meters," National Cyber-Forensics & Training Alliance (NCFTA) in front of senior government officials, Nov. 2013
8. "Why I compiled TrueCrypt and how I matched the official binaries," invited talk at **Google Montreal**, Nov. 2013

LEADERSHIP & MANAGEMENT SKILLS

- Supervision of a Master's student research internship, Concordia University, Montreal, QC, Canada (2020)
- Led a team of security enthusiasts towards the NorthSec CTF competition (2014–2020)
  - Organized weekly trainings with team-based challenges
  - Presented challenge solutions
  - Ranked 15/28 (2014), 22/40 (2016), 12/50 (2018), 15/74 (2019), 16/76 (2020)
- Supervision of an intern at Genetec, Montreal, QC, Canada (2018, 4 months)
- Advising and collaboration of Master's students
  - Briti Mondal, M.A.Sc.: Binary Analysis Tool For Identification Variable Types In Binary Programs
  - Parul Khanna, M.A.Sc.: Detecting Privacy Leaks Through Existing Android Frameworks

PROFESSIONAL ACTIVITIES

- Journal Reviewer
  - IEEE Transactions on Information Forensics and Security
  - Elsevier Computers & Security
- Journal External Reviewer
  - IEEE Transactions on Information Forensics and Security
  - IEEE Transactions on Dependable and Secure Computing
  - ACM Transaction on Information and System Security
- Conference External Reviewer
  - 1st Workshop on Cloud Security and Privacy (CLOUD S&P'19)
  - 26th ACM Conference on Computer and Communications Security (CCS'19)
  - 27th USENIX Security Symposium (USENIX Security 18)
  - 13th ACM Symposium on Information, Computer and Communications Security (AsiaCCS'18)
  - 25th ACM Conference on Computer and Communications Security (CCS'18)
  - 23rd ACM Conference on Computer and Communications Security (CCS'16)
  - 2016 New Security Paradigms Workshop (NSPW'16)
  - 6th ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM'16)
  - 5th ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM'15)
  - 10th ACM Symposium on Information, Computer and Communications Security (AsiaCCS'15)
  - 7th International Conference on Trust and Trustworthy Computing (TRUST'14)
  - 30th Annual Computer Security Applications Conference (ACSAC'14)
- Systems Administrator at Madiba Security Research Group, Montreal, QC, Canada (2014–2019)

PERSONAL

- Personal blog with tutorials, CTF challenge write-ups and thoughts on security: `https://blog.xavier2dc.fr` *Feb. 2020 – present*
  Selected post: *An Analysis of Modified VeraCrypt binaries*
- Classical Music studies (16 years)
  - Music Academy, l'Haÿ-les-Roses, France (1 year) *Sep. 2010 – Apr. 2011*
    - 1st violin in the Val de Bièvre Symphonic Orchestra
  - Music Academy, Grasse, France (15 years) *Sep. 1994 – June 2009*
    - **First Prize** in Violin performance (unanimously with distinction)
    - Academia's Gypsy Ensemble (3 years)
    - Provence-Alpes-Côte-d'Azur Regional Symphonic Orchestra (4 years)