Yury Zhauniarovich

HBKU - Research Complex
P.O. Box 5825
Doha, Qatar
✉ *yzhauniarovich@hbku.edu.qa*
zhauniarovich.com

Career Track

Jul. 2017 – current **Scientist**, *Qatar Computing Research Institute (`www.qcri.com`), HBKU*, Doha, Qatar.
Responsibilities:
- Research and development

Dec. 2015 – Jun. 2017 **Postdoctoral Researcher**, *Qatar Computing Research Institute (`www.qcri.com`), HBKU*, Doha, Qatar.
Responsibilities:
- Research and development

Sep. 2016 – Dec. 2016 **Lecturer of the Course "Network security"**, *Hamad Bin Khalifa University (`www.hbku.edu.qa`)*, Doha, Qatar.
Responsibilities:
- Preparation and giving lectures on Wireless and Mobile Security
- Homework and exam tasks preparation and check

May 2014 – Oct. 2015 **Postdoctoral Researcher**, *University of Trento (`www.unitn.it`)*, Trento, Italy.
Responsibilities:
- Project coordination
- Development of research prototypes

Feb. 2015 – Sep. 2015 **Lecturer of the Course "Network security"**, *University of Trento (`www.unitn.it`)*, Trento, Italy.
Responsibilities:
- Preparation and giving lectures on Network Security

May 2014 – May 2014 **Teaching Assistant for the Course "Network security"**, *University of Trento (`www.unitn.it`)*, Trento, Italy.
Responsibilities:
- Giving lectures on Android security (2h: Essentials of Android OS security; 4h: Android App Security, dissection of an app using AndroGuard to show insecure patterns, Overview of the latest Android security research achievements)

Mar. 2013 – Apr. 2013 **Teaching Assistant for the Course "Network security"**, *University of Trento (`www.unitn.it`)*, Trento, Italy.
Responsibilities:
- Giving lectures on Android security (2h: Essentials of Android OS security; 2h: Android App Security, dissection of an app using AndroGuard to show insecure patterns)

Feb. 2011 – July 2011 **Teaching Assistant for the Course "Network security"**, *University of Trento (www.unitn.it)*, Trento, Italy.

Responsibilities:

- Giving lectures on Android security (2h: Essentials of Android OS and app security)
- Giving lectures on Android app development (4h: Introduction to app development)
- Conduction of laboratory classes (12h: Development of security-related Android apps)
- Controlling of results (2h: Presentation of apps developed during the course)

Apr. 2007 – Oct. 2009 **SAP SD/LE Consultant, Business Analyst**, *SAP Consulting Department, Itransition (www.itransition.com)*, Minsk, Belarus.

SAP SD/LE consultant responsibilities:

- Customer interviewing
- Initial training of business users
- Business processes modeling and re-engineering
- SAP ERP SD/LE modules customization

Business analyst responsibilities:

- Prototype design
- Business requirement management
- Business process design, review and modeling

Jan. 2006 – Mar. 2007 **Part-time Developer**, *Department of Applied programs, Belarusian State University (www.bsu.by)*, Minsk, Belarus.

Responsibilities:

- Borland C++ Builder developer
- MS SQL database designer

Research Projects

Cyber Intelligence

Qatar Cyber Intelligence Platform

The purpose of this project is to build a highly scalable, opened cyber intelligence platform that can be used to analyze data in a near real time basis. Therefore, as building blocks for this platform we use the components that are open-sources and can be easily scaled horizontally, e.g., Apache Storm or Elasticsearch. Further, we aim at applying this platform for the analysis of data in different areas of security research. In particular, so far we have used this platform to collect, store and analyze the data obtained from honeypots used to understand amplification denial of service attacks [2]. On top of that we proposed a system and a tool to assess and visualize the amount of traffic that enters and leaves ISP network in case it contains innocent amplifiers. The work was presented at the IEEE Symposium on Visualization for Cyber Security 2016 [4].

Technologies: Elasticsearch, Apache Storm, Apache Kafka, Kibana, Java, Python (jupyter notebook, scikit-learn, pandas, elasticsearch-py, amppot)

Android Security

Android Permission Evolution Analysis

In the scope of this project we have explored the evolution of the permission system in the Android operating system. In particular, we have analyzed what permissions are added, deleted or modified between different versions of Android; how protection level and permission flags influence on the behavior or the corresponding permissions. The results of this works were published at the International Symposium on Research in Attacks, Intrusions and Defenses 2016 [6].

Technologies: AOSP, Python (pandas, jupyter notebook)

MobileShield In the scope of this project we have developed a prototype of the system that is able to detect the fraud of a smartphone on a near real-time basis. Moreover, we have proposed a new machine learning based method for passive user authentication using smartphone sensor data. This work will be presented at the IEEE International Conference on Identity, Security and Behavior Analysis 2017 conference [3].
Technologies: Java, Android, WebSockets, VPN, Python (scikit-learn, pandas, jupyter notebook)

Analysis of the Android apps in the presence of dynamic code update features In this project we have studied how Android applications use dynamic code updates features, in particular, reflection and dynamic class loading. These features are often used to conceal malicious behavior of Android apps. We have proposed a novel approach for dissection of the apps containing dynamic code update features combining static and dynamic analysis techniques. The results of this work were presented at the ACM Conference on Data and Application Security and Privacy 2015 conference [8].
Technologies: AOSP, Java, Python (AndroGuard)

Detection of Repackaged Android Applications In the scope of this project we explore novel techniques to detect repackaged Android applications. Based on the research we proposed an approach that compares Android apps detects the repackaged ones in a very fast way. We presented the results of this work at the DBSec '14 [14] and the NordSec '16 [5] conferences.
Technologies and tools: Java, Python (AndroGuard, scikit-learn)

Trusted Stores in Android During this project we investigated how the concept of "trusted stores" can be implemented for Android. Our approach ensures that a user can install only the applications vetted and attested by trusted stores. The demo of our system was presented at the ACM Conference on Computer and Communications Security 2013 conference [16], while the detailed description is given in the technical report [13].
Technologies and tools: AOSP, Java

Enforcing Security Profiles in Android During this project we developed a policy-based framework for enforcing software isolation of applications and data that may help to improve the security of end-user devices. The operation of our system was shown at the ACM Conference on Computer and Communications Security 2012 conference [18], while the paper discovering the peculiarities of MOSES will be published in the IEEE Transactions on Dependable and Secure Computing [15].
Technologies and tools: AOSP, Java, C, TaintDroid

Context-Related Policy Enforcement In this work we implemented a system called CRêPE that allows to specify and enforce the behavior of smartphone applications depending on the context. In CRêPE a context may be defined using the values provided by physical sensors or/and logical sensors. The policies enforced by CRêPE may be set both by a user or authorized third party locally (using a special application) or remotely (through SMS/MMS, QR codes and Bluetooth). The results of this work are published in the IEEE Transactions on Information Forensics and Security [17].
Technologies and tools: AOSP, Java, C

Collusion Attack Prevention in Android In the work we extended the Android operating system with an ability to enforce fine-grained policies, which in turn help to mitigate the problem of applications leaking sensitive information using collaboration. In particular, we used TaintDroid to assign special taints to the sensitive information and implemented an enforcement point that enforces the fine-grained decisions according to the specified policies. This work was presented at the PASSAT/SocialCom 2011 conference [19].
Technologies and tools: AOSP, Java, C, TaintDroid

Education

Nov. 2009 – Apr. 2014 **Ph.D. in Information and Communication Technology**, *University of Trento (www.unitn.it)*, Trento, Italy.
Thesis: Improving the Security of the Android Ecosystem
Advisor: Bruno Crispo

Sep. 2006 – June 2007 **M.Sc. (eq.) in Computer Science**, *Belarusian State University (www.bsu.by)*, Minsk, Belarus.
Thesis: Steganographic Data Hiding Audiosystem with Heightened Throughput Capacity
Advisor: Vasiliy Sadov

Sep. 2002 – June 2006 **B.Sc. in Computer Science**, *Belarusian State University (www.bsu.by)*, Minsk, Belarus.
Thesis: Development of a Web Ordering System for the University Computer Classes
Advisor: Natalia Novikova

Important Achievements

- The author of the free book "Android Security (and Not) Internals" [11] (www.zhauniarovich.com/files/asani/asani.pdf)
- Reviewer of the book "Android Systems Development" by Earlence Fernandes (www.packtpub.com/android-systems-development-how-instant/book)
- 15.000+ reputation on StackOverflow (www.stackoverflow.com/users/1108213/yury)
- Android Open Source Project contributor

Honors, Awards and Grants

Nov. 2009 Ph.D. Scholarship from the University of Trento
Sep. 2002 Scholarship from Belarusian State University
June 2002 Graduated Cum Laude from Lyceum BSU
May 2002 Winner of the BSU Olympiad in Physics

Talks

Mar. 06, 2017 Invited talk at the University of Luxembourg, organized by Dr. Olga Gadyatskaya; Luxembourg, Luxembourg
Sep. 21, 2016 Conference talk at the RAID '16 conference; Evry, France
Apr. 30, 2014 PhD thesis defence talk at the University of Trento; Trento, Italy
Feb. 27, 2014 Invited talk at the University of Rome "La Sapienza", organized by Prof. Luigi V. Mancini; Rome, Italy

Feb. 20, 2014 Invited talk at the University of Luxembourg, organized by Dr. Olga Gadyatskaya; Luxembourg, Luxembourg

Aug. 27, 2014 Tutorial on Android Security at the CRISiS '14 conference [7]; Trento, Italy

July 14, 2014 Conference talk at the DBSec '14 conference; Vienna, Austria

References

[1] Yury Zhauniarovich, Issa Khalil, Ting Yu, and Marc Dacier. "A Survey on Malicious Domains Detection through DNS Data Analysis". In: *ACM Computing Surveys* (2018).

[2] Laure Berti-Equille and Yury Zhauniarovich. "Profiling DRDoS Attacks with Data Analytics Pipeline". In: *Proceedings of the 2017 ACM Conference on Information and Knowledge Management*. CIKM '17. 2017, pp. 1983–1986.

[3] Attaullah Buriro, Bruno Crispo, and Yury Zhauniarovich. "Please Hold On: Unobtrusive User Authentication Using Smartphone's Built-in Sensors". In: *Proceedings of the 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*. Feb. 2017, pp. 1–8.

[4] Michael Aupetit, Yury Zhauniarovich, Giorgos Vasiliadis, Marc Dacier, and Yazan Boshmaf. "Visualization of Actionable Knowledge to Mitigate DRDoS Attacks". In: *Proceedings of the 2016 IEEE Symposium on Visualization for Cyber Security (VizSec)*. Oct. 2016, pp. 1–8.

[5] Olga Gadyatskaya, Andra-Lidia Lezza, and Yury Zhauniarovich. "Evaluation of Resource-based App Repackaging Detection in Android". In: *Proceedings of the 21st Nordic Conference on Secure IT Systems*. 2016, pp. 135–151.

[6] Yury Zhauniarovich and Olga Gadyatskaya. "Small Changes, Big Changes: An Updated View on the Android Permission System". In: *Proceedings of 19th International Symposium on Research in Attacks, Intrusions and Defenses*. 2016, pp. 346–367.

[7] Yury Zhauniarovich. "Security of the Android Operating System". In: *Risks and Security of Internet and Systems*. Vol. 8924. Lecture Notes in Computer Science. Springer International Publishing, 2015, pp. 272–274.

[8] Yury Zhauniarovich, Maqsood Ahmad, Olga Gadyatskaya, Bruno Crispo, and Fabio Massacci. "StaDynA: Addressing the Problem of Dynamic Code Updates in the Security Analysis of Android Applications". In: *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*. 2015, pp. 37–48.

[9] Yury Zhauniarovich, Anton Philippov, Olga Gadyatskaya, Bruno Crispo, and Fabio Massacci. "Towards Black Box Testing of Android Apps". In: *2015 Tenth International Conference on Availability, Reliability and Security*. Aug. 2015, pp. 501–510.

[10] Olga Gadyatskaya, Fabio Massacci, and Yury Zhauniarovich. "Security in the Firefox OS and Tizen Mobile Platforms". In: *IEEE Computer* 47.6 (June 2014), pp. 57–63.

[11] Yury Zhauniarovich. *Android Security (and Not) Internals*. `http://zhauniarovich.com/files/asani/asani.pdf`. Web, 2014.

[12] Yury Zhauniarovich. "Improving the Security of the Android Ecosystem". PhD thesis. University of Trento, Apr. 2014. URL: `http://eprints-phd.biblio.unitn.it/1266/`.

[13] Yury Zhauniarovich, Olga Gadyatskaya, and Bruno Crispo. *TruStore: Implementing a Trusted Store for Android*. Tech. rep. DISI-14-010. Department of Engineering and Computer Science, University of Trento, May 2014.

[14] Yury Zhauniarovich, Olga Gadyatskaya, Bruno Crispo, Francesco La Spina, and Ermanno Moser. "FSquaDRA: Fast Detection of Repackaged Applications". In: *Proceedings of the 28th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy*. 2014, pp. 131–146.

[15] Yury Zhauniarovich, Giovanni Russello, Mauro Conti, Bruno Crispo, and Earlence Fernandes. "MOSES: Supporting and Enforcing Security Profiles on Smartphones". In: *IEEE Transactions on Dependable and Secure Computing* 11.3 (May 2014), pp. 211–223.

[16] Yury Zhauniarovich, Olga Gadyatskaya, and Bruno Crispo. "DEMO: Enabling trusted stores for Android". In: *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13)*. 2013, pp. 1345–1348.

[17] Mauro Conti, Bruno Crispo, Earlence Fernandes, and Yury Zhauniarovich. "CRêPE: A System for Enforcing Fine-Grained Context-Related Policies on Android". In: *IEEE Transactions on Information Forensics and Security* 7.5 (2012), pp. 1426–1438.

[18] Giovanni Russello, Mauro Conti, Bruno Crispo, Earlence Fernandes, and Yury Zhauniarovich. "Demonstrating the Effectiveness of MOSES for Separation of Execution Modes". In: *Proceedings of the 2012 ACM SIGSAC Conference on Computer & Communications Security*. 2012, pp. 998–1000.

[19] Giovanni Russello, Bruno Crispo, Earlence Fernandes, and Yury Zhauniarovich. "YAASE: Yet Another Android Security Extension". In: *Proceedings of the 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT) and the 2011 IEEE Third International Conference on Social Computing (SocialCom)*. 2011, pp. 1033–1040.