Yury Zhauniarovich, PhD

Assistant Professor in Cybersecurity
R&D Professional

https://zhauniarovich.com
zhauniarovich
zyrikby

Important Achievements

- I am in the "**Top 2% Overall**" on StackOverflow
  `https://stackoverflow.com/users/1108213/yury`
- More than **20** scientific publications; **1** patent; more than **1000** citations; h-index: **16**
  `https://scholar.google.com/citations?user=jEBiXlQAAAAJ`
- More than **40** technical articles in the personal blog
  `https://zhauniarovich.com/post/`
- More than **25K/4K** monthly website pageviews according to Cloudflare/Google Analytics
  `https://zhauniarovich.com/post/2021/2021-09-comparison-of-cf-and-ga-data/`
- The author of the web book "Android Security (and Not) Internals" [Zha14a]
  `https://zhauniarovich.com/publication/2014/asani-zhauniarovich-2014/`

Experience

2021/10 – present **Assistant Professor**, *TU Delft*, Delft, Netherlands.

2020/07 – 2021/09 **R&D Engineer**, *Vertx Technologies Inc.*, San Francisco, USA, Remotely.

2020/01 – 2021/09 **Lead Data Scientist**, *AI Superior*, Darmstadt, Germany, Remotely.

2019/04 – 2019/11 **Head of R&D**, *Perfect Equanimity*, Minsk, Belarus.

2015/12 – 2019/04 **Scientist**, *Qatar Computing Research Institute*, Doha, Qatar.
- *2017/06 – 2019/04*: Scientist
- *2016/09 – 2016/12*: Lecturer for the course "Network security"
- *2015/12 – 2017/06*: Postdoctoral researcher

2014/05 – 2015/10 **Postdoctoral Researcher**, *University of Trento*, Trento, Italy.
- *2014/05 – 2015/10*: Postdoctoral researcher
- *2015/02 – 2015/09*: Lecturer for the course "Network security"
- *2014/04 – 2014/05*: Teaching assistant for the course "Network security"

2009/11 – 2014/04 **PhD Student**, *University of Trento*, Trento, Italy.
- *2009/11 – 2014/04*: PhD Student
- *2013/03 – 2013/04*: Teaching assistant for the course "Network security"
- *2011/02 – 2011/07*: Teaching assistant for the course "Network security"

2007/04 – 2009/10 **SAP SD/LE Consultant, Business Analyst**, *Itransition*, Minsk, Belarus.

2006/01 – 2007/03 **Part-time C++/SQL Developer**, *Department of Applied programs, Belarusian State University*, Minsk, Belarus.

Education

2009/11 – 2014/04 **Ph.D. in Computer Security**, *University of Trento*, Trento, Italy.
Thesis: Improving the Security of the Android Ecosystem
Advisor: Bruno Crispo

2006/09 – 2007/06 **M.Sc. (eq.) in Computer Security**, *Belarusian State University*, Minsk, Belarus.
Thesis: Steganographic Data Hiding Audiosystem with Heightened Throughput Capacity
Advisor: Vasiliy Sadov

2002/09 – 2006/06 **B.Sc. in Computer Security**, *Belarusian State University*, Minsk, Belarus.
Thesis: Development of a Web Ordering System for the University Computer Classes
Advisor: Natalia Novikova

Industrial Projects

Vertx Technologies Inc.

Dashboard to Compare Videos I implemented a dashboard that allows us to analyze a video match found by the Vertx system. The dashboard application parses a JSON file with match data and creates a timeline graph that shows the matches. If you click on a match, the system loads two video players, sets the start positions to the corresponding offsets, and plays the matching sections of two videos synchronously. That allows us to understand if a match is a true or false positive and why.
Technologies: Python (plotly, dash), Nginx, Docker, docker-compose

Real-time Multimedia Search I extended the company's service portfolio by implementing a service prototype to perform a real-time multimedia search for broadcast videos.
Technologies: Golang (gin, go-redis), SRS (Simple Realtime Server), Nginx (RTMP module), KeyDB (Redis), docker, docker-compose

Data Analysis I tested the Vertx system on several datasets to understand when the algorithm produces false positives and false negatives and why this happens. This analysis allowed us to improve the algorithm performance in some corner cases (e.g., when an adversary modifies a video play speed or when the found matches are short).
Technologies: Python (pandas, modin, plotly, jupyter lab)

Pre-sale Activities I developed crawlers to scrape the data of potential customers, ran the Vertx system to find video and audio matches, and analyzed the obtained results finding duplicated content or potentially copyrighted content. Based on the analysis, we generated actionable data (e.g., what duplicated or copyrighted videos require the customer's attention) and prepared sale presentations for the customer.
Technologies: Python (pandas, modin, plotly, jupyter lab, beautifulsoup4, selenium), bash

Website Migration I developed a new company website using Hugo static website generator (considerably extending the theme); created new sections (blog, news, and docs), filling them with the content that I also partially wrote. In addition, I developed a bash script to automate the website deployment process.
Technologies: Hugo, HTML/CSS/JS, bash, Nginx, Docker

Marketing I participated in the Vertx promotion. In particular, I proposed blog post ideas, wrote the content, and advertised it on various platforms (Reddit, Quora, etc.). For instance, I have discovered that the Vertex system can find the origin videos of deep fakes. I proved this finding experimentally and wrote a blog post describing the results.
I was involved in customer finding and analysis activities.

AI Superior

Bank Transaction Analysis I was a member of the team analyzing the credit card transactions data of the bank customers. Based on the analysis, we provided recommendations on where the bank should install ATMs and open subsidiaries. In addition, we gave insights on what marketing activities the bank should run and how to do this.
Technologies: Python (pandas, matplotlib, plotly)

Data Augmentation Within this project, I developed a crawler used to augment the developer expertise data with the information about her/his contributions to open-source projects. We used this data to provide better matches of developers for particular positions.
Technologies: Python (PyGithub), GitHub REST API

Perfect Equanimity

E-voting System Design I was a member of the team designing an e-voting system based on a public blockchain (state-of-the-art exploration, architecture proposal, pitfalls, and limitations analysis).
Technologies: Blockchain (Ethereum, TON, IOTA)

Qatar Computing Research Institute

Certificate Transparency Monitor I developed a platform that extracts certificate entries from the Certificate Transparency logs, indexes them, and provides a visual search across them.
Technologies: Certificate Transparency, Python (asyncio, aiohttp, elasticsearch-py), Elasticsearch, Kibana

Qatar Security Posture Assessment I was a member of the team that designed and developed the portal assessing the country's public security posture and reporting found security issues.
Technologies: Internet-wide scanners (zmap, masscan), nmap, ansible, Python (jupyter notebook, pandas)

DRDoS Visualization Portal I developed a portal that visualizes DRDoS attacks in real-time using the data collected from several amplification honeypots.
Technologies: Elasticsearch, Kibana, Python (elasticsearch-py), rsyslog

Itransition

Car Dealer Service Management System I was involved in the pre-sale activities (customer business examination and description) and then participated in the project as a business analyst during the implementation phase. During this phase, I collected business and user requirements, translated them into functional and non-functional requirements, prepared UI prototypes, and reconciled them with the customer.
Technologies: Borland Caliber RM, Axure RP, Microsoft Visio

SAP ERP for Agriculture Products Processing Company The goal of this project was to integrate an SAP ERP system into the company's business processes. During this project, I collected business and user requirements, adapted them according to the SAP's best practices, and configured Sales&Distribution and Logistics Execution modules.
Technologies: Microsoft Visio, SAP ERP (SD and LE modules)

Belarusian State University

Information System for the Ministry of Labor I was involved in the development of the information system for the Ministry of Labor. I designed a module to update data through modem connection using Win API and developed several system UI windows and forms.
Technologies: Borland C++ Builder 6.0, Microsoft SQL Server 2005

Information System for Computer Classroom Reservation I developed a prototype of the system for students to reserve time slots in computer classrooms.
Technologies: ASP.NET, C#, Microsoft SQL Server 2005, html/css

Academic Projects

Network Security

Community-Run RTBH Service Study

Within this project, we explore the Unwanted Traffic Removal Service (UTRS) – a free, global Remotely Triggered Black Hole (RTBH) alternative. In the work [Ang+23], we explore its global adoption and to what extent it is used to mitigate amplification and IoT-botnet-driven DDoS attacks. We found that during our study, only 124 Autonomous Systems (AS) out of more than 1200 UTRS members triggered blackholing events. Among those, only 25 Autonomous Systems (ASes) reacted on AmpPot attacks, mitigating 0.025% of them; and 2 countered IoT-botnet-driven attacks, alleviating 0.001% of them.
Technologies: Python (jupyter, pandas, matplotlib, netaddr)

Removing DRDoS Garbage Traffic from ISP Networks

Internet Service Provider (ISP) Networks may accommodate thousands of hosts running UDP protocols vulnerable to amplification. If abused, these amplifiers can collectively generate large volumes of garbage traffic that costs the provider money and degrades the quality of service for its customers. We proposed a novel idea to filter out this garbage traffic from an ISP network. We employed special honeypots, which collect information about the ongoing DRDoS attacks, and the Software Defined Network (SDN) paradigm, which offers us a unified interface to deploy firewall rules to a large variety of network devices. Based on the information collected from amplification honeypots about the ongoing attacks, we generate firewall rules that block incoming amplification requests from reaching the amplifiers located within the provider network. That rescues vulnerable hosts from being abused. This work was presented at IEEE NetSoft '19 [ZD19], while the demonstration of the prototype occurred at the ACM CCS '19 conference [DZ19]. A patent was obtained for the approach in 2021 [ZD21].
Technologies: Elasticsearch, Kibana, SDN, OpenFlow, Python (jupyter notebook, pandas, elasticsearch-py, amppot, POX)

Suspicious Domain Detection

This project goal is to build a scalable, effective and efficient platform to detect domains involved in different malicious activities, e.g., botnet C&C domains, domains generated algorithmically, phishing domains, etc. We aimed at detecting these domains before being used in malicious campaigns. During the first step, we surveyed the state-of-the-art on how malicious domains can be detected [Zha+18].
Technologies: Elasticsearch, Kibana, Python (jupyter notebook, scikit-learn, pandas, elasticsearch-py, asyncio, aiohttp)

Cyber Intelligence Platform

The goal of this project is to build a highly scalable, open-source intelligence platform to analyze and detect cybersecurity incidents in near real-time. Therefore, as building blocks for this platform, we used horizontally scalable open-source systems, e.g., Apache Storm and Elasticsearch. We aimed at using this platform in different areas of security research. In particular, we employed this platform to collect, store and analyze the data obtained from amplification honeypots. We presented the results of this data analysis at ACM CIKM '17 [BEZ17]. Additionally, on top of our platform, we built a tool allowing one to assess the influence of different firewall rules on the amount of traffic entering and leaving an ISP network if it contains hosts vulnerable to amplification attacks. This work was presented at the IEEE Symposium on Visualization for Cyber Security 2016 [Aup+16].
Technologies: Elasticsearch, Kibana, Apache Storm, Apache Kafka, Java, Python (jupyter notebook, scikit-learn, pandas, elasticsearch-py, amppot)

Blockchain Data Analysis

Characterizing Bitcoin Donations to Open Source Software

Within this project, we studied the use of Bitcoin to make donations to open source repositories on GitHub. In particular, we analyzed the amount and the volume of donations over time, their relationship to the repository age and popularity. We scanned over three million repositories looking for donation addresses. We then extracted and analyzed their transactions from the Bitcoin public blockchain. Overall, we found a limited adoption of Bitcoin as a payment method for receiving donations, with nearly 44 thousand deposits adding up to only 8.3 million dollars in the last 10 years. All our findings are available in the technical report [Zha+19].
Technologies: Bitcoin, BlockSci, Google BigQuery, Python (jupyter notebook, pandas, TkInter)

Android Security

Android Cryptocurrency Miners

Within this project, we collected a large dataset of Android cryptocurrency miners. We carefully analyzed the samples from the dataset, identified static features specific to mobile miners and proposed a system to detect miners on a device at runtime. We shared the preliminary findings of our work in the technical report [Das+19]; and presented our final results in the ACM CODASPY 2020 paper [Das+20].
Technologies: Virustotal, Koodous, YARA rules, Snapdragon Profiler, Python (pandas, jupyter notebook, scikit-learn)

Android Blackbox Code Coverage

We explored how code coverage metrics collected in a blackbox manner can be used in various Android application analysis scenarios. We demonstrated the prototype of the system collecting fine-grained code coverage metrics at the ARES workshop [Zha+15b]. Later, we developed a new approach for app instrumentation and presented it at the ACM CCS '18 conference [Pil+18a]. The technical report [Pil+18b] and the journal article [Pil+20] provide a detailed description of this new system. With the help of this new tool, we evaluated how fine-grained code coverage metrics can improve the efficiency of automated testing tools. We presented the results of this research at the ACM CCS '18 conference [Das+18].
Technologies: Python (pandas, jupyter notebook)

Android Permission Analysis

In this work, we explored the evolution of the permission system in the Android operating system. In particular, we analyzed permissions added, deleted, or modified between different versions of Android; how protection level and permission flag values influence the behavior of the corresponding permissions. We presented the results of this work at the RAID symposium in 2016 [ZG16].
Technologies: AOSP, Python (pandas, jupyter notebook, matplotlib)

Passive Mobile User Authentication

In the scope of this project, we proposed a new method for passive user authentication using smartphone sensor data. The data from sensors are collected during a short interval just after the screen unlock event. Using the features extracted from the collected data and applying a machine learning model, we are able to discriminate a genuine user from an adversary. We presented this work at the IEEE ISBA '17 conference [BCZ17].
Technologies: Java, Android, Python (scikit-learn, pandas, jupyter notebook)

Analysis of the Android apps in the presence of dynamic code update features

In this work, we studied how Android applications use dynamic code updates features, in particular, reflection and dynamic class loading. Adversaries often use this functionality to conceal the malicious behavior of Android apps. Based on this observation, we proposed a novel approach, which combines static and dynamic analysis techniques, to analyze Android apps containing dynamic code update features and developed a system based on this approach called StaDynA. We presented our system and the findings at the ACM CODASPY '15 [Zha+15a] conference. Later, based on StaDynA, we developed StaDART, the tool that analyzes dynamic code update features but does not require modification of the Android framework. We published the details of our approach in Elsevier's JSS article [Ahm+20].
Technologies: AOSP, Java, Python (androguard, networkx)

Detection of Repackaged Android Applications

Within this project, we explored novel techniques to detect repackaged Android applications. Our approach relies on the calculation of a similarity metric based on the hashes of the files that constitute two Android packages. The main know-how of our approach is that we do not compute the hashes of files ourselves. Instead, we rely on the hashes computed during the Android package signing process. Thus, we can speed up the process of finding similar pairs considerably. We presented the results of this work at the DBSec '14 [Zha+14a] conference. In the NordSec '16 [GLZ16] paper, we explored what similarity metric is the better and what type of resources are more and less likely to be modified during the repackaging process. Both systems are open source.
Technologies: Java, Python (androguard, pandas, scikit-learn)

Android Trusted Stores

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 ACM CCS '13 [ZGC13], while the technical report [ZGC14] contains a detailed description of our approach.
Technologies: AOSP, Java

Enforcing Security Profiles in Android

We proposed a policy-based framework for enforcing software isolation of applications and data that helps to improve the security of end-user devices. The demo of MOSES was presented at ACM CCS '12 [Rus+12], while the paper published in IEEE TDSC [Zha+14b] describes our system in detail.
Technologies: AOSP, Java, C, TaintDroid

Context-Related Policy Enforcement

We implemented a system called CRêPE that allows one to define and enforce the behavior of smartphone applications depending on the context. In CRêPE, a context can 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). We published the results of this work in the IEEE TIFS [Con+12] journal.
Technologies: AOSP, Java, C

Collusion Attack Prevention in Android

We extended the Android operating system with a subsystem allowing one to enforce fine-grained policies that help to mitigate the threat of colluding applications leaking sensitive information. We use TaintDroid to assign special taints to the sensitive information and implemented an enforcement point that imposes the fine-grained decisions according to the specified policies. We presented our system at the PASSAT/SocialCom 2011 conference [Rus+11].
Technologies: AOSP, Java, C, TaintDroid

Funding Projects

Delft University of Technology

THESEUS **Description:** The central goal of the THESEUS project is to empower organizations to patch security vulnerabilities much faster, more efficiently and with less risk.
My Role: Within the team at TU Delft, I am responsible for developing novel methods for assessing the patching status of organizations and benchmarking them using this data. Additionally, we want to discover the factors that can explain the difference in patching levels of similar organizations and can guide us in the development of better patching procedures and policies.
Additionally, I am the developer of the project website.
Publications within the Project: [Eth+24]
Funding Agency: NWO
Duration: October 2021 - October 2027
Status: Ongoing

University of Trento

MobileShield 2015 **Description:** The goal of the project is the launch and offering of security services for the detection and identification of mobile malware, the security rating of mobile applications and their trusted distribution.
My Role: I developed a prototype of the platform that performs remote attestation of an Android device to assess if it is secure enough to run sensitive applications. The working principle of this platform, which consists of a library embedded into a protected app and a server, is the following. The client collects information about the device (e.g., if the device is rooted or runs block-listed apps) and sends this information to the server. The server also creates a VPN tunnel allowing one to analyze all the network traffic from the device. Based on the analysis of the network traffic and the provided client's data, the server decides if the device is secure.
Funding Agency: EIT Digital
Duration: January 2015 - December 2015
Status: Finished

Public Talks

2023/11/27 **Event talk**, *Collaborative DDoS Mitigation Event*, Utrecht, Netherlands.
Peering into the Darkness: The Use of UTRS in Combating DDoS Attacks

2023/09/25 **Conference talk**, *ESORICS '23*, The Hague, Netherlands.
Peering into the Darkness: The Use of UTRS in Combating DDoS Attacks

2022/11/18 **Invited talk**, *Leiden University (LIACS)*, Leiden, Netherlands.
Detection of Internet-wide BGP RTBH Communities

2022/11/01 **Invited talk**, *TU Delft (EEMCS)*, Delft, Netherlands.
Detection of Internet-wide BGP RTBH Communities

2022/05/31 **Guest lecture**, *TU Delft (EEMCS)*, Delft, Netherlands.
Locality Sensitive Hashing (LSH)

2019/06/24 **Invited talk**, *University of Luxembourg*, Luxembourg.
Characterizing Bitcoin Donations to Open Source Software on GitHub

2018/06/29 **Invited talk**, *University of Luxembourg*, Luxembourg.
Sorting the Garbage: Filtering Out DRDoS Amplification Traffic in ISP Networks

2017/03/06 **Invited talk**, *University of Luxembourg*, Luxembourg.
Small Changes, Big Changes: An Updated View on the Android Permission System

2016/09/21 **Conference talk**, *RAID '16*, Evry, France.
Small Changes, Big Changes: An Updated View on the Android Permission System

2014/04/30 **PhD defense**, *University of Trento*, Rome, Italy.
Improving the Security of the Android Ecosystem

2014/02/27 **Invited talk**, *University of Rome "La Sapienza"*, Rome, Italy.
StaDynA: Addressing the Problem of Dynamic Code Updates in the Security Analysis of Android Apps

2014/02/20 **Invited talk**, *University of Luxembourg*, Luxembourg.
StaDynA: Addressing the Problem of Dynamic Code Updates in the Security Analysis of Android Apps

2014/08/27 **Tutorial**, *CRISiS '14*, Trento, Italy.
Android Security

2014/07/14 **Conference talk**, *DBSec '14*, Vienna, Austria.
FSquaDRA: Fast Detection of Repackaged Applications

Academic Advising

PhD Researchers

2023/02 – ~2027 **Szu-Chun Huang**, TU Delft (TPM), daily supervisor.
Benchmarking of Organizational Patching Behavior

2021/10 – ~2025 **Radu Anghel**, TU Delft (TPM), daily co-supervisor.
Securing Internet Routing

2021/08 – ~2025 **Aksel Ethembabaoglu**, TU Delft (TPM), daily co-supervisor.
Patching Landscape Exploration

Master Students

2023/02 – 2023/10 **Berend Kloeg**, TU Delft (TPM), 1^{st} supervisor.
Unraveling Incentives: Understanding the Adoption Barriers of SBOM in the Software Supply Chain

2022/11 – 2023/09 **Erik Sennema**, TU Delft (EEMCS), co-supervisor.
Elastic CatBoost Uncertainty (eCBU): Elastic Gradient Boosting Decision Trees under Limited Labels by Sequential Epistemic Uncertainty Quantification

2023/03 – 2023/08 **Dorukhan Yesilli**, TU Delft (TPM), 1^{st} supervisor.
Operational Resilience: Backup Strategies for Crisis Management in the Age of Ransomware

2023/03 – 2023/08 **Hilmy Hanif**, TU Delft (TPM), 1^{st} supervisor.
Enhancing AI Systems Classification Framework: A Study of the EU's Proposed AI Act
The results are presented at JURIX'23 [Han+23]

2023/02 – 2023/08 **Anne-Kee Doing**, TU Delft (TPM), 2^{nd} supervisor.
Learning from Phishing Emails: Creating New Metrics to Measure the Effect of Anti-phishing Training in a Large Company

2022/11 – 2023/07 **Feiyang Sun**, Leiden University (LIACS), 2^{nd} supervisor.
Explanation of XAI Clustering Methods on Android Malware Family Categorization

2022/11 – 2023/07 **Daan Hofman**, TU Delft (EEMCS), co-supervisor.
VoBERT: Unstable Log Sequence Anomaly Detection
The results are presented at BlackHat Europe 2023

2022/11 – 2023/05 **Job Onkenhout**, TU Delft (TPM), 2^{nd} supervisor.
Secure Payments in the Quantum Era: A Technology Roadmap for the Post-Quantum Cryptography Transition in the Dutch Banking Sector

2022/09 – 2023/03 **Yunus Sezer**, TU Delft (TPM), 1^{st} supervisor.
The Cryptogeddon of Blockchain: Designing Policy Recommendations for Public Blockchains to Transition towards a Quantum-safe Environment

2022/02 – 2022/08 **Abdulkhamid Mukhamedov**, TU Delft (TPM), 1^{st} advisor.
The Risks and Regulation of Decentralized Finance: A Recommendation to EU Policy Makers

2017/07 – 2018/12 **Talal Shoeb**, Hamad Bin Khalifa University, supervisor.
Insight: A Kibana Visualization Plugin for Multidimensional Data Exploration

2017/07 – 2018/06 **Priyanka Dodia**, Hamad Bin Khalifa University, supervisor.
Honeypot-Based Filtering of Amplification Traffic in ISP Networks
The results are presented at IEEE NetSoft'19 [ZD19] and ACM CCS'19 [DZ19]

Bachelor Students

2022/03 – 2022/06 **Victor de Jong**, TU Delft (EEMCS), co-supervisor.
Storage and Retrieval Mechanisms in Mobile Spam Blocking Applications

2022/03 – 2022/06 **Christiaan van Luik**, TU Delft (EEMCS), co-supervisor.
Dynamic Analysis of Android Applications to Extract Spam Caller IDs

2022/03 – 2022/06 **Colin Busropan**, TU Delft (EEMCS), co-supervisor.
Analysis of Components in the Manifest File of Spam Call Blocking Applications on Android

2022/03 – 2022/06 **Yoon Hwan Jeong**, TU Delft (EEMCS), co-supervisor.
Static Analysis of Spam Call Blocking Applications: Common Android APIs Used for Call Interception and Blocking

2022/03 – 2022/06 **Atanas Pashov**, TU Delft (EEMCS), co-supervisor.
Analysing Android Spam Call Applications: Developing a Methodology For Dynamic Analysis

Honors, Awards, and Grants

2009/11 Ph.D. Scholarship from the University of Trento
2002/10 Scholarship from Belarusian State University
2002/06 Graduated Cum Laude from Lyceum BSU
2002/05 Winner of the BSU Olympiad in Physics

Publications

Conference Papers

[Eth+24] Aksel Ethembabaoglu, Rolf van Wegberg, Yury Zhauniarovich, and Michel van Eeten. "The Unpatchables: Why Municipalities Persist in Running Vulnerable Hosts". In: *33rd USENIX Security Symposium*. USENIX Security '24. Aug. 2024.

[Ang+23] Radu Anghel, Swaathi Vetrivel, Elsa Turcios Rodriguez, Kaichi Sameshima, Daisuke Makita, Katsunari Yoshioka, Carlos H. Gañán, and Yury Zhauniarovich. "Peering into the Darkness: The Use of UTRS in Combating DDoS Attacks". In: *European Symposium on Research in Computer Security (ESORICS)*. 2023, to appear.

[Han+23] Hilmy Hanif, Jorge Constantino, Marie-Therese Sekwenz, Michel van Eeten, Jolien Ubacht, Ben Wagner, and Yury Zhauniarovich. "Tough Decisions? Supporting System Classification According to the AI Act". In: *International Conference on Legal Knowledge and Information Systems*. Frontiers in Artificial Intelligence and Applications. IOS Press, Dec. 2023, pp. 353–358. DOI: 10.3233/faia230987.

[Nos+23] Yevheniya Nosyk, Qasim Lone, Yury Zhauniarovich, Carlos H. Gañán, Emile Aben, Giovane C. M. Moura, Samaneh Tajalizadehkhoob, Andrzej Duda, and Maciej Korczyński. "Intercept and Inject: DNS Response Manipulation in the Wild". In: *Passive and Active Measurement (PAM)*. 2023, pp. 461–478.

[Das+20] Stanislav Dashevskyi, Yury Zhauniarovich, Olga Gadyatskaya, Aleksandr Pilgun, and Hamza Ouhssain. "Dissecting Android Cryptocurrency Miners". In: *ACM Conference on Data and Application Security and Privacy (CODASPY)*. 2020, pp. 191–202.

[ZD19] Yury Zhauniarovich and Priyanka Dodia. "Sorting the Garbage: Filtering Out DRDoS Amplification Traffic in ISP Networks". In: *IEEE Conference on Network Softwarization (NetSoft)*. 2019, pp. 142–150.

[BEZ17] Laure Berti-Equille and Yury Zhauniarovich. "Profiling DRDoS Attacks with Data Analytics Pipeline". In: *ACM Conference on Information and Knowledge Management (CIKM)*. 2017, pp. 1983–1986.

[BCZ17] Attaullah Buriro, Bruno Crispo, and Yury Zhauniarovich. "Please Hold On: Unobtrusive User Authentication Using Smartphone's Built-in Sensors". In: *IEEE Conference on Identity, Security and Behavior Analysis (ISBA)*. 2017, pp. 1–8.

[Aup+16] Michael Aupetit, Yury Zhauniarovich, Giorgos Vasiliadis, Marc Dacier, and Yazan Boshmaf. "Visualization of Actionable Knowledge to Mitigate DRDoS Attacks". In: *IEEE Symposium on Visualization for Cyber Security (VizSec)*. 2016, pp. 1–8.

[GLZ16] Olga Gadyatskaya, Andra-Lidia Lezza, and Yury Zhauniarovich. "Evaluation of Resource-based App Repackaging Detection in Android". In: *Nordic Conference on Secure IT Systems (NordSec)*. 2016, pp. 135–151.

[ZG16] Yury Zhauniarovich and Olga Gadyatskaya. "Small Changes, Big Changes: An Updated View on the Android Permission System". In: *Symposium on Research in Attacks, Intrusions and Defenses (RAID)*. 2016, pp. 346–367.

[Zha15] Yury Zhauniarovich. "Security of the Android Operating System". In: *Risks and Security of Internet and Systems (CRiSIS)*. Vol. 8924. Lecture Notes in Computer Science. Springer International Publishing, 2015, pp. 272–274.

[Zha+15a] 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: *ACM Conference on Data and Application Security and Privacy (CODASPY)*. 2015, pp. 37–48.

[Zha+14a] Yury Zhauniarovich, Olga Gadyatskaya, Bruno Crispo, Francesco La Spina, and Ermanno Moser. "FSquaDRA: Fast Detection of Repackaged Applications". In: *Conference on Data and Applications Security and Privacy (DBSec)*. 2014, pp. 131–146.

[Rus+11] Giovanni Russello, Bruno Crispo, Earlence Fernandes, and Yury Zhauniarovich. "YAASE: Yet Another Android Security Extension". In: *IEEE Conference on Privacy, Security, Risk and Trust (PASSAT) and the IEEE Conference on Social Computing (SocialCom)*. 2011, pp. 1033–1040.

Journal Papers

[Ahm+20] Maqsood Ahmad, Valerio Costamagna, Bruno Crispo, Francesco Bergadano, and Yury Zhauniarovich. "StaDART: Addressing the Problem of Dynamic Code Updates in the Security Analysis of Android Applications". In: *Journal of Systems and Software (JSS)* 159 (2020), p. 110386.

[Pil+20] Aleksandr Pilgun, Olga Gadyatskaya, Yury Zhauniarovich, Stanislav Dashevskyi, Artsiom Kushniarou, and Sjouke Mauw. "Fine-grained Code Coverage Measurement in Automated Black-box Android Testing". In: *ACM Transactions on Software Engineering and Methodology (TOSEM)* 29.4 (2020).

[Zha+18] Yury Zhauniarovich, Issa Khalil, Ting Yu, and Marc Dacier. "A Survey on Malicious Domains Detection through DNS Data Analysis". In: *ACM Computing Surveys (CSUR)* 51.4 (2018), 67:1–67:36.

[GMZ14] Olga Gadyatskaya, Fabio Massacci, and Yury Zhauniarovich. "Security in the Firefox OS and Tizen Mobile Platforms". In: *IEEE Computer* 47.6 (2014), pp. 57–63.

[Zha+14b] 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 (TDSC)* 11.3 (2014), pp. 211–223.

[Con+12] 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 (TIFS)* 7.5 (2012), pp. 1426–1438.

Workshop Papers

[Zha+15b] Yury Zhauniarovich, Anton Philippov, Olga Gadyatskaya, Bruno Crispo, and Fabio Massacci. "Towards Black Box Testing of Android Apps". In: *Conference on Availability, Reliability and Security (ARES)*. 2015, pp. 501–510.

Poster/Demo Papers

[DZ19] Priyanka Dodia and Yury Zhauniarovich. "Poster: SDN-based System to Filter Out DRDoS Amplification Traffic in ISP Networks". In: *ACM Conference on Computer and Communications Security (CCS)*. 2019, pp. 2645–2647.

[Das+18] Stanislav Dashevskyi, Olga Gadyatskaya, Aleksandr Pilgun, and Yury Zhauniarovich. "The Influence of Code Coverage Metrics on Automated Testing Efficiency in Android". In: *ACM Conference on Computer and Communications Security (CCS)*. 2018, pp. 2216–2218.

[Pil+18a] Aleksandr Pilgun, Olga Gadyatskaya, Stanislav Dashevskyi, Yury Zhauniarovich, and Artsiom Kushniarou. "An Effective Android Code Coverage Tool". In: *ACM Conference on Computer and Communications Security (CCS)*. 2018, pp. 2189–2191.

[ZGC13] Yury Zhauniarovich, Olga Gadyatskaya, and Bruno Crispo. "DEMO: Enabling trusted stores for Android". In: *ACM Conference on Computer and Communications Security (CCS)*. 2013, pp. 1345–1348.

[Rus+12] Giovanni Russello, Mauro Conti, Bruno Crispo, Earlence Fernandes, and Yury Zhauniarovich. "Demonstrating the Effectiveness of MOSES for Separation of Execution Modes". In: *ACM Conference on Computer and Communications Security (CCS)*. 2012, pp. 998–1000.

Technical Reports

[Das+19] Stanislav Dashevskyi, Yury Zhauniarovich, Olga Gadyatskaya, Aleksandr Pilgun, and Hamza Ouhssain. *Dissecting Android Cryptocurrency Miners*. Tech. rep. 2019. arXiv: 1905.02602 [cs.CR].

[Zha+19] Yury Zhauniarovich, Yazan Boshmaf, Husam Al Jawaheri, and Mashael Al Sabah. *Characterizing Bitcoin Donations to Open Source Software on GitHub*. Tech. rep. 2019. arXiv: 1907.04002 [cs.CR].

[Pil+18b] Aleksandr Pilgun, Olga Gadyatskaya, Stanislav Dashevskyi, Yury Zhauniarovich, and Artsiom Kushniarou. *Fine-grained Code Coverage Measurement in Automated Black-box Android Testing*. Tech. rep. 2018. arXiv: 1812.10729 [cs.CR].

[ZGC14] 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, 2014.

Patents

[ZD21] Yury Zhauniarovich and Priyanka Dodia. "Methods and Systems for Reducing Unwanted Data Traffic in a Computer Network". Pat. US Patent 11,206,286. 2021.

Others

[Zha14a] Yury Zhauniarovich. *Android Security (and Not) Internals*. https://zhauniarovich.com/publication/2014/asani-zhauniarovich-2014/asani-zhauniarovich-2014.pdf. Web, 2014.

[Zha14b] Yury Zhauniarovich. "Improving the Security of the Android Ecosystem". PhD thesis. University of Trento, 2014. URL: http://eprints-phd.biblio.unitn.it/1266/.