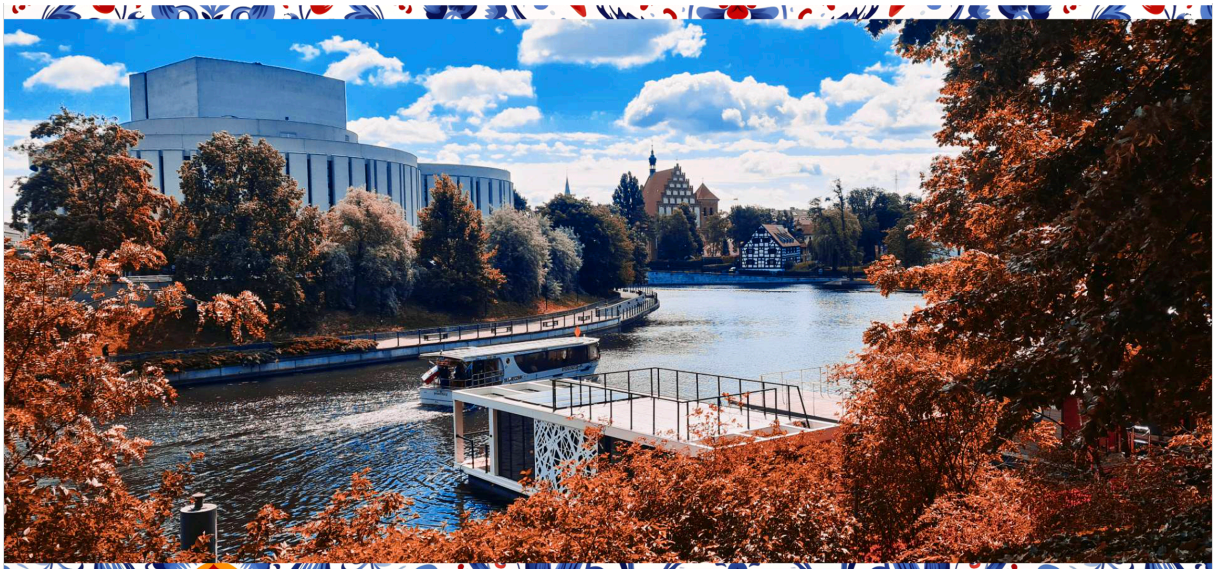
ESORICS



29th European Symposium on Research in Computer Security

September 16-20, 2024
Bydgoszcz, Poland

Conference Handbook

as of 3rd September 2024

Handbook by:
Aleksandra Pawlicka
Marek Pawlicki
Michał Choraś
Joaquin Garcia-Alfaro
General inquiries:
michal.choras@pbs.edu.pl

Table of Contents

How to Get to the Conference

Note: Google Maps works well for public transportation and route planning in Poland. The information it provides on buses, trams, and trains is usually very reliable, accurate, and up to date.

Conference location

Politechnika Bydgoska im. Jana i Jędrzeja Śniadeckich
(Bydgoszcz University of Science and Technology)
Al. prof. S. Kaliskiego 7
85-796 Bydgoszcz
Poland
https://maps.app.goo.gl/sXG1tdTGQYf5K9yNA

NEW! Special Lufthansa Group airlines fares

The Lufthansa Group airlines bring people together - every day, all around the world. The global route network of Austrian Airlines, Lufthansa, SWISS, Brussels Airlines and Eurowings offers optimal connection and combination options, so you will benefit from quick and direct flights to the event.
You will reach the booking platform via this link https://www.lufthansa.com/de/en/meetings-and-events-delegates and with the event code PLAPDBX.
The reduced fares are automatically displayed.
NB: Please enable pop-ups permanently in your browser while booking, otherwise the window in the booking platform will not open.

Getting to Bydgoszcz from major cities

From Warsaw Chopin Airport

By Train:

- For example, you can take the S2 or S3 line from Warszawa Lotnisko Chopina (Chopin Airport) train station to **Warszawa Zachodnia** train station. The journey takes approximately 20 minutes. Or: Take bus number 175 directly from the airport to **Warszawa Centralna / Dworzec Centralny** train station. The journey takes about 25-30 minutes.
- At **Warszawa Zachodnia/ Warszawa Centralna**, direct trains to **Bydgoszcz Główna** are available. The journey takes

approximately 3 hours. Check the Polish Railways website for schedules and tickets: https://rozklad-pkp.pl/en

By Car:

- Take the A2 motorway westwards towards Poznań, then switch to the S5 motorway northwards directly to Bydgoszcz. The drive takes approximately 3 hours.

From Poznań Ławica Airport

By Train:

- Take bus number 159 from the airport to **Poznań Główny**. The journey takes about 20-25 minutes or take a taxi; taxis are available outside the arrivals terminal. The journey to the main train station takes about 15 minutes.
- Direct trains from **Poznań Główny** to **Bydgoszcz Główna** are available. The journey takes approximately 1.5-2 hours. Check the Polish Railways website for schedules and tickets: https://rozklad-pkp.pl/en

By Car:

- Take the S5 motorway northwards directly to Bydgoszcz. The drive takes approximately 2 hours.

From Gdańsk Lech Wałęsa Airport

By Train:
Take the train from the **Gdańsk Port Lotniczy** train station or take bus number 210 from the airport directly to **Gdańsk Główny**. The journey takes about 35-40 minutes. Direct trains from **Gdańsk Główny** to **Bydgoszcz Główna** are available. The journey takes approximately 1.5-2 hours. Check the Polish Railways website for schedules and tickets: https://rozklad-pkp.pl/en

By Car:

- Take the A1 motorway southwards towards Toruń, then switch to the S5 motorway westwards to Bydgoszcz. The drive takes approximately 2 hours.

Getting around Bydgoszcz

You can explore Bydgoszcz using the public bus and tram network, or you may prefer the convenience of taxis and ride-sharing services. For those who enjoy outdoor activities, bike and scooter sharing services are readily available throughout the city.

Bus/ tram

Navigating Bydgoszcz by bus or tram is quite convenient, with GoogleMaps working well as far as routes are concerned. You'll find the up-to-date timetables here: https://www.zdmikp.bydgoszcz.pl/pl/rozkady

In many buses and trams, you can purchase a ticket with a contactless payment card. Each vehicle where tickets can be purchased with a contactless payment card is marked with a special sticker on the window near the middle doors. In the case of two-car trams, the Open Payment System device is available only in the first car.

In order to buy a ticket, on the Open Payment System device screen, select the appropriate type of ticket. Next, place your payment card near the reader, and the ticket will be purchased. During ticket inspections, simply show the payment card used for the transaction to the inspector, or place the card near the Open Payment System device.

For smoother travelling, it is recommended to buy a ticket before entering the vehicle, though. You can use the following apps/services to do so:

- Mint mobile https://bydgoskakartamiejska.com.pl/pl/news/aid/3595
- zbiletem https://zbiletem.pl/
- Skycash https://www.skycash.com/bilety-komunikacji-miejskiej-w-telefonie/
- Jakdojade https://www.jakdojade.pl
- mPay https://www.mpay.pl/

Most bus and tram stops are equipped with digital boards that display up-to-the-minute arrival information.

Taxi

The names of streets can be real tongue twisters! For your convenience, use an app where you provide the target address beforehand, for example ExpressTaxi Bydgoszcz (one of the official taxi companies in Bydgoszcz, the link to the app is to be found at https://19629.pl), or freelance services like Bolt or Uber.

In addition, unlike hailing a taxi directly from the street, ordering a taxi via an app provides the advantages of knowing your fare in advance and paying by card upfront.

Car

Driving in Bydgoszcz is an option for those who prefer to travel by car, with ample parking and several main routes throughout the city. Please be aware that ongoing construction and renovation projects may affect traffic flow and accessibility in certain areas. We recommend using Google Maps to check current traffic conditions and any obstacles before you set out.

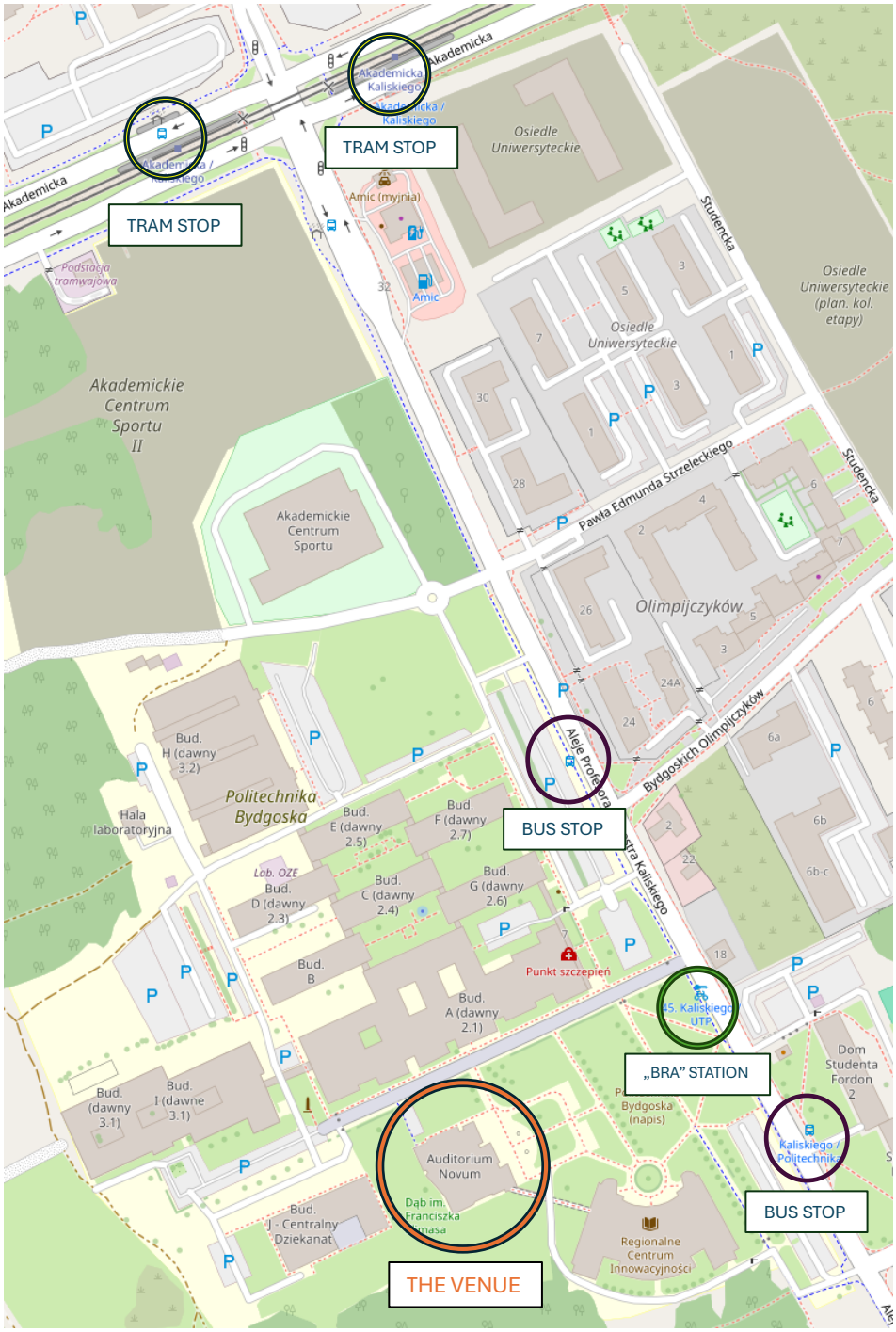
Short-term parking zones are liable for costs in Bydgoszcz's city centre; parking around the venue is free of charge.

Bike

To navigate the city and discover its attractions in a convenient, cheap and eco-friendly way you may consider using the Bydgoski Rower Aglomeracyjny (BRA) bike rental system, with one of the stations located directly at the PBS Campus.
Check https://bra.org.pl for more details.

How to get to the venue?

The conference takes place in the Auditorium Novum building, which is part of the Bydgoszcz University of Science and Technology Campus (shown in the map below).



The nearest bus stop is called "Kaliskiego - Politechnika" while the tram stop closest to the venue is called "Akademicka - Kaliskiego".

The address:
Al. prof. S. Kaliskiego 7 (7 Kaliskiego Street), 85-796 Bydgoszcz

To get there from the **Bydgoszcz Airport (Ignacy Jan Paderewski Airport, BZG),** use **public transport**:

- Exit the airport terminal and head towards the bus stop.
- Take bus number 80 heading towards "Dworzec Główny".

- Alight at the “Rondo Inowrocławskie” bus stop and transfer to bus no. 89, heading towards “Tatrzańskie”.
- Get off at the “Kaliskiego – Politechnika” but stop, directly by the campus.
- Alternatively, when in bus no. 80., get off at the "Dworzec Autobusowy" bus stop and transfer to tram lines 3 or 5 (both heading towards “Łoskoń"), or 10 (heading either towards “Łoskoń" or “Niepodległości”).
- Get off at the “Akademicka – Kaliskiego” tram stop and take a short walk to the venue.

You can also take **a taxi** (use an app, or choose one of the taxis available outside the arrivals terminal. Provide the driver with the address “Politechnika Bydgoska im. Jana i Jędrzeja Śniadeckich, Profesora Sylwestra Kaliskiego 7, 85-796”.) The journey should take about 15-20 minutes, depending on traffic.

From Bydgoszcz Główna (Main Train Station):
By Taxi:

- Use an app, or choose one of the taxis available outside the main entrance of the train station. Provide the driver with the address “Politechnika Bydgoska im. Jana i Jędrzeja Śniadeckich, Profesora Sylwestra Kaliskiego 7, 85-796”. The journey should take about 15-30 minutes, depending on traffic.

By Public Transport:

- Exit the train station and walk to the tram stop "Dworzec Główny".
- Take the tram number 5 heading towards "Łoskoń" (about a 30-minute trip).
- Alight at "Akademicka - Kaliskiego" and take a short walk to the venue.

Conference Programme

MONDAY 16.09.2024			
	Venue: **AUDITORIUM NOVUM** (Kaliskiego 7, Bydgoszcz)		
8:30	Registration		
9:00	Opening		
9:10	Keynote Prof.dr hab. inż. Józef Pieprzyk		
10:10	Coffee Break		
		Aula A	**Aula B**
10:30	Conference Sessions	AI/ML & Security I	Network, Web & Privacy I
12:10	Lunch		
13:30	Conference Sessions	SW & Systems Security I	Crypto I
15:30	Coffee Break		
15:50	Conference Sessions	AI/ML & Security II	Network, Web & Privacy II
17:30	End of Day 1		
19:30	Welcome Reception (City Centre)		

TUESDAY 17.09.2024

Venue: **AUDITORIUM NOVUM** (Kaliskiego 7, Bydgoszcz)

9:00	Keynote Prof. dr hab. inż. Wojciech Mazurczyk		
10:10	Coffee Break		
		Aula A	**Aula B**
10:30	Conference Sessions	AI/ML & Security III	Network, Web & Privacy III
12:10	Lunch		
13:30	Conference Sessions	HW & Cloud Security I	Crypto II
15:30	End of Day 2		
17:00	Gniew Castle Tour Gala Dinner		

WEDNESDAY 18.09.2024

Venue: **AUDITORIUM NOVUM** (Kaliskiego 7, Bydgoszcz)

		Aula A	**Aula B**
10:30	Conference Sessions	AI/ML & Security IV	Attacks & Defense I
12:10	Lunch		
13:30	Conference Sessions	Network, Web & Privacy IV	Attacks & Defense II
15:10	Coffee Break		
15:30	Conference Sessions	HW & Cloud Security II SW & Systems Security II Crypto III	Attacks & Defense III
17:30	Conference Closing		

Thursday	Day 4			
19.09.2024				
09:00-10:30	Workshop sessions:	DPM	CPS4CIP	CBT
10:30-10:45	Coffee Break			
10:45-12:15	Workshop sessions:	DPM	DiSA	CBT
12:15-13:45	Lunch			
13:45-15:15	Workshop sessions:	DPM	DiSA	CBT
15:15-15:30	Coffee Break			
15:30-17:00	Workshop sessions:	DPM	SECAI	CBT
17:30	Ice Breaker Social Event			

Friday	Day 5				
20.09.2024					
09:00-10:30	Workshop sessions:	STM	SECAI	CyberICPS	SecAssure
10:30-10:45	Coffee Break				
10:45-12:15	Workshop sessions:	STM	SECAI	CyberICPS	SecAssure
12:15-13:45	Lunch				
13:45-15:15	Workshop sessions:	STM	SECAI	CyberICPS	SecAssure
15:15-15:30	Coffee Break				
15:30-17:00	Workshop sessions:	STM	SECAI	CyberICPS	SecAssure

Detailed programme

MONDAY, 16.09.2024				
Time	**ID**	**Presentation**	**ID**	**Presentation**
08:30	Registration			
09:00	Opening			
09:10	Keynote: **Prof. Dr hab. Inż. Józef Pieprzyk**			
10:10	Coffee Break			
10:30	**AI/ML & Security I**		**Network, Web & Privacy I**	
	12	Vasisht Duddu, Anudeep Das, Nora Khayata, Hossein Yalame, Thomas Schneider, N. Asokan; **Attesting Distributional Properties of Training Data for Machine Learning**	77	Choongin Lee, Isa Jafarov, Sven Dietrich, Heejo Lee; **PRETT2: Discovering HTTP/2 DoS Vulnerabilities via Protocol Reverse Engineering**
10:50	69	Julien Piet, Maha Alrashed, Chawin Sitawarin, Sizhe Chen, Zeming Wei, Basel Alomair, David Wagner; **Jatmo: Prompt Injection Defense by Task-Specific Finetuning**	118	David Joseph, Carlos Aguilar-Melchor, Douglas Stebila, Jason Goertzen, Adrien Guinet, Thomas Bailleux; **TurboTLS: TLS connection establishment with 1 less round trip**
11:10	32	Bao Gia Doan, Dang Quang Nguyen, Paul Montague, Tamas Abraham, Olivier De Vel, Seyit Camtepe, Salil S. Kanhere, Ehsan Abbasnejad, Damith C. Ranasinghe; **Bayesian Learned Models Can Detect Adversarial Malware For Free**	160	Baiyang Li, Yujia Zhu, Yong Ding, Yong Sun, Yuedong Zhang, Qingyun Liu, Li Guo; **From Fingerprint to Footprint: Characterizing the Dependencies in Encrypted DNS Infrastructures**
11:30	57	Fabio De Gaspari, Dorjan Hitaj, Luigi V. Mancini; **Have You Poisoned My Data? Defending Neural Networks against Data Poisoning**	164	Ning Luo, Chenkai Weng, Jaspal Singh, Gefei Tan, Mariana Raykova, Ruzica Piskac; **Privacy-Preserving Regular Expression Matching using TNFA**
11:50	504	Yuying Li, Zeyan Liu, Junyi Zhao, Liangqin Ren, Fengjun Li, Jiebo Luo and Bo Luo; **The Adversarial AI-Art: Understanding, Generation, Detection, and Benchmarking**	210	Jeroen Robben, Mathy Vanhoef; **Netfuzzlib: Adding First-Class Fuzzing Support to Network Protocol Implementations**
12:10	Lunch			

13:30	**SW & Systems Security I**		**Crypto I**	
	68	Yangyang Shi, Linan Tian, Liwei Chen, Yanqi Yang, Gang Shi; **Scheduled Execution-based Binary Indirect Call Targets Refinement**	19	Hojune Shin, Jina Choi, Dain Lee, Kyoungok Kim, Younho Lee; **Fully Homomorphic Training and Inference on Binary Decision Tree and Random Forest**
13:50	143	Michal Tereszkowski-Kaminski, Santanu Kumar Dash, Guillermo Suarez-Tangil; **A Study of Malicious Source Code Reuse Among GitHub, StackOverflow and Underground Forums**	65	Feixiang Zhao, Huaxiong Wang, Jian Weng; **Constant-Size Unbounded Multi-Hop Fully Homomorphic Proxy Re-Encryption from Lattices**
14:10	150	Yu Luo, Weifeng Xu, Dianxiang Xu; **Predicting Code Vulnerability Types via Heterogeneous GNN Learning**	72	Zhiwei Li, Jun Xu, Yanli Zou, Lei Hu; **Key Recovery Attack on CRYSTALS-Kyber and Saber KEMs in Key Reuse Scenario**
14:30	162	Shangtong Cao, Ningyu He, Yao Guo, Haoyu Wang; **WASMixer: Binary Obfuscation for WebAssembly**	208	Yuxi Xue, Xingye Lu,Man Ho Au and Chengru Zhang; **Efficient Linkable Ring Signatures: New Framework and Post-Quantum Instantiations**
14:50	169	Pyeongju Ahn, Yeonseok Jang, Seunghoon Woo, Heejo Lee; **BLOOMFUZZ: Unveiling Bluetooth L2CAP Vulnerabilities via State Cluster Fuzzing with Target-Oriented State Machines**	100	Changsong Jiang, Chunxiang Xu, Guomin Yang; **Device-Enhanced Secure Cloud Storage with Keyword Searchable Encryption and Deduplication**
15:10	199	Nanyu Zhong, Yueqi Chen, Yanyan Zou, Xinyu Xing, Jinwei Dong, Bingcheng Xian, Jiaxu Zhao, Menghao Li, Binghong Liu and Wei Huo; **TGRop: Top Gun of Return-Oriented Programming Automation**	128	Luisa Siniscalchi, Ivan Visconti; **Incremental Time-Deniable Signatures**
15:30	Coffee Break			
15:50	**AI/ML & Security II**		**Network, Web & Privacy II**	
	205	Xianlong Wang, Shengshan Hu, Peng Xu, Wei Liu, Leo Yu Zhang, Minghui Li, Yanjun Zhang; **PointAPA: Towards Availability Poisoning Attacks in 3D Point Clouds**	252	Rui Lian, Yulong Ming, Chengjun Cai, Yifeng Zheng, Cong Wang, Xiaohua Jia; **Nemesis: Combating Abusive Information in Encrypted Messaging with Private Reporting**

16:10	299	Xianlong Wang, Shengshan Hu, Yechao Zhang, Ziqi Zhou, Leo Yu Zhang, Peng Xu, Wei Wan, Hai Jin; **ECLIPSE: Expunging Clean-label Indiscriminate Poisons via Sparse Diffusion Purification**	258	Junlin He, Lingguang Lei, Yuewu Wang, Pingjian Wang, Jiwu Jing; **ARPSSO: An OIDC-Compatible Privacy-Preserving SSO Scheme based on RP Anonymization**
16:30	301	Omar Ibrahim, Roberto Di Pietro; **MAG-JAM: Jamming Detection via Magnetic Emissions**	281	Md Mushfekur Rahman, Philip W.L. Fong; **Social Control and Interactivity in Anonymous Public Events**
16:50	308	Hamid Mozaffari, Sunav Choudhary; **Fake or Compromised? Making Sense of Malicious Clients in Federated Learning**	286	Yukun Yan, Peng Tang, Rui Chen, Qilong Han, Ruochen Du; **DPC: Filtering out Patch-based Poisoned Samples with Differential Privacy**
17:10	315	Sonakshi Garg, Vicenc Torra; **Task-Specific Knowledge Distillation with Differential Privacy in LLMs**	298	Jiaxuan Fu, Ke Cheng, Yuheng Xia, Anxiao Song, Qianxing Li, Yulong Shen; **Private Decision Tree Evaluation with Malicious Security via Function Secret Sharing**
17:30	End of Day 1			
19:30	Welcome Reception (City Centre)			

TUESDAY, 17.09.2024				
Time	**ID**	**Presentation**	**ID**	**Presentation**
09:10	Keynote: **Prof. Dr hab. Inż. Wojciech Mazurczyk**			
10:10	Coffee Break			
	AI/ML & Security III		**Network, Web & Privacy III**	
10:30	316	Yulian Sun, Li Duan, Ricardo Mendes, Derui Zhu, Yue Xia, Yong Li and Asja Fischer; **Exploiting Internal Randomness for Privacy in Vertical Federated Learning**	297	Jieyu Zheng, Haoliang Zhu, Yifan Dong, Zhenyu Song, Zhenhao Zhang, Yafang Yang and Yunlei Zhao; **Faster Post-Quantum TLS 1.3 Based on ML-KEM: Implementation and Assessment**
10:50	326	Ubaid Ullah, Sonia Laudanna, Vinod P, Andrea Di Sorbo, Corrado Aaron Visaggio and Gerardo Canfora; **Beyond Words: Stylometric Analysis for Detecting AI Manipulation on Social Media**	304	Keyang Liu, Xingxin Li and Tsuyoshi Takagi; **Review the Cuckoo Hash-based Unbalanced Private Set Union: Leakage, Fix, and Optimization**

11:10	341	Peng Yang, Zoe Lin Jiang, Jiehang Zhuang, Junbin Fang, Siu-Ming Yiu and Xuan Wang; **FSSiBNN: FSS-based Secure Binarized Neural Network Inference with Free Bitwidth Conversion**	307	David Eklund, Alfonso Iacovazzi, Han Wang, Apostolos Pyrgelis and Shahid Raza; **BMI: Bounded Mutual Information for Efficient Privacy-Preserving Feature Selection**
11:30	421	Yuejun Guo, Constantinos Patsakis, Qiang Hu, Qiang Tang and Fran Casino; **Outside the Comfort Zone: Analysing LLM Capabilities in Software Vulnerability Detection**	325	Veronique Cortier, Alexandre Debant and Florian Moser; **Code voting: when simplicity meets security**
11:50	475	M. Caner Tol and Berk Sunar; **ZeroLeak: Automated Side-Channel Patching in Source Code Using LLMs**	363	Yu Chen, Lin Liu, Rongmao Chen, Shaojing Fu, Yuexiang Yang, Jiangyong Shi and Liangzhong He; **Speedy Privacy-Preserving Skyline Queries on Outsourced Data**
12:10	Lunch			
13:30	**HW & Cloud Security I**		**Crypto II**	
	95	Prashanthi Mallojula, Fengjun Li, Xiaojiang Du and Bo Luo; **Companion Apps or Backdoors? On the Security of Automotive Companion Apps**	93	Li-Chang Lai, Jiaxiang Liu, Xiaomu Shi, Ming-Hsien Tsai, Bow-Yaw Wang, Bo-Yin Yang; **Automatic Verification of Cryptographic Block Function Implementations with Logical Equivalence Checking**
13:50	115	Weijie Chen, Yu Zhao, Yinqian Zhang, Weizhong Qiang, Deqing Zou and Hai Jin; **ReminISCence: Trusted Monitoring Against Privileged Preemption Side-channel Attacks**	283	Xiangyu Hui and Sid Chi-Kin Chau; **LLRing: Logarithmic Linkable Ring Signatures with Transparent Setup**
14:10	126	Lola-Baie Mallordy, Léo Robert, Pascal Lafourcade and Charles Olivier-Anclin; **Secure Keyless Multi-Party Storage Scheme**	496	Huseyin Gokay, Foteini Baldimtsi and Giuseppe Ateniese; **Atomic Swap Protocol for Boneh–Lynn–Shacham (BLS) based Blockchains**
14:30	192	Volodymyr Bezsmertnyi, Jean-Michel Cioranesco and Thomas Eisenbarth; **Duplication-Based Fault Tolerance for RISC-V Embedded Software**	509	Seoyeon Hwang, Stanislaw Jarecki, Zane Karl, Elina van Kempen and Gene Tsudik; **PIVA: Privacy-Preserving Identity Verification Methods for Accountless Users via Private List Intersection and Variants**

14:50	273	Yihao Luo, Yunjie Deng, Jingquan Ge, Zhenyu Ning and Fengwei Zhang; **BootRIST: Detecting and Isolating Mercurial Cores at the Booting Stage**	528	Bhuvnesh Chaturvedi, Anirban Chakraborty, Ayantika Chatterjee and Debdeep Mukhopadhyay; **"Ask and Thou Shall Receive": Reaction-based Full Key Recovery Attacks on FHE**
15:10	503	Wenxuan Wu, Soamar Homsi, Yupeng Zhang; **Confidential and Verifiable Machine Learning Delegations on the Cloud**	533	Jiuheng Su, Zhili Chen, Haifeng Qian and Junqing Gong; **Efficient and Scalable Circuit-based Protocol for Multi-Party Private Set Intersection**
15:30	End of Day 2			
17:00	Gniew Castle Tour Gala Dinner			

WEDNESDAY 18.09.2024				
Time	**ID**	**Presentation**	**ID**	**Presentation**
	AI/ML & Security IV		**Attacks & Defense I**	
10:30	534	Emad Efatinasab, Alessandro Brighente, Mirco Rampazzo, Nahal Azadi and Mauro Conti; **GAN-GRID: A Novel Adversarial Attack on Smart Grid Stability Prediction**	336	Swantje Lange, Francesco Gringoli, Matthias Hollick and Jiska Classen; **Wherever I May Roam: Stealthy Interception and Injection Attacks through Roaming Agreements**
10:50	508	Diksha Goel, Kristen Moore, Mingyu Guo, Derui Wang, Minjune Kim and Seyit Camtepe; **Optimizing Cyber Defense in Dynamic Active Directories through Reinforcement Learning**	53	Kamil Malinka, Anton Firc, Petr Kaška, Tomáš Lapšanský, Oskar Šandor and Ivan Homoliak; **Resilience of Voice Assistants to Synthetic Speech**
11:10	515	Kane Walter, Surya Nepal and Salil Kanhere; **Exploiting Layerwise Feature Representation Similarity For Backdoor Defence in Federated Learning**	157	Lucien K. L. Ng, Panagiotis Chatzigiannis, Duc V. Le, Mohsen Minaei, Ranjit Kumaresan and Mahdi Zamani; **Cumulus: A Plug-and-Play Long Range Defense System for Proof of Stake Blockchains**
11:30	531	Heewon Baek, Minwook Lee and Hyoungshick Kim; **CryptoLLM: Harnessing the Power of LLMs to Detect Cryptographic API Misuse**	167	Zhiqiang Hao, Chuanyi Li, Xiao Fu, Bin Luo and Xiaojiang Du; **Leveraging Hierarchies: HMCAT for Efficiently**

				Mapping CTI to Attack Techniques
11:50			193	Björn Ho, Huanhuan Chen, Zeshun Shi and Kaitai Liang; **Similar Data is Powerful: Enhancing Inference Attacks on SSE with Volume Leakages**
12:10	Lunch			
13:30	**Network, Web & Privacy IV**		**Attacks & Defense II**	
	396	Daniel De Pascale, Giuseppe Cascavilla, Damian Tamburri and Willem-Jan Van Den Heuvel; **CRATOR a CRAwler for TOR: Turning Dark Web Pages Into Open Source INTelligence**	207	Yifan Wu, Yinshuai Li, Hong Zhu and Yinqian Zhang; **SAEG: Stateful Automatic Exploit Generation**
13:50	404	Maximilian Radoy, Sven Hebrok and Juraj Somorovsky; **In Search of Partitioning Oracle Attacks Against TLS Session Tickets**	274	Shang Shang, Zhongjiang Yao, Yepeng Yao, Liya Su, Zijing Fan, Xiaodan Zhang and Zhengwei Jiang; **IntentObfuscator: A Jailbreaking Method via Confusing LLM with Prompts**
14:10	455	Mirco Beltrame, Mauro Conti, Pierpaolo Guglielmin, Francesco Marchiori and Gabriele Orazi; **RedactBuster: Entity Type Recognition from Redacted Documents**	292	Nan Hu, Hua Wu, Hangyu Zhao, Shanshan Ni and Guang Cheng; **Breaking Through the Diversity: Encrypted Video Identification Attack Based on QUIC Features**
14:30	462	Hongbo Xu, Zhenyu Cheng, Shuhao Li, Chenxu Wang, Peishuai Sun, Jiang Xie and Qingyun Liu; **ProxyKiller: An Anonymous Proxy Traffic Attack Model Based on Traffic Behavior Graphs**	324	Jiahao Wu, Heng Pan, Penglai Cui, Yiwen Huang, Jianer Zhou, Peng He, Yanbiao Li, Zhenyu Li and Gaogang Xie; **Patronum: In-network Volumetric DDoS Detection and Mitigation with Programmable Switches**
14:50	510	Radu-Alexandru Mantu, Mihai Chiroiu and Costin Raiciu; **Process identity based firewalling**	10	Jan Philip Thoma, Florian Stolz and Tim Güneysu; **CIPS: The Cache Intrusion Prevention System**
15:10	Coffee Break			
15:30	**HW & Cloud Security II** **SW & Systems Security II** **Crypto III**		**Attacks & Defense III**	
	382	Fei Hongming, Prosanta Gope, Owen Millwood, Biplab Sikdar;	349	Alessandro Palma, Marco Angelini; **It Is Time To Steer: A Scalable Framework for**

		Optimal Machine-Learning Attacks on Hybrid PUFs		**Analysis-driven Attack Graph Generation**
15:50	338	Jean-Loup Hatchikian-Houdot, Pierre Wilke, Frédéric Besson and Guillaume Hiet; **Formal Hardware/Software Models for Cache Locking Enabling Fast and Secure Code**	389	Vincent Gramoli, Zhenliang Lu, Qiang Tang, Pouriya Zarbafian; **Resilience to Chain-Quality Attacks in Fair Separability**
16:10	433	Xinrong Liu, He Wang, Meng Xu, Yuqing Zhang; **SerdeSniffer: Enhancing Java Deserialization Vulnerability Detection with Function Summaries**	460	Youcef Korichi, Sébastien Gambs, Nadia Tawbi, Josée Desharnais; **Leveraging Transformer Architecture for Effective Trajectory-User Linking (TUL) Attack and Its Mitigation**
16:30	507	Qirui Liu, Wenbo Shen, Jinmeng Zhou, Zhuoruo Zhang, Jiayi Hu, Shukai Ni, Kangjie Lu, Rui Chang; **Interp-flow Hijacking: Launching Non-control Data Attack via Hijacking eBPF Interpretation Flow**	465	Yungi Cho, Woorim Han, Miseon Yu, Younghan Lee, Ho Bae, Yunheung Paek; **VFLIP: A Backdoor Defense for Vertical Federated Learning via Identification and Purification**
16:50	546	Junping Wan, Danjie Li, Junbing Fang, Zoe L. Jiang; **LPFHE: Low-complexity Polynomial CNNs for Secure Inference over FHE**	467	Marc-Antoine Faillon, Baptiste Bout, Julien Francq, Christopher Neal, Nora Boulahia-Cuppens, Frédéric Cuppens, Reda Yaich; **How to Better Fit Reinforcement Learning for Pentesting: A New Hierarchical Approach**
17:10	549	Tjard Langhout, Huanhuan Chen, Kaitai Liang; **File-Injection Attacks on Searchable Encryption, Based on Binomial Structures**	491	Alpesh Bhudia, Dan O'Keeffe, Darren Hurley-Smith; **Revoke: Mitigating Ransomware Attacks against Ethereum Validators**
17:30	Conference Ending End of Day 3			

THURSDAY 19.09.2024			
Time	**Workshop Sessions**		
09:00	**DPM 2024 - International Workshop on Data Privacy Management**	**CPS4CIP - The 5th International Workshop on Cyber-Physical Security for Critical**	**CBT - Cryptocurrencies and Blockchain Technology**

		Infrastructures Protection	
10:30	Coffee Break		
10:45	**DPM 2024 - International Workshop on Data Privacy Management**	**DisA - Computational methods for emerging problems in disinformation analysis**	**CBT - Cryptocurrencies and Blockchain Technology**
12:15	Lunch		
13:45	**DPM 2024 - International Workshop on Data Privacy Management**	**DisA - Computational methods for emerging problems in disinformation analysis**	**CBT - Cryptocurrencies and Blockchain Technology**
15:15	Coffee Break		
15:30	**DPM 2024 - International Workshop on Data Privacy Management**	**SECAI - Workshop on Security and Artificial Intelligence**	**CBT - Cryptocurrencies and Blockchain Technology**
17:30	Ice Breaker Social Event		

FRIDAY 20.09.2024				
Time	**Workshop Sessions**			
09:00	**STM - The 20th International Workshop on Security and Trust Management**	**SECAI - Workshop on Security and Artificial Intelligence**	**CyberICPS - 10th Workshop On The Security Of Industrial Control Systems & Of Cyber-Physical Systems**	**SecAssure - System Security Assurance**
10:30	Coffee Break			
10:45	**STM - The 20th International Workshop on Security and Trust Management**	**SECAI - Workshop on Security and Artificial Intelligence**	**CyberICPS - 10th Workshop On The Security Of**	**SecAssure - System Security Assurance**

			Industrial Control Systems & Of Cyber-Physical Systems	
12:15	Lunch			
13:45	**STM - The 20th International Workshop on Security and Trust Management**	**SECAI - Workshop on Security and Artificial Intelligence**	**CyberICPS - 10th Workshop On The Security Of Industrial Control Systems & Of Cyber-Physical Systems**	**SecAssure - System Security Assurance**
15:15	Coffee Break			
15:30	**STM - The 20th International Workshop on Security and Trust Management**	**SECAI - Workshop on Security and Artificial Intelligence**	**CyberICPS - 10th Workshop On The Security Of Industrial Control Systems & Of Cyber-Physical Systems**	**SecAssure - System Security Assurance**
17:30	End of Workshop Sessions			

Keynote Talks

Cryptographic Applications of the ANS Compression

Speaker: Josef Pieprzyk
Affiliations: Institute of Computer Science,
Polish Academy of Sciences,
Warsaw, Poland
and Data61, CSIRO,
Sydney, Australia
Date: Monday, 16.09.2024, 9:10 AM, Auditorium Novum

Abstract: The talk explores possible applications of ANS in Cryptography. It presents the ANS algorithms and their properties that can be useful for security sensitive applications. The ANS with randomised states can be seen as the basic cryptographic tool that can be used to convert uniformly random sequences into an arbitrary probability distribution calibrated by appropriate selection of symbol spreads. The talk presents two generic joint compression and encryption (also called compcrypt). The first uses the sponge structure and the second follows the CBC mode. Security of the compcrypt algorithm is discussed. The main take away is that both the linear and differential analysis become less effective due to fact that the adversary needs to guess lengths of ANS encoding.

Short Biography: Dr Josef Pieprzyk is a Senior Principal Research Scientist at Data61, CSIRO, Sydney, Australia and a Professor at Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland. His main research interest focus is Cryptology and Information Security and includes design and analysis of cryptographic algorithms (such as encryption, hashing and digital signatures), secure multiparty computations, cryptographic protocols, copyright protection, e-commerce, web security and cybercrime prevention. Dr Pieprzyk published 5 books, edited 11 books (conference proceedings), 6 book chapters, and more than 300 papers in refereed journals and refereed international conferences.

Stegomalware: basics, development trends and detection opportunities

Speaker: Wojciech Mazurczyk
Affiliation: Warsaw University of Technology,
Warsaw, Poland
https://dblp.org/pid/91/874.html
http://mazurczyk.com/
Date: Tuesday, 17.09.2024, 9:00 AM, Auditorium Novum

Abstract: Information hiding techniques are currently increasingly utilized by threat actors to elude countermeasures and prevent reversing the attack chain. Such methods are gaining popularity among attackers as they want to cloak their malicious actions from defensive systems and stay undetected for as long as possible. Currently, cybercriminals apply data hiding schemes, for example, to make their communication with the compromised machine stealthily, secretly download additional malicious components/tools, or exfiltrate confidential data. Unfortunately, detection and mitigation of threats taking advantage of information hiding pose many new challenges for digital forensics analysts, academics, law enforcement agencies, and security professionals.

During this keynote talk, the main types of data hiding techniques used by real-life malware (a.k.a. stegomalware) will be presented, and potential future development trends will be highlighted. Moreover, the main challenges that the current countermeasures face will be outlined, and the recent and novel approaches to thwart such threats will be discussed.

Social Events

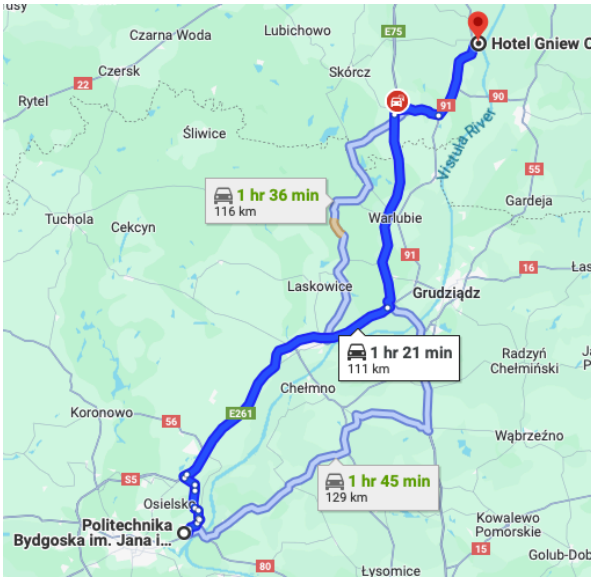
We are excited to offer a series of engaging social events during the conference to provide networking opportunities and a chance to unwind and enjoy the local culture.

Monday, 16 Sep.: Welcome Dinner

Kick off the conference with a delightful Welcome Dinner at Hotel City in Bydgoszcz.

Tuesday, 17 Sep.: Gala Dinner at Gniew Castle

Join us for a Gala Dinner at the historic Gniew Castle.



journey by bus

journey on foot – don't miss the bus

As a reminder, the buses will depart from PBS at 17:00 sharp (5 p.m.). The journey to Gniew Castle will take approximately an hour and a half.

Given the schedule, we kindly request that everyone arrives on time. Unfortunately, the buses will not be able to wait for anyone who is late, as this could delay the entire group. We appreciate your understanding and cooperation in helping us keep the evening running smoothly and on schedule. Your punctuality will allow us all to enjoy the event to the fullest.

Thank you, and we look forward to a memorable evening together!

Expect a night filled with medieval charm and knightly entertainment, returning to Bydgoszcz around midnight.

Thursday, 19 Sep.: Ice Breaker for Workshops

Conclude the week with an Ice Breaker event for workshop participants at the university on Thursday.

Hotels

Here are some hotels you may pick for your stay in Bydgoszcz:

Bohema
*****

ul. Konarskiego 9,
85-066 Bydgoszcz
https://www.booking.com/hotel/pl/hotelbohemabydgoszcz.pl.html

City Hotel
****

ul. 3 Maja 6,
85-016 Bydgoszcz
https://www.booking.com/hotel/pl/city-bydgoszcz.pl.html

Book using the password 'Esorics':

- Single room: 320 PLN
- Double room: 430 PLN

Gross price including breakfast.
Room pool available until June 30, 2024,
afterwards price guarantee is not assured.

Słoneczny Młyn
****

ul. Jagiellońska 96,
85-066 Bydgoszcz
https://www.booking.com/hotel/pl/slonecznymlynbydgoszcz.pl.html

Mercure
****

ul. Focha 20,
85-070 Bydgoszcz
https://www.booking.com/hotel/pl/mercure-bydgoszcz-sepia.pl.html

Holiday Inn
****

ul. Grodzka 36,
85-109 Bydgoszcz
https://www.booking.com/hotel/pl/holiday-inn-bydgoszcz.pl.html

Campanile
***

ul. Jagiellońska 59,
85-027 Bydgoszcz
https://www.booking.com/hotel/pl/campanile-bydgoszcz.pl.html

Practical tips

Here are some practical tips when traveling to Bydgoszcz, Poland from other countries:

Currency Used

The currency in Poland is the Polish Zloty (PLN). While most places accept Visa, Mastercard and Revolut, it's advisable to have some local currency on hand.

Exchanging Money

- **Currency Exchange:** It's advisable to exchange some money to Polish Zloty before you arrive or at the airport, although rates at airports can be less favourable. One of the exchange offices with fair rates and a wide choice of currencies is https://kantorbydgoszcz.com
- **ATMs:** Withdrawals from ATMs (called "bankomat" in Polish) are a convenient way to get Polish Zloty. ATMs are widely available in train stations, airports, and public areas. Be aware of your bank's foreign transaction fees.

Using Credit and Debit Cards

- **Card Acceptance:** Visa and MasterCard are widely accepted in Poland, especially in hotels, restaurants, and larger stores. However, it's less common in small local shops, rural areas, or for street vendors.
- **Transaction Fees:** Check with your card issuer about foreign transaction fees. Some banks charge additional fees for each transaction in a foreign currency.
- **Contactless Payments:** Poland has a high adoption rate for contactless payments, including services like Apple Pay and Google Pay.

Shopping and Business Hours

Shops in Poland are usually open from 10 am to 6 pm on weekdays and have shorter hours on Saturdays. Most stores close on Sundays.

Tipping Practices

Tipping is customary but not mandatory in Poland. It's common to leave a 10% tip in restaurants if the service is good. Tips can be left in cash or added to your card payment.

Local Cuisine

Polish cuisine is hearty and flavourful. Don't miss dishes like pierogi (stuffed dumplings), bigos (hunter's stew), powidła (fried plum jam) and żurek (sour rye soup). Poland also boasts a variety of excellent beers and vodkas.

Weather in September

Temperatures: September marks the transition from summer to autumn in Poland. Early in the month, you can still enjoy relatively warm weather with average daytime temperatures ranging from 14°C to 20°C (57°F to 68°F). However, temperatures can begin to drop towards the end of the month.
Precipitation: Rainfall is moderate but less frequent than in the summer months. It's still wise to carry a light raincoat or an umbrella.
Clothing: Pack layers to accommodate fluctuating temperatures. Include a mix of short-sleeved and long-sleeved shirts, and bring a sweater or light jacket for cooler evenings.

Connectivity

- Free WiFi is usually available in public areas, cafes, and hotels.
- If you wish to buy one of the physical local SIM cards, which are cheap and available everywhere, bear that in mind that you need to visit a provider’s shop to activate it; you’ll also need your ID or passport to do so.
- If your device supports eSIM, consider buying a card for mobile data, as it's quite affordable (e.g. from Airalo – $4.5 USD for 1 GB of data $5.5 USD for 2 GB and so on) and the most hassle-free.

Health and Safety

Tap water is safe to drink in most places, but if you're unsure, bottled water is widely available.

Basic Polish Phrases

In Poland, English proficiency varies. In urban areas and among younger people, you're more likely to find English speakers, particularly at hotels, restaurants, and during professional events like conferences. However, in rural areas and among older populations, fewer people speak English. While you can manage most interactions at a scientific conference and major tourist spots with English, having some basic Polish phrases handy can be beneficial.

Basic Greetings and Polite Expressions

- Dzień dobry (Jen doh-brih): Hello/Good day
- Do widzenia (Doh veed-zen-ya): Goodbye
- Proszę (Proh-sheh): Please
- Dziękuję (Jen-koo-yeh): Thank you
- Tak (Tahk): Yes
- Nie (Nyeh): No
- Przepraszam (Psheh-prah-sham): Excuse me/Sorry
- Proszę bardzo (Proh-sheh bar-zho): You’re welcome

At the Conference

- Konferencja (Kon-fe-ren-tsya): Conference
- Wykład (Vee-kwat): Lecture
- Badania (Bah-dah-nya): Research
- Prezentacja (Preh-zen-tat-sya): Presentation
- Sesja (Ses-ya): Session
- Pytanie (Pee-tah-nyeh): Question
- Odpowiedź (O-dpo-vyench): Answer

Directions and Locations

- Gdzie jest…? (G-jeh yest…?): Where is…?
- Pokój (Po-koy): Room
- Toaleta (Toh-ah-let-ah): Bathroom
- Wyjście (Vee-ysht-cheh): Exit
- Wejście (Vey-ysht-cheh): Entrance
- Winda (Vin-dah): Elevator
- Jak mogę dojść do...? (Yahk mo-ghe doyshch doh...?) - How do I get to...?
- Lewo (Leh-vo) - Left
- Prawo (Prah-vo) - Right
- Prosto (Pro-sto) - Straight ahead
- Wstecz (Vstech) - Back

Dining and Food

- Restauracja (Rest-ow-rat-sya): Restaurant
- Menu (Men-oo): Menu
- Woda (Vo-dah): Water
- Kawa (Kah-vah): Coffee
- Herbata (Her-bah-tah): Tea
- Piwo (Pee-vo): Beer
- Can I have the bill, please?: Czy mogę prosić rachunek? (Chih mo-geh proh-sich rah-hoo-nek?)

Emergency and Health

- Pomocy! (Po-mo-tsi!): Help!
- Lekarz (Leh-karsh): Doctor
- Apteka (Ap-teh-kah): Pharmacy
- Szpital (Shpital): Hospital
- Potrzebuję lekarza (Po-tshe-boo-yeh leh-kar-zah): I need a doctor

At the Airport

- Terminal (Ter-mee-nal) - Terminal
- Odbiór bagażu (Od-byoor bah-gah-zhoo) - Baggage claim
- Stanowisko odprawy (Sta-no-vis-ko od-pra-vy) - Check-in desk
- Kontrola bezpieczeństwa (Kon-tro-la bezh-pe-chen-stva) - Security check
- Karta pokładowa (Kar-ta pok-law-do-va) - Boarding pass

At the Train Station or Bus Station

- Kasa biletowa (Kah-sah bee-le-to-va) - Ticket office
- Peron (Peh-ron) - Platform
- Rozkład (Roz-kwad) - Schedule
- Odjazdy (Od-yaz-dy) - Departures
- Przyjazdy (Pshy-yaz-dy) - Arrivals
- Bilet (Bee-let) - Ticket

Buying Tickets

- Jeden bilet do..., proszę (Ye-den bee-let doh..., pro-sheh) - One ticket to..., please
- Bilet powrotny (Bee-let po-vrot-ny) - Return ticket
- Pierwsza klasa/Druga klasa (Pyer-sha klah-sah/Droo-gah klah-sah) - First class/Second class

Time and Directions

- Kiedy odjeżdża...? (Kye-dy od-yeh-jah?) - When does the... leave?
- Czy to jest właściwa droga do...? (Chi to yest vwah-shchi-va dro-ga doh...?) - Is this the right way to...?
- Ile czasu zajmuje dojście do...? (E-le chah-soo zai-moo-ye doysh-che doh...?) - How long does it take to get to...?

Miscellaneous

- Nie rozumiem (Nyeh ro-zoo-myem): I don’t understand
- Czy mówi Pan/Pani po angielsku? (Chih moo-vee pan/pani po an-gyel-skoo?): Do you speak English?
- Czy możesz mi pomóc? (Chi mo-zhesh mee po-moats?) - Can you help me?
- Zgubiłem się (Zgoo-byehm sh-eh) - I am lost
- Potrzebuję taksówki (Po-tshe-boo-yeh tak-suf-kee) - I need a taxi
- Nigdy nie zrezygnuję z Ciebie (Nee-gdy nye zheh-zig-noo-yeh z cheh-bye) - Never gonna give you up
- Nigdy Cię nie zawiodę (Nee-gdy cheh nye za-vyo-deh) - Never gonna let you down

About Bydgoszcz

The city of Bydgoszcz, located in the heart of the Kuyavian-Pomeranian region, and the Bydgoszcz University of Science and Technology (PBŚ) have been pioneers in cybersecurity and information technology in Poland.

We are excited to bring our expertise and hospitality to host ESORICS 2024, offering a blend of rich history, academic excellence, and modern innovation.

Poland - the IT Backbone of Europe

Poland has the largest tech talent pool in Europe, and is in the TOP3 best-in-class tech talents in the World, TOP3 best Developers in The World ranging by SkillValue, TOP10 TopCoder Country Ranking, and holds the 2nd place in the DDI development IT competitiveness index.
Many of the world's biggest most recognizable names in IT utilise the Poland's immense talent pool: DELL, Lenovo, HP, Intel, Asseco, Samsung, Microsoft, Apple, ASUS, Acer, Comarch, Capgemini, Google, Amazon and many more.

Poland also ranks among the Top 20 in English proficiency (13th place to be exact), consistently ranked in the top 20 since 2015, making it a popular country for outsourcing development.

Unique Security Perspective

Bydgoszcz, and its strategic placement on the banks of the Brda and the Vistula rivers, has a rich history in the defensive industries.

Currently, Bydgoszcz houses, among others, the NATO Joint Force Training Centre (JFTC), NATO Information and Communication Agency CIS Support Unit (NCIA CSU), NATO Force Integration Unit (NFIU), Command of 3rd NATO Signal Battalion and NATO Military Police Centre of Excellence

According to the ABSL report, Bydgoszcz has the largest percentage of personnel working in the IT services in all of Poland. Besides bringing innovations in the defence and cyberdefence sectors, Bydgoszcz is also a renowned academic hub, a lead in cyber-research, and the Bydgoszcz University of Science and Technology has a strong track record in scientific dissemination and international projects.

Enjoy Bydgoszcz!

There is much to see in Bydgoszcz: From the Gothic Cathedral of St. Martin and St. Nicholas to the stunning Art Nouveau details found throughout the city. Explore the charmingly restored Old Town, a canvas of Renaissance and baroque architecture. Don’t miss the Bydgoszcz Canal and its historic waterway structures, which paint a picture of the city's rich industrial past. Engage with modernity at the Exploseum, an offbeat museum dedicated to wartime technology, or marvel at contemporary art installations at the Municipal Art Center. The cityscape of Bydgoszcz blends historical depth with vibrant cultural expressions, making every corner an invitation to explore.

For a comprehensive resource on everything Bydgoszcz has to offer, from local attractions and events to dining and shopping recommendations, be sure to visit the official tourism website of Bydgoszcz at https://visitbydgoszcz.pl/pl/ for up-to-date information to help you make the most of your stay in our city.

To enhance your experience in Bydgoszcz, download the "Bydgoszcz – Mobilny Przewodnik" app (iOS/ Android), the official digital guide to exploring the city. This application offers detailed information on attractions, tours, restaurants, and much more.

Emergency Contacts in Poland

- **112** - The main emergency number for all services. This number can be dialled from any phone, free of charge, to reach ambulance, fire, and police services.
- **997** - Police
- **998** - Fire Brigade
- **999** - Ambulance
- **986** - Municipal Police (for non-life-threatening situations such as noise complaints or minor disturbances)