“Lucian Blaga” University of Sibiu
Computer Science and Electrical Engineering Department

SECURITY ISSUES IN COMPUTER ARCHITECTURE – RESEARCH PROJECT

PhD Candidate: Teodora VASILAS

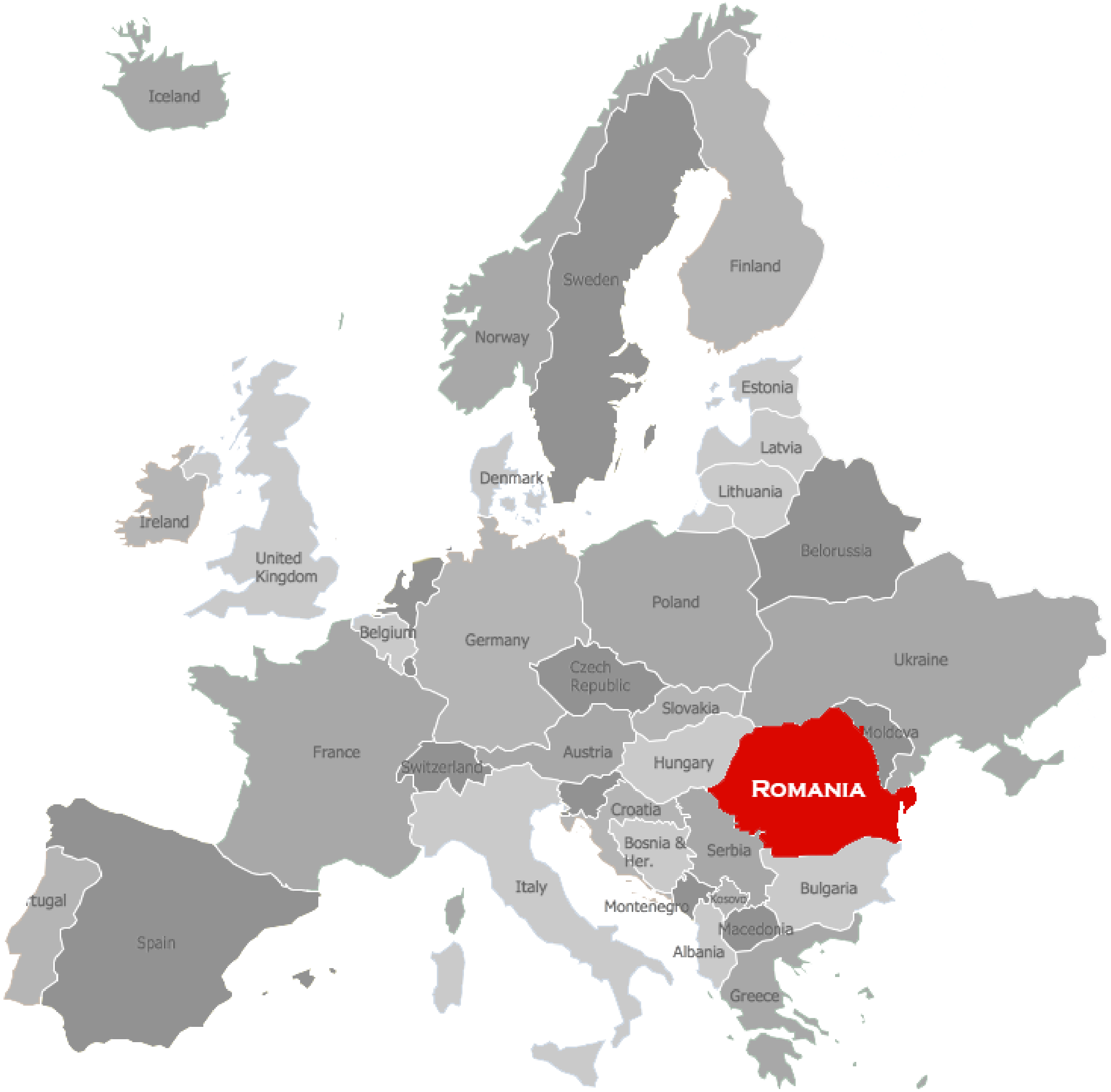
PhD Advisors: Prof. Remus BRAD, Prof. Adrian FLOREA

CONTENTS

- About me & where I come from
- Introduction
- Methodology
- Current state
  - Attacks
  - Countermeasures
- Research ideas
- Next steps

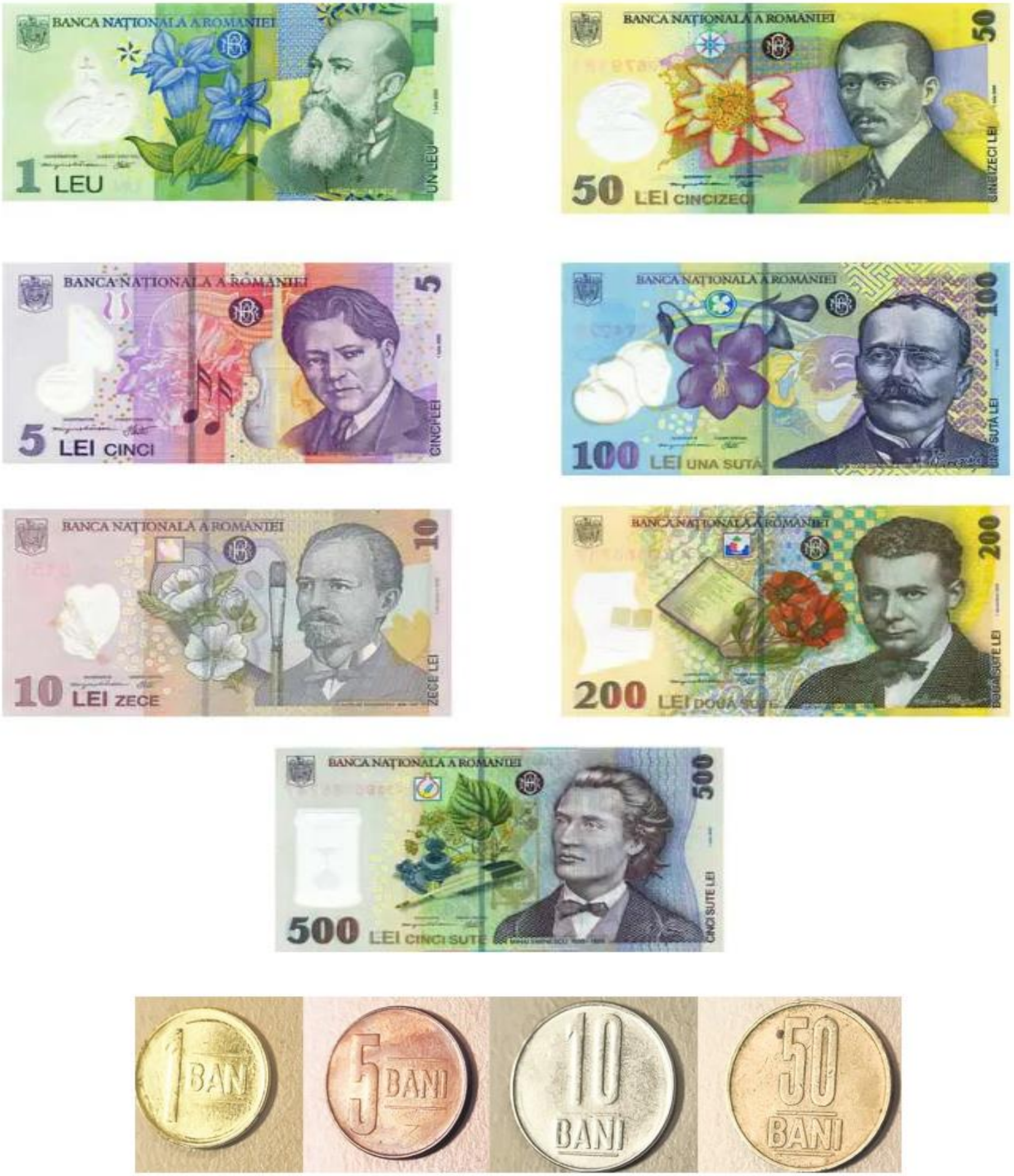
ROMANIA

- Location: Eastern Europe
- Capital: Bucharest
- Population: 19 mil (2022)
- Neighbors:
  - Ukraine (N)
  - Hungary (W)
  - Serbia (S-W)
  - Bulgaria (S)
  - Moldova & Black Sea (E)



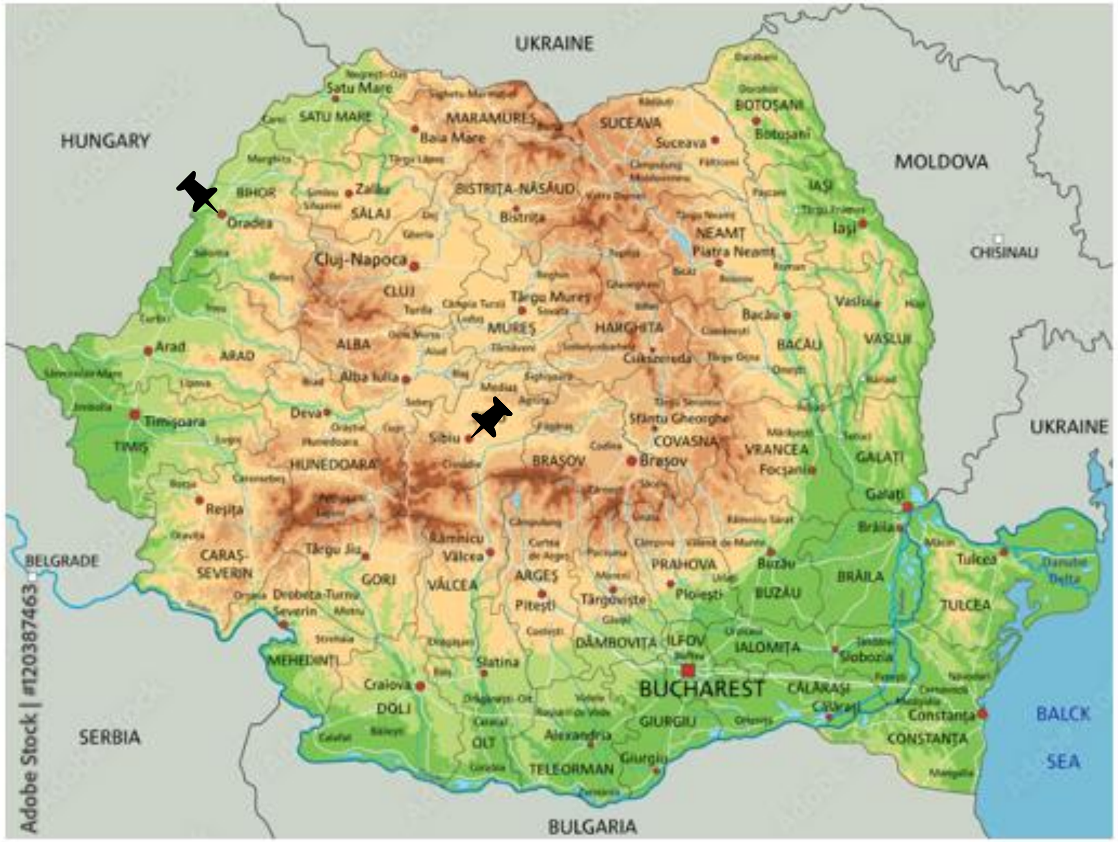
ROMANIA

- Location: Eastern Europe
- Capital: Bucharest
- Population: 19 mil (2022)
- Neighbors:
  - Ukraine (N)
  - Hungary (W)
  - Serbia (S-W)
  - Bulgaria (S)
  - Moldova & Black Sea (E)
- Currency: Romanian LEU
  - 5 LEI ≅ 1 EURO



ROMANIA

- Location: Eastern Europe
- Capital: Bucharest
- Population: 19 mil (2022)
- Neighbors:
  - Ukraine (N)
  - Hungary (W)
  - Serbia (S-W)
  - Bulgaria (S)
  - Moldova & Black Sea (E)
- Currency: Romanian LEU
  - 5 LEI ≅ 1 EURO
- It has mountains, hills, plains, opening to the sea, and a delta



13 FACTS ABOUT ROMANIA

- Sapanta-Peri Monastery - the tallest wooden church in the world (78m/255feet)

13 FACTS ABOUT ROMANIA

- Sapanta-Peri Monastery - the tallest wooden church in the world (78m/255feet)
- The Black Church of Brașov - the biggest Gothic church between Vienna and Istanbul

13 FACTS ABOUT ROMANIA

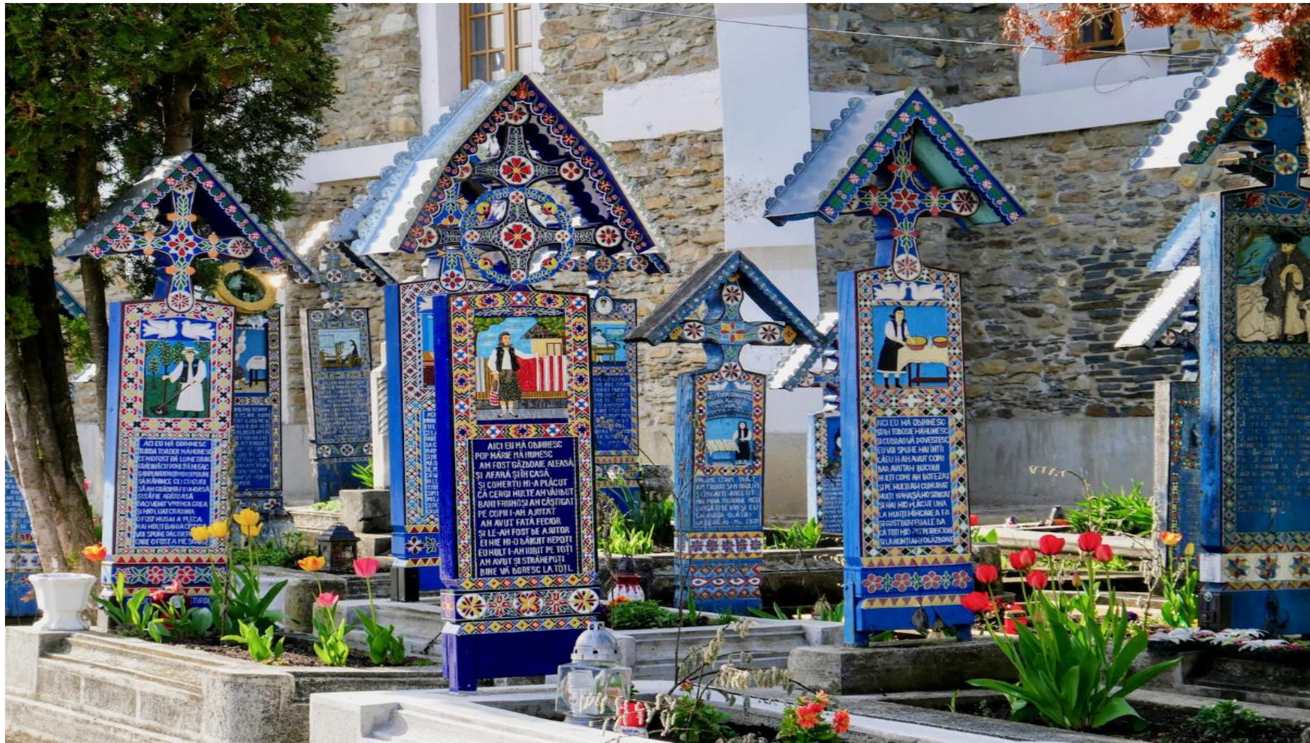
- Sapanta-Peri Monastery - the tallest wooden church in the world (78m/255feet)
- The Black Church of Brașov - the biggest Gothic church between Vienna and Istanbul
- Bigar Waterfall - World Geography’s top of ’Unique Waterfalls Around the World’

13 FACTS ABOUT ROMANIA

- Sapanta-Peri Monastery - the tallest wooden church in the world (78m/255feet)
- The Black Church of Brașov - the biggest Gothic church between Vienna and Istanbul
- Bigar Waterfall - World Geography's top of 'Unique Waterfalls Around the World'
- Transfăgărășan Road - the 'world's best driving road' (declared by Top Gear).
  - Over 151 kilometres (93 miles)
  - Cutting through the Făgăraș Mountains
  - The top is at 2,134 meters (7,000 feet).

13 FACTS ABOUT ROMANIA (2)

- The Merry Cemetery – on the crosses the deceased's message for the living world
  - *Under this heavy cross, lies my poor mother-in-law, if she was alive another three days, I would have been lying here instead of her. You who pass by here try not to wake her up, because if she comes home, she will scold me again. Stay here, my dear mother-in-law.*



13 FACTS ABOUT ROMANIA (2)

- The Merry Cemetery – on the crosses the deceased’s message for the living world
  - *Under this heavy cross, lies my poor mother-in-law, if she was alive another three days, I would have been lying here instead of her. You who pass by here try not to wake her up, because if she comes home, she will scold me again. Stay here, my dear mother-in-law.*
- The Palace of the Parliament – the second biggest administrative building in the world after the Pentagon & the heaviest building in the world (made of marble,4.10 million tones)

13 FACTS ABOUT ROMANIA (2)

- The Merry Cemetery – on the crosses the deceased's message for the living world
  - *Under this heavy cross, lies my poor mother-in-law, if she was alive another three days, I would have been lying here instead of her. You who pass by here try not to wake her up, because if she comes home, she will scold me again. Stay here, my dear mother-in-law.*
- The Palace of the Parliament – the second biggest administrative building in the world after the Pentagon & the heaviest building in the world (made of marble,4.10 million tones)
- Francesco Illy – the creator of the coffee machine was born in Timisoara

13 FACTS ABOUT ROMANIA (3)

- Nadia Comaneci - The first gymnast with a perfect 10, at 1976 Olympic Summer Games, Montreal, Canada

13 FACTS ABOUT ROMANIA (3)

- Nadia Comaneci - The first gymnast with a perfect 10, at 1976 Olympic Summer Games, Montreal, Canada
- The 7th fastest internet speed in the world with a peak of 58.7 Mbps

13 FACTS ABOUT ROMANIA (3)

- Nadia Comaneci - The first gymnast with a perfect 10, at 1976 Olympic Summer Games, Montreal, Canada
- The 7th fastest internet speed in the world with a peak of 58.7 Mbps
- Peles Castel – the first castle entirely lit by electrical current in Europe

13 FACTS ABOUT ROMANIA (3)

- Nadia Comaneci - The first gymnast with a perfect 10, at 1976 Olympic Summer Games, Montreal, Canada
- The 7th fastest internet speed in the world with a peak of 58.7 Mbps
- Peles Castel – the first castle entirely lit by electrical current in Europe
- Timisoara - the first city with electric street lamps

13 FACTS ABOUT ROMANIA (3)

- Nadia Comaneci - The first gymnast with a perfect 10, at 1976 Olympic Summer Games, Montreal, Canada
- The 7th fastest internet speed in the world with a peak of 58.7 Mbps
- Peles Castel – the first castle entirely lit by electrical current in Europe
- Timisoara - the first city with electric street lamps
- Danube delta – second biggest in Europe & the best preserved delta

13 FACTS ABOUT ROMANIA (3)

- Nadia Comaneci - The first gymnast with a perfect 10, at 1976 Olympic Summer Games, Montreal, Canada
- The 7th fastest internet speed in the world with a peak of 58.7 Mbps
- Peles Castel – the first castle entirely lit by electrical current in Europe
- Timisoara - the first city with electric street lamps
- Danube delta – second biggest in Europe & the best preserved delta
- Bran Castle – known as castle of Dracula, but Count Vlad Tepes (which inspired the Dracula character) didn't actually live there

CITY OF SIBIU/HERMANNSTADT

- Middle size historical city
- Population: 170,000
- European capital of culture in 2007, together with Luxembourg

CITY OF SIBIU/HERMANNSTADT

- Middle size historical city
- Population: 170,000
- European capital of culture in 2007, together with Luxembourg
- "ASTRA" National Museum of Ethnography, Civilization and Folk Arts – 3 Michelin stars

ABOUT ME

- **Practiced Speed Skating during Primary School and High School (~10 years)**
- **Like to read and travel**

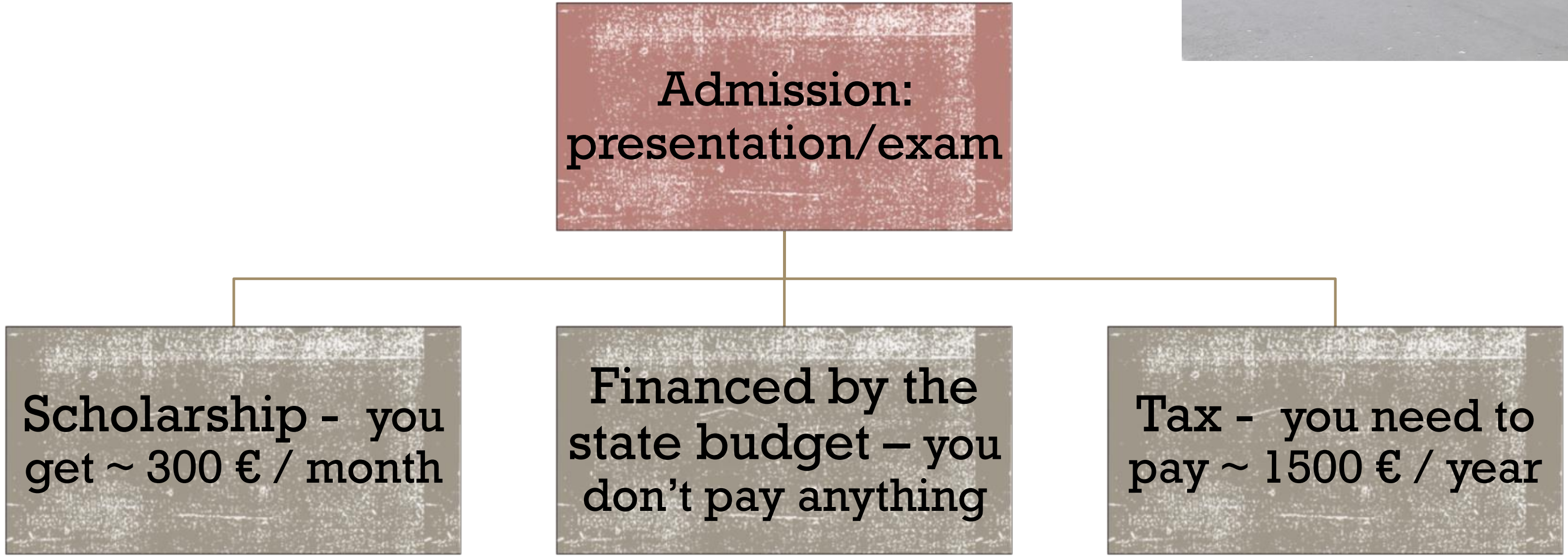
- BSc - Computer Science, Faculty of Engineering, ULBS (2014-2018)
- MSc – Advanced Computing Systems, Faculty of Engineering, ULBS (2018-2020)
- PhD Candidate – Security Issues on Computer Architecture, ULBS (2020-present)
- Software Validation Engineer on Network Devices at Continental (2016-present)

Prof Lucian VINTAN
Dynamic Neural
Branch Prediction
(IJCNN '99, Washington
DC)

- Teaching Assistant (Labs, Projects, Grading) – prof. Adrian FLOREA
  - Simulation and Optimization of Computing Architectures (different types of caches and predictors)
  - Embedded Systems (VEX simulator - Linux)
  - Microprocessors Systems (MIPS & DLX Assembly)

- PhD Coordinator – prof. Remus BRAD

FACULTY OF ENGINEERING & PHD PROGRAMS


Admission: presentation/exam

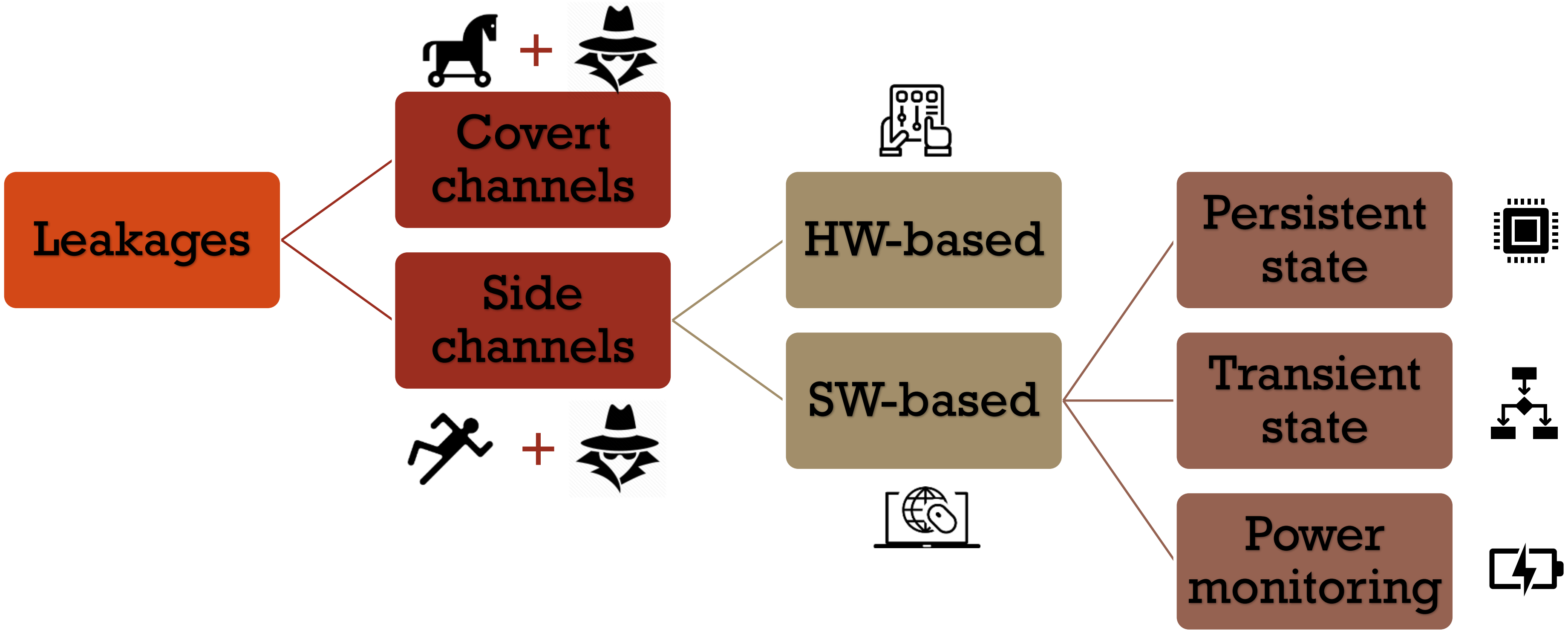
Scholarship - you get ~ 300 € / month

Financed by the state budget – you don't pay anything

Tax - you need to pay ~ 1500 € / year

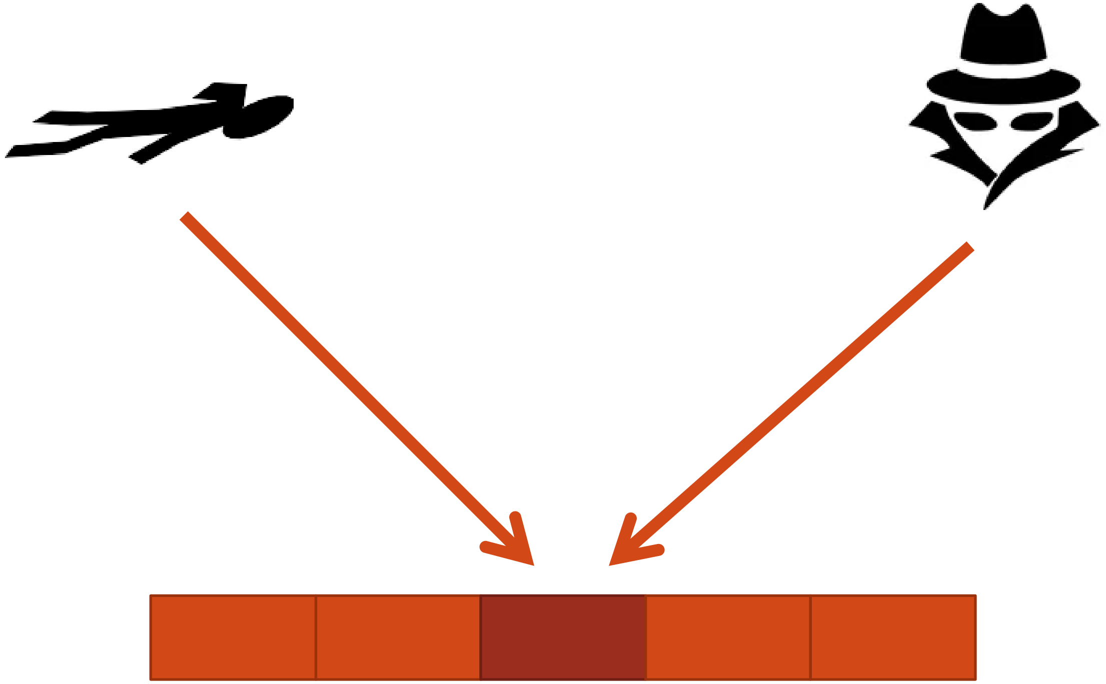
INTRODUCTION

- The movement to the virtual space, apart from the huge benefits, comes with the unwanted threats too



METHODOLOGY

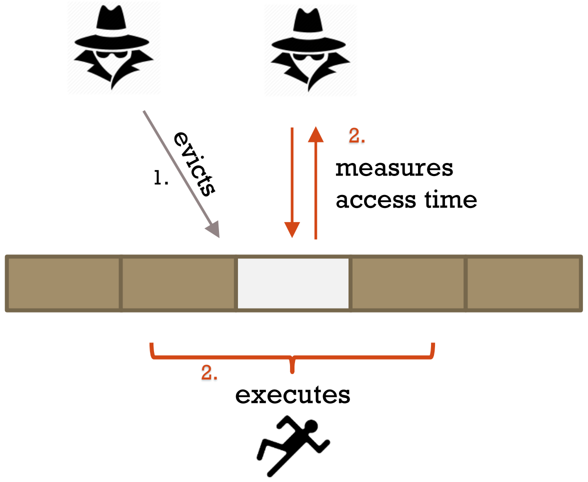
- The attack techniques run in spy processes, and they target the cryptographic algorithms which are running as victim processes.

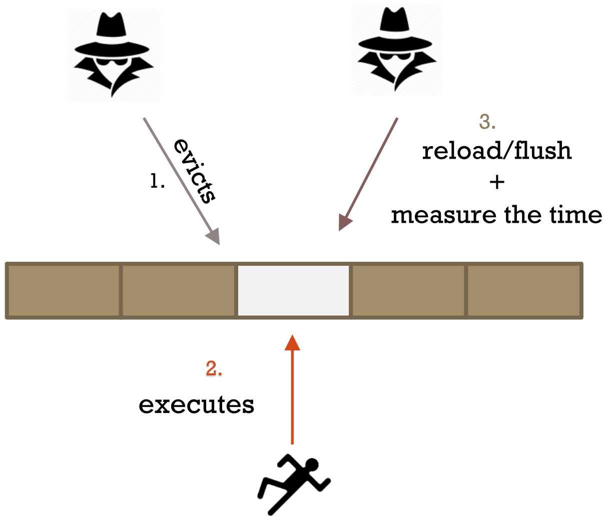


- Cryptographic algorithms:
  - AES
  - RSA
  - ECDSA
  - ElGamal

PERSISTENT STATE CHANNELS - CACHE

- Timing-based attacks - the attacker is analyzing the **time** taken to execute cryptographic algorithm
  - Evict&Time



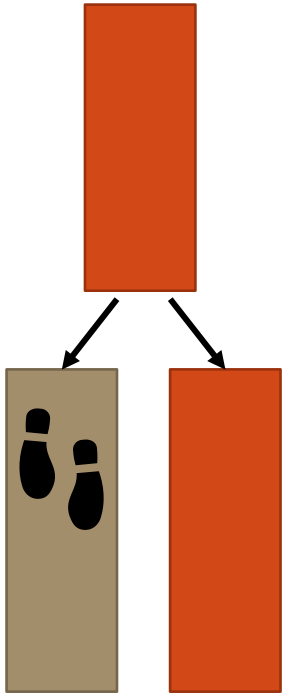


- Access-based attacks - the attacker is monitoring the **accesses** done by the victim to execute cryptographic algorithm
  - Flush&Reload
  - Flush&Flush
  - Evict&Reload
  - Prime&Probe
  - Prime&Abort

Current State

TRANSIENT STATE CHANNELS

- Appear due to the high parallelism in the modern CPUs which execute instructions in an **out-of-order** way, or before their turn in the program.
- The predictor can be trained to misspsculate
- The microarchitectural state won't be cleared of data in case of a wrong speculation.
- A series of very well known "speculation" attacks are Spectre, Meltdown and their variations.



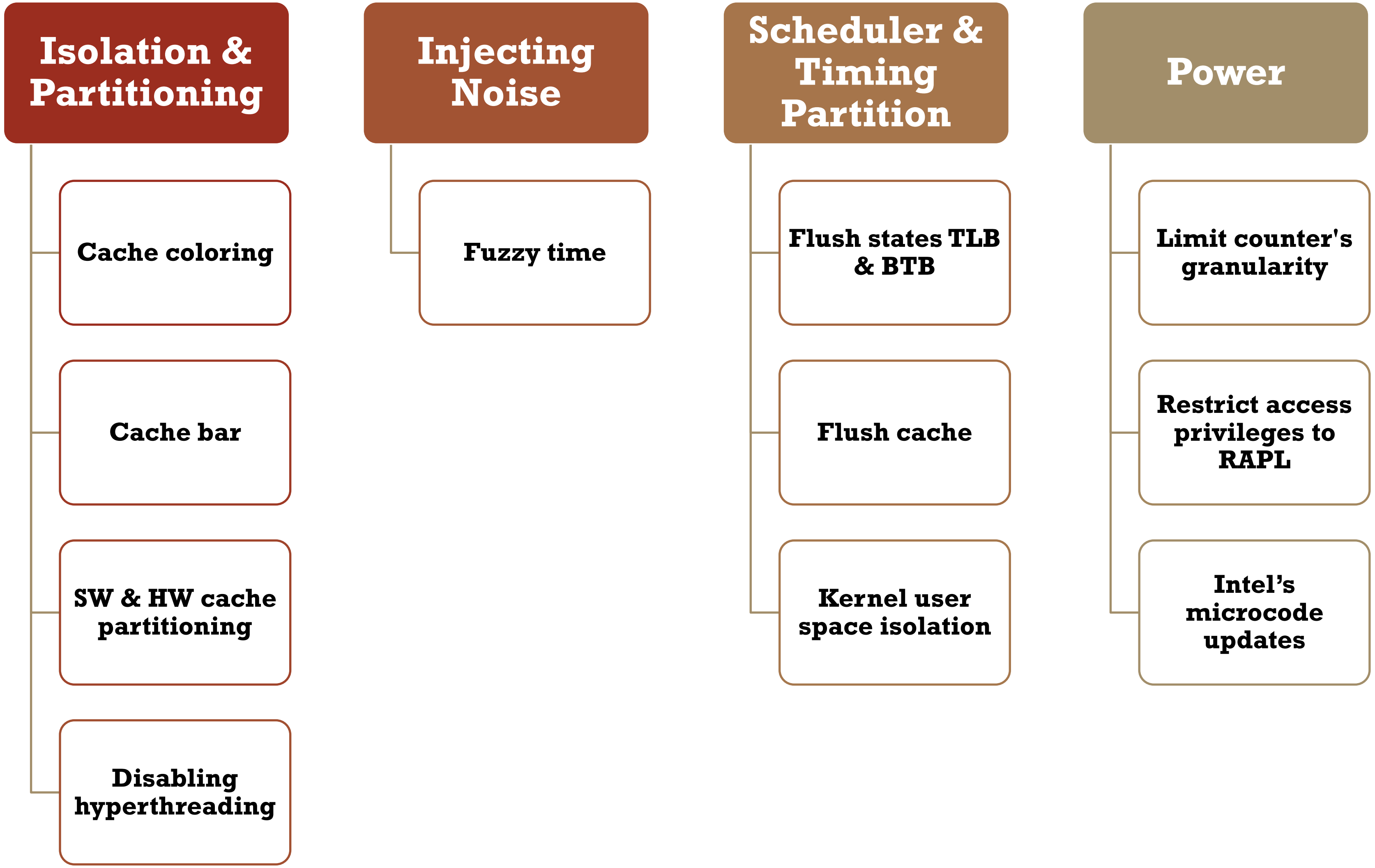
```
if(x < arrayLength)
{
    i = array[x];
    y = array2[i*256];
}
```

Current State

POWER MONITORING

- The power side-channel attacks analyze the variations of the power consumption of a device to extract secret data, without physical accessing the targeted system.
- Platypus attacks use the Intel RAPL system to gain information about the power consumption of the system and based on some analysis **each kind of instruction can be distinguished**.
- ThermalBleed is using the *hwmon* interface in Linux that can read the temperature sensor for each core to **break the KASLR** (Kernel Address Space Layout Randomization)

DETECTION & COUNTERMEASURES



Isolation & Partitioning

- Cache coloring
- Cache bar
- SW & HW cache partitioning
- Disabling hyperthreading

Injecting Noise

- Fuzzy time

Scheduler & Timing Partition

- Flush states TLB & BTB
- Flush cache
- Kernel user space isolation

Power

- Limit counter's granularity
- Restrict access privileges to RAPL
- Intel's microcode updates

RESEARCH IDEAS

- **Combine the idea from Persistent State channels with Power monitoring channels**
- In ThermalBleed they didn’t explore the cache, using the following affirmation:
  - Thermal difference appears when the cache is accessed (higher temp) and when the main memory is accessed (lower temp)
- Same as in Flush+Reload attack, instead of reading the time of the reloading data in cache after the victim executes, we can measure the temperature to see if there was a cache hit or not

NEXT STEPS/OBJECTIVES

- The collecting app which measures the temperature - done
- The target app which makes the encryptions (RSA algorithm) - in work
- Distinguish between cache and main memory accesses –> reproduce
- Apply the distinguish technique on the encryptions
- Recover the encryption key

REFERENCES

- M. Mushtaq, M. A. Mukhtar, et al., "Winter is here! A decade of cache-based sidechannel attacks, detection & mitigation for RSA", in Information Systems, 92, 2020.
- Q. Ge, Y. Yarom, D. Cock, et al. "A survey of microarchitectural timing attacks and countermeasures on contemporary hardware", J Cryptogr Eng 8, 1–27 (2018).
- A. Fuchs, R. B. Lee, "Disruptive Prefetching: Impact on Side-Channel Attacks and Cache Designs", in 8th ACM International Systems and Storage Conference, 2015.
- P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, et al., "Spectre Attacks: Exploiting Speculative Execution", San Francisco, CA, USA, 2019.
- M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, S. Mangard, P. Kocher, D. Genkin, Y. Yarom and M. Hamburg, "Meltdown," in arXiv preprint arXiv:1801.01207, 2018.
- M. Lipp, A. Kogler, et al. "PLATYPUS: Software-based Power Side-Channel Attacks on x86" in IEEE Symposium on Security and Privacy, San Francisco, CA, 2021.
- T. Kim; Y. Shin, "ThermalBleed: A Practical Thermal Side-Channel Attack", in IEEE Access (volume 10), p 25718 – 25731, 2022

THANK YOU!