Security-first Heterogeneous Architecture for AI-chip

Jing Li

lixeon.lij@gmail.com

Dec. 30, 2020

Huairou, Beijing

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

Outline

I. Background & Basic

II. Problem Statement

III. Solve idea

Which ones are chips?

Wireless Headphones

Smart Watch

Phone SoC

LCD Monitor

Solid State Disk

But also semiconductor

Hard Disk Drive

Memory

Laptop CPU

Flash Disk

Game Host

Magnetic

What is Computer Security (aka InfoSec)?

- **Safe**
  - Natural property
  - Resist natural disasters
  - Non-human attack
  - uncertainty

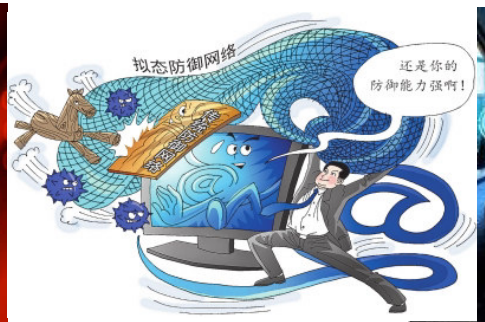
- **Security**
  - Man-made
  - against deliberate attacks
  - Strong certainty

InfoSec means Computer Security

The goal is CIAA

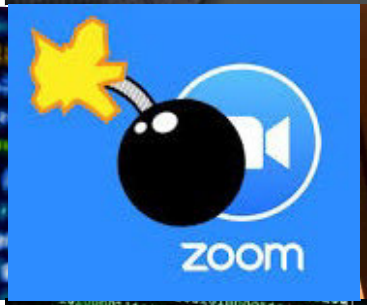
(Confidentiality Integrity Availability Authenticity)

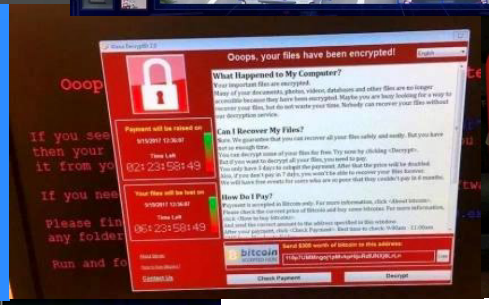
Cyber attacks threaten system security even national security

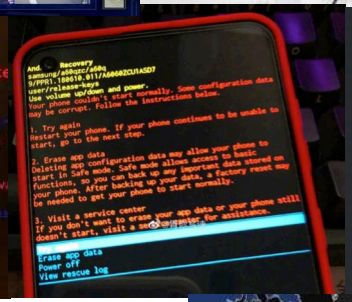



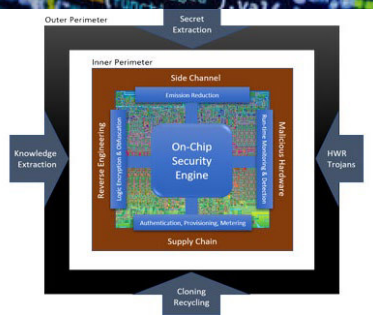


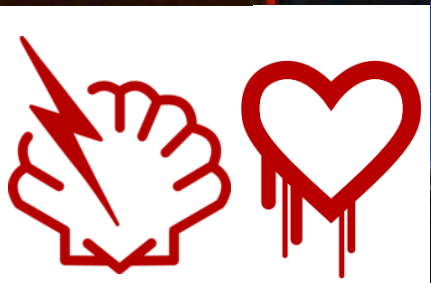








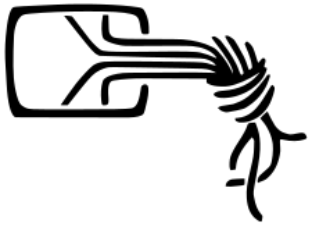






Offense and Defense is a GAME


DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

公安部第三研究所
The Third Research Institute Of Ministry Of Public Security
EUROPOL EC3 European Cybercrime Centre



中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

HERJAVEC GROUP



CYBERARK


Worse in Chip (or Micro Architecture)

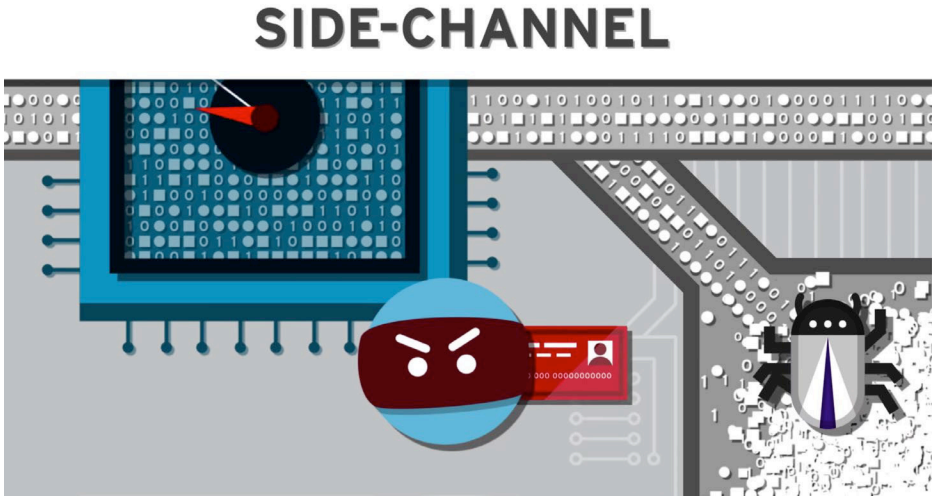
Spectre
v1, v2, v4, v5,
Spectre-BTB,
Spectre-RSB,
ret2spec,
SGXPectre,
SmotherSpectre,
NetSpectre?

Meltdown
v3, v3.1, v3a,
RDCL?

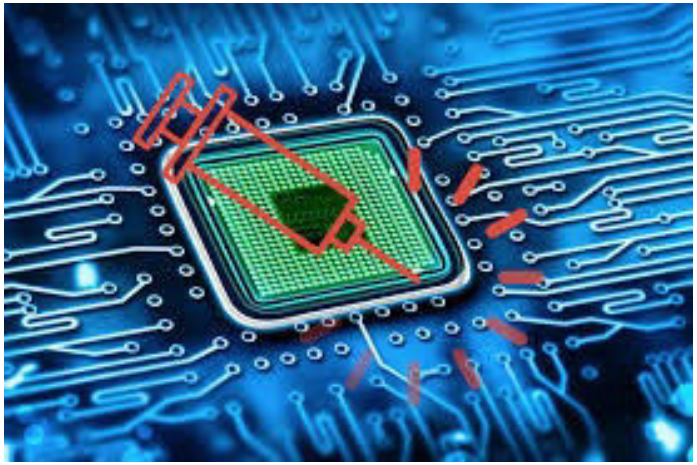
ZombieLoad, MDS?

Foreshadow
Foreshadow-NG,
L1TF?

RIDL, Fallout?



Affected almost ALL CHIPS after 1995



Worse in AI

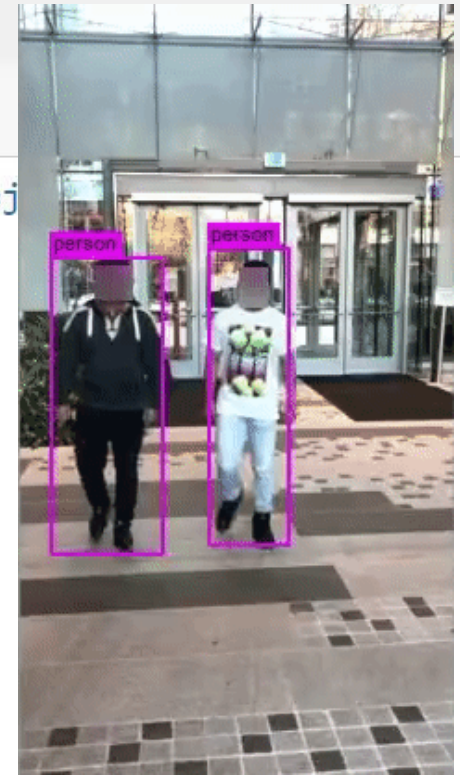
CASE 1:

```
img = PILImage.create(img_c)
img.to_thumb(192)
```

```
https://pbs.twimg.com/media/EqW4Xi1U8AA_KzH?format=j
```

Out[50]:

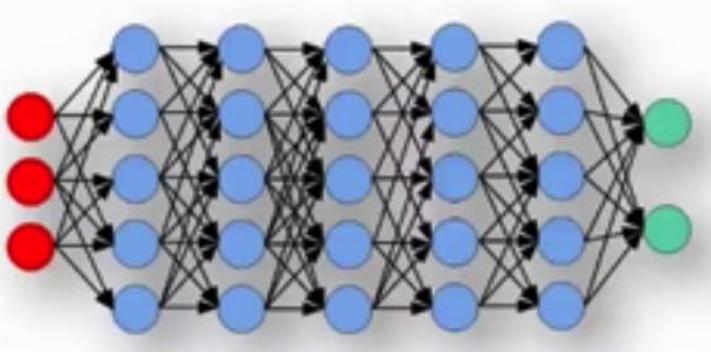
CASE 2:

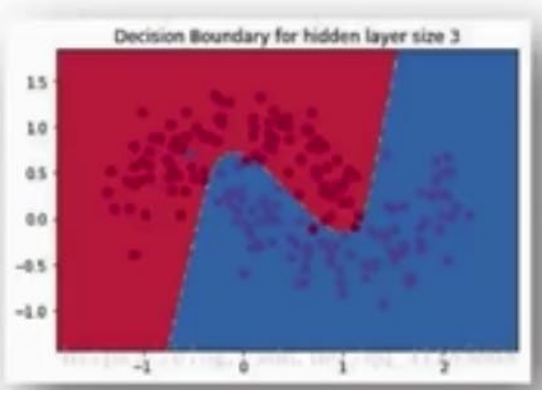



```
Is this a boy?: True.
Probability it's a boy: 98.66%
Probability it's a girl: 1.34%
Time cost: 323ms
```

Stealth!

Worse in AI Chip



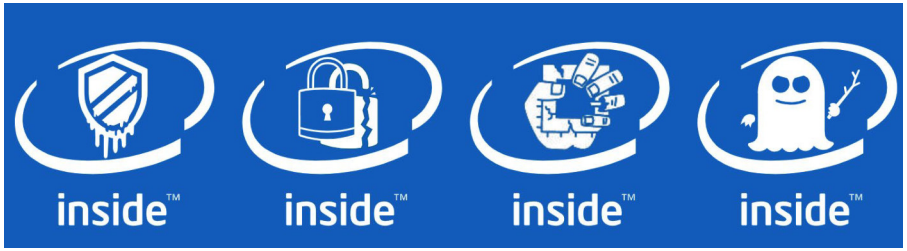


- AI Key Information:
  Structure, Parameters, Decision boundary, Functional

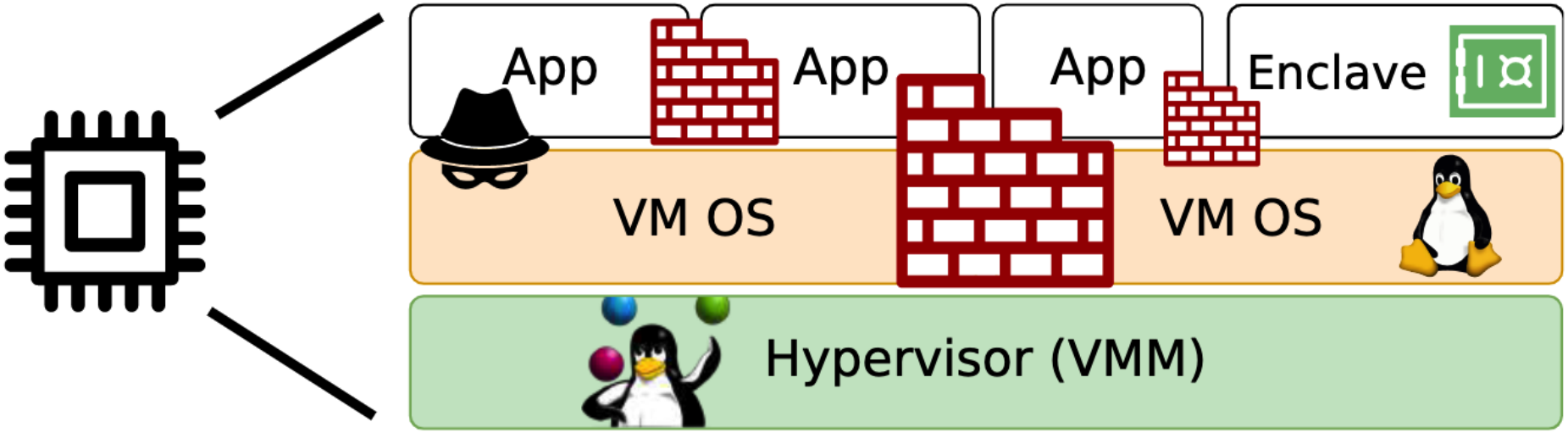
- Mainstream commercial AI chips are not secure
  - instructions are not encrypted
  - **Model could stolen at any time**

Worse in AI and Chip (or Micro Architecture)

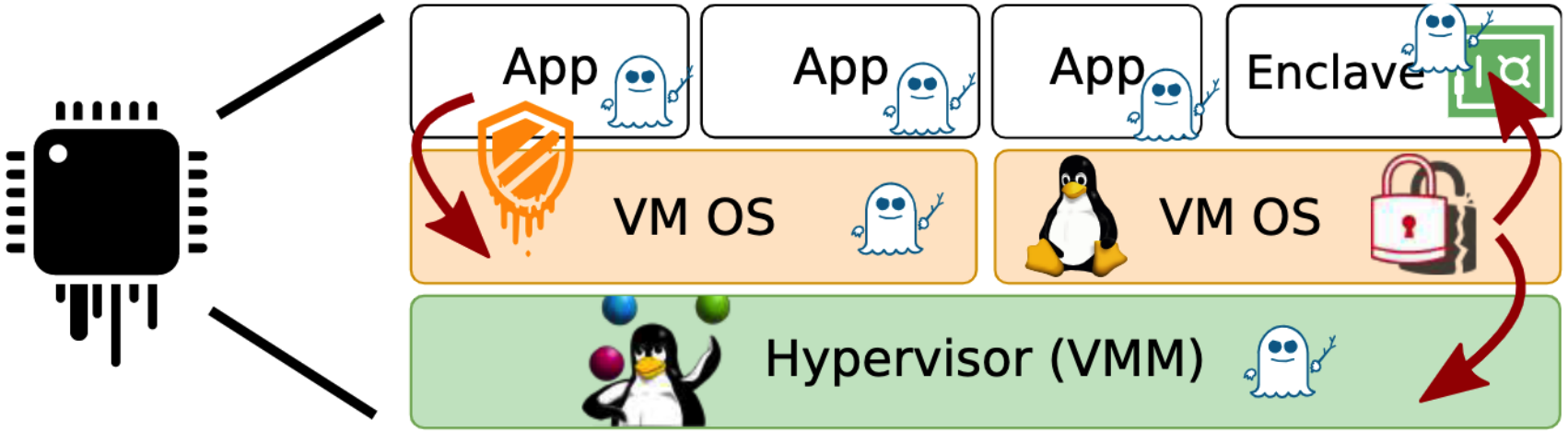
- during the last two decades,
  - primary goal :
    optimizing performance & saving cost
  - placing security as a secondary priority
- Classic chip design principles have security risks
  - (NO MATTER CPU GPU TPU or AI Chips accelerator)
  - Principle 1: Share resource => Side channel ATTACK
  - Principle 2: Speculative execution => Meltdown
  - Principle 3: Logical isolation => Information residue
- **Recent defense lose** !
  - Intel SGX
    -> bypassed
  - AMD Trust Zone
    -> hacked



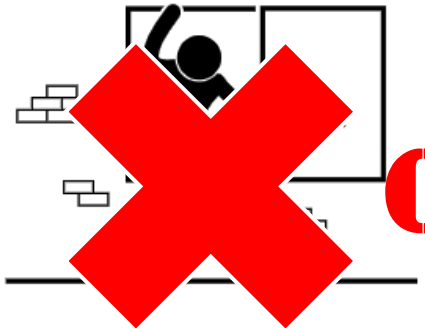
Worse in AI and Chip (or MicroArchitecture)



The fortifications were breached



Change the Game Rule



Unauthorized access

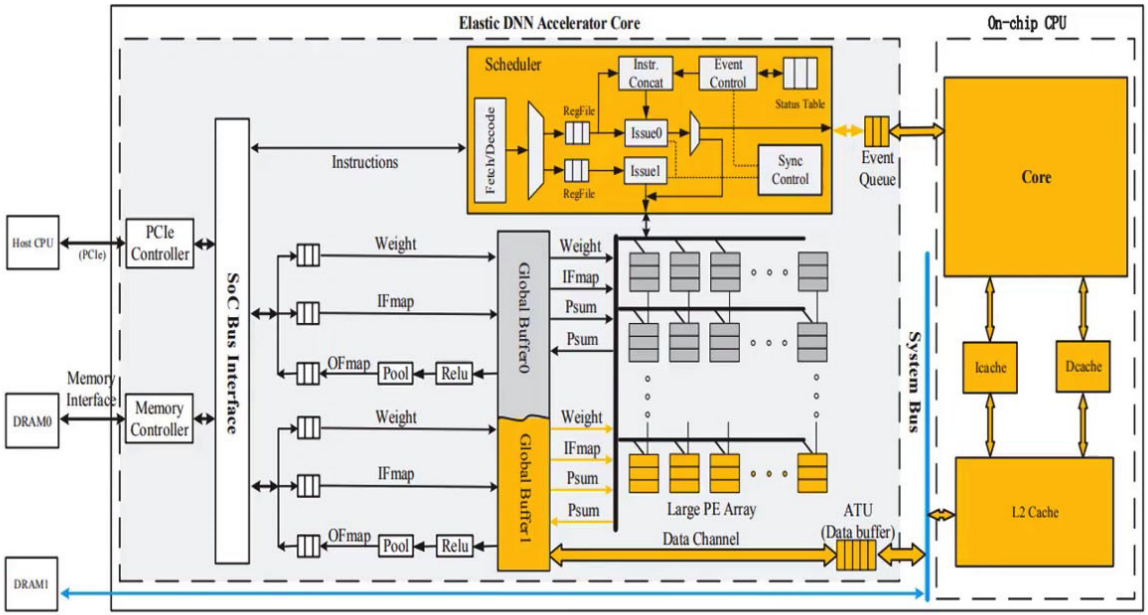
Transient out-of-order window

Exception handler

Heterogeneous Active Security Processor

Two Worlds :

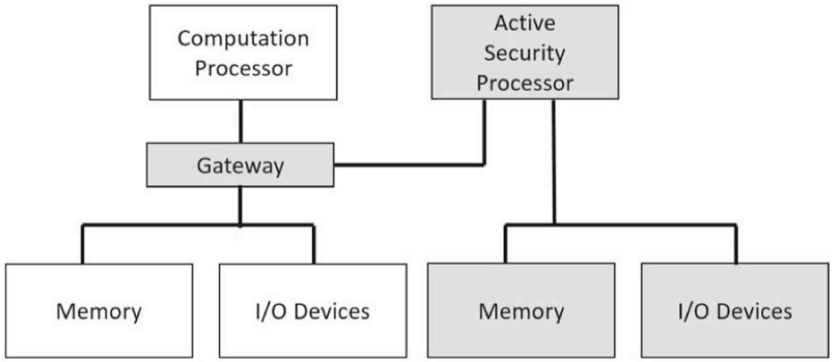
- **Traditional CPU**
  - ▶Computing Task
- **Active Security Processor**
  - ▶Security mechanisms

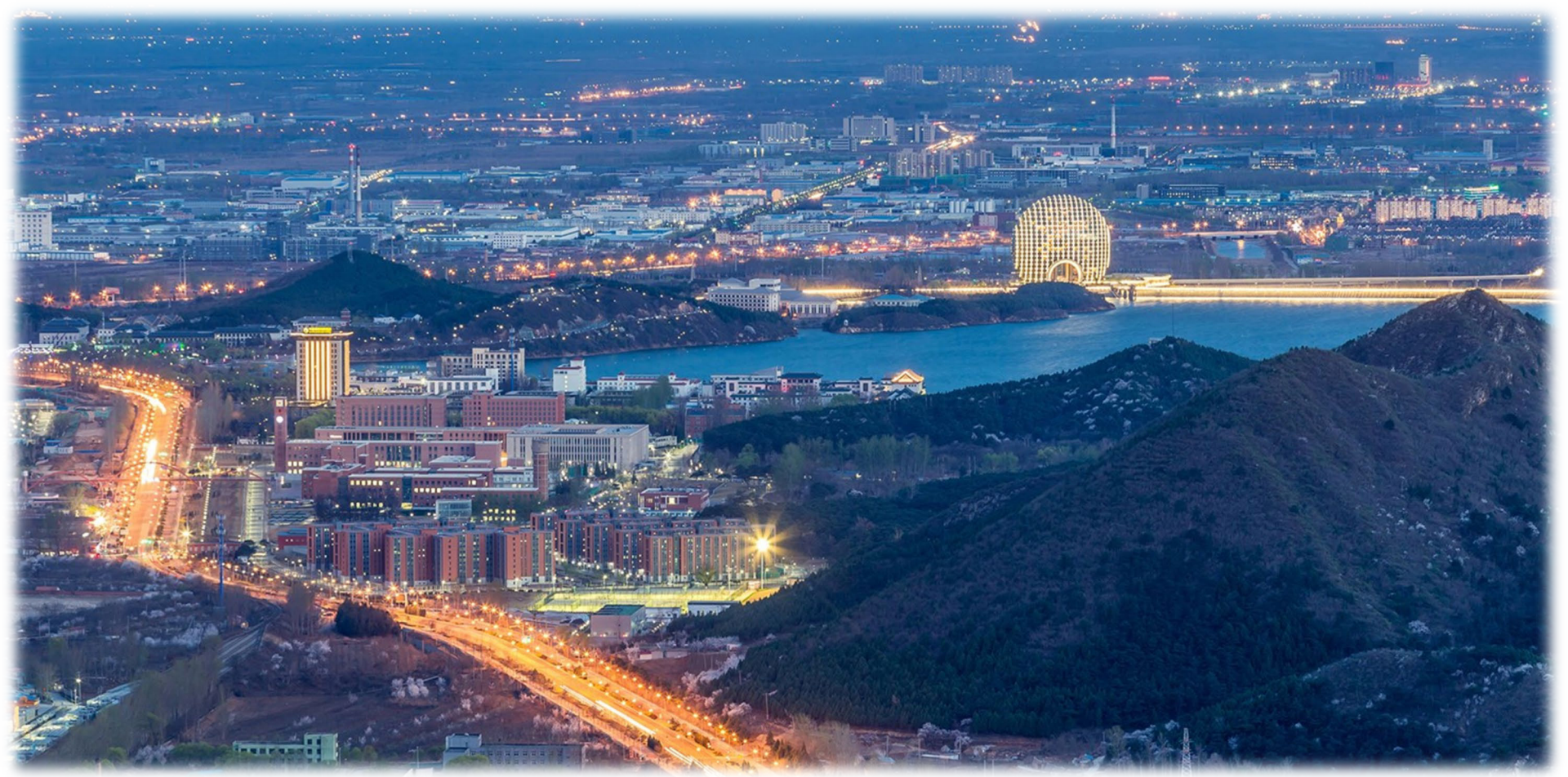


- Tightly coupled heterogeneous architecture
- Task-level Data Communication and sharing
- Task-level Synchronization and Scheduling

Two goals :

- **Reduce loss**
  - ▶Trade off Performance and cost
- **Heterogeneous**
  - ▶Ensure Attack is difficult





THANKS

中国科学院大学
University of Chinese Academy of Sciences