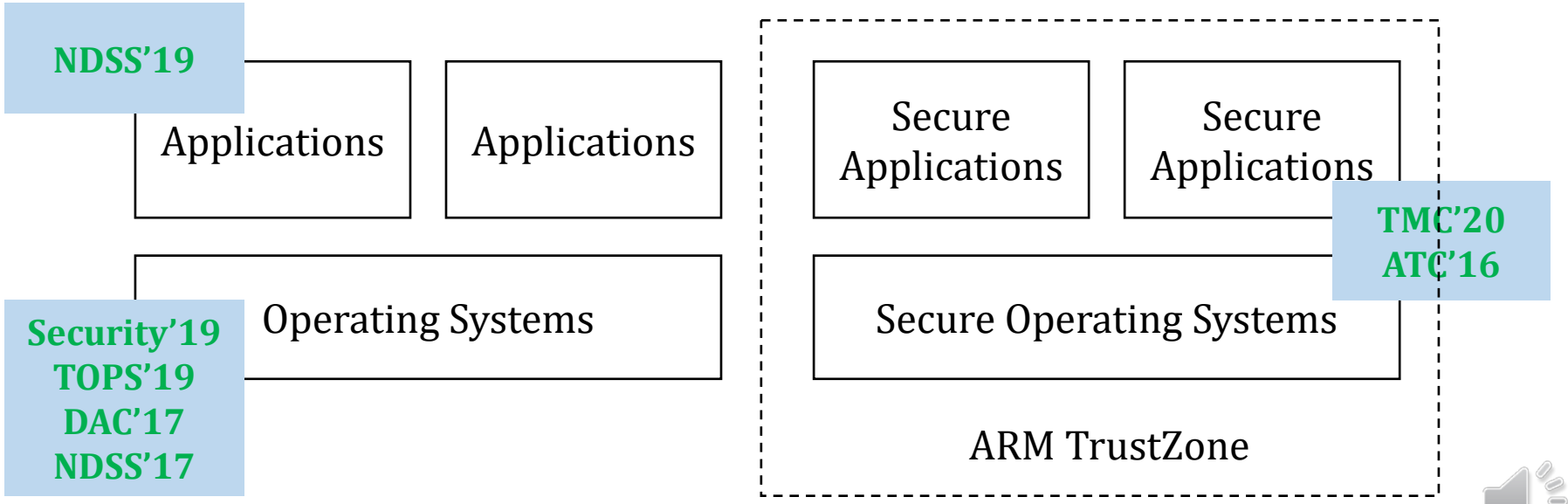
# Hardware-Based Techniques for Memory Safety

조영필

한양대학교

# Who am I

- 조영필 (Yeongpil Cho)
  - B.S. POSTECH, EE
  - Ph.D. Seoul National University, ECE
  - Before Soongsil University, Software
  - Now Hanyang University, CS



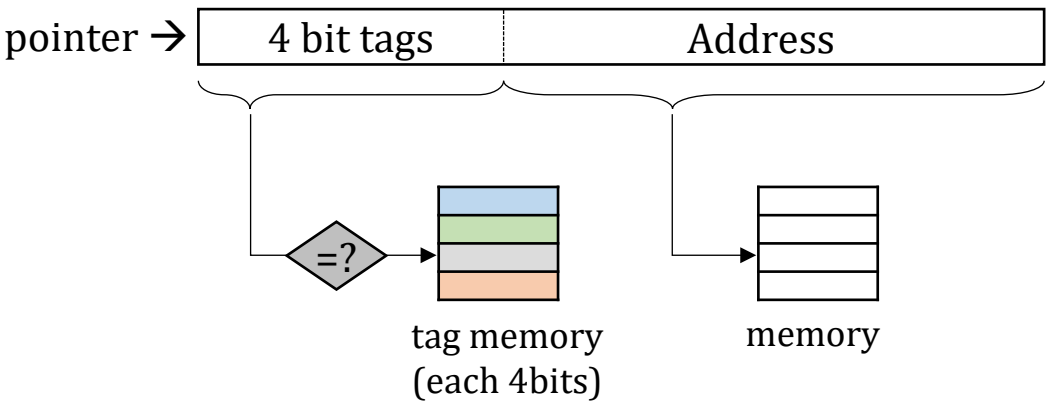
# Bounds comparison

- **Intel MPX** (Memory Protection eXtensions)
  - Pointer-level bounds comparison
  - Hardware-assisted per-pointer bounds managements and checks
    - Trie-structured bounds table
    - four bounds registers
  - Recent work
    - BOGO: buy spatial memory safety, get temporal memory safety (almost) free , ASPLOS 2019

```
void init() {
        char A[10];
        char B[20];
        bnd0 = bndmk A, A+10
        bndstx A, bnd0
        …
         strcpy (A, B, 10);
}

void strcpy (char *dest, char *src) {
        bndldx bnd0, dest
        bndldx bnd1, src
        while (*src != '\0') {
                bndcl bnd0, dest
                bndcu bnd0, dest
                bndcl bnd1, src
                bndcu bnd1, src
                *dest++ = *src++;
        }
}
```

# Tag comparison

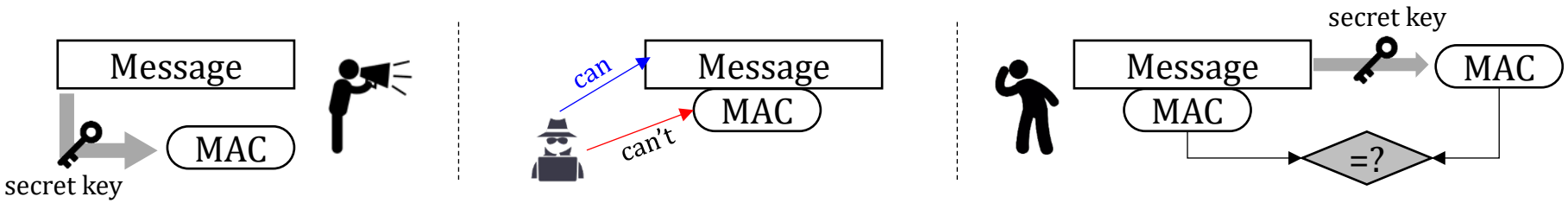
- **ARM MTE** (Memory Tagging Extension)
  - Pointers are allowed to access the memory with the matching tag
  - Hardware-assisted efficient tag management
  - Recent work
    - Memory Tagging and how it improves C/C++ memory safety, Report



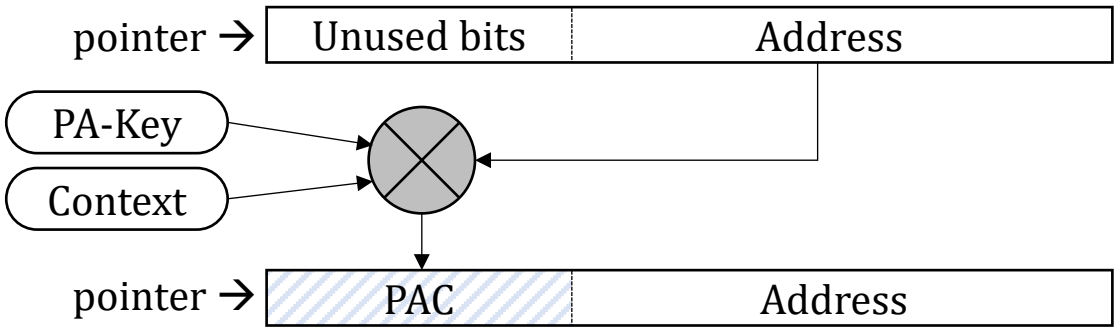

```
void init() {
        char A[10];
        char B[20];
        irg A, A
        for (i=0; i<10; i++)
                stg A[i];
        irg B, B
        for (i=0; i<10; i++)
                stg A[i];
        …
         strcpy (A, B, 10);}

void strcpy (char *dest, char *src) {
        while (*src != '\0') {
                *dest++ = *src++;
        }
}
```

# Pointer protection

- MAC (Message Authentication Code)




- **ARM PA** (Pointer Authentication)
  - Attaches PAC (Pointer Authentication Code) to a pointer
  - Recent work
    - PAC it up: Towards Pointer Integrity using ARM Pointer Authentication




```
pacia lr, sp      } prologue
push  lr

...
blr   ...         } body
...

pop   lr
autia lr, sp      } epilogue
ret   lr
```