Data oblivious programming

Eduardo Chielle
Oleg Mazonka

What is it (Data Oblivious Programming)?

Fancy name for no changing computation behaviour on sensitive data:

- Branching (if-else)
- Evaluating sensitive data resulting in access addresses

Example IF-ELSE

```
if (x > y) a = b;
else a = c;
```

```
cond = x > y;
a = cond * b + !cond * c;
```

Example IF

```
if (x > y) a = b;
```

```
cond = x > y;
a = cond * b + !cond * a;
```

Example WHILE

```
sum = i = 0;
while (i < n) sum += arr[i++];
```

```
sum = i = 0;
while (i < maxIter) sum += (i < n) * arr[i++];
```

Example []

```
int a[10];

int i=3;

int b = a[i];
```

```
Secure b = 0;

Secure i = 3;

for( int j=0; j<10; j++ ) b += a[j]*(i==j);
```

Problem 1

```
int a[10] = {…};

int b = MIN;

for( int x : a) if( x>b) b=x;
```

?

Problem 1 solution

```
int a[10] = {…};

int b = MIN;

for( int x : a) if( x>b) b=x;
```

```
for( sec x : a )

{

        k=x>b;

        b=k*x+(1-k)*b

}
```

Problem 2

```
int a[10] = {...};

int b1 = MIN, b2=MIN;

for( int x : a) if( x>=b1) { b1=x; b2=b1; }

else if (x>b2) b2=x;
```

?

Problem 2 solution

```
int a[10] = {...};

int b1 = MIN, b2=MIN;

for( int x : a) if( x>=b1) { b1=x; b2=b1; }

else if (x>b2) b2=x;
```

```
for( sec x : a ){

        k1 = x>b1; k2=x>b2;

        t1=k1*x+(1-k1)*b1

        t2=k1*k2*b1+k2*(1-k1)*x+(1-k2)*b2;

        b1=t1; b2=t2;

}
```

YOU SHALL NOT
VIOLATE MY PRIVACY
memegenerator.net