Technion
Israel Institute of Technology

ANDREW AND ERNA VITERBI
FACULTY OF ELECTRICAL ENGINEERING

Zero-effort adaptable security

Mark Silberstein

Hiroshi Fujiwara
Cyber Security
Research Center

- **Security-sensitive code**
  - **Tiny TCB**
  - **Thoroughly verified**
  - **Hand-crafted protection against side channels**

Security-sensitive code development

Only for experts

Security-sensitive code development

And for the rest of us

Nowadays

Power to the people!

Security for masses!


RECIPE
How to prepare
secure applications

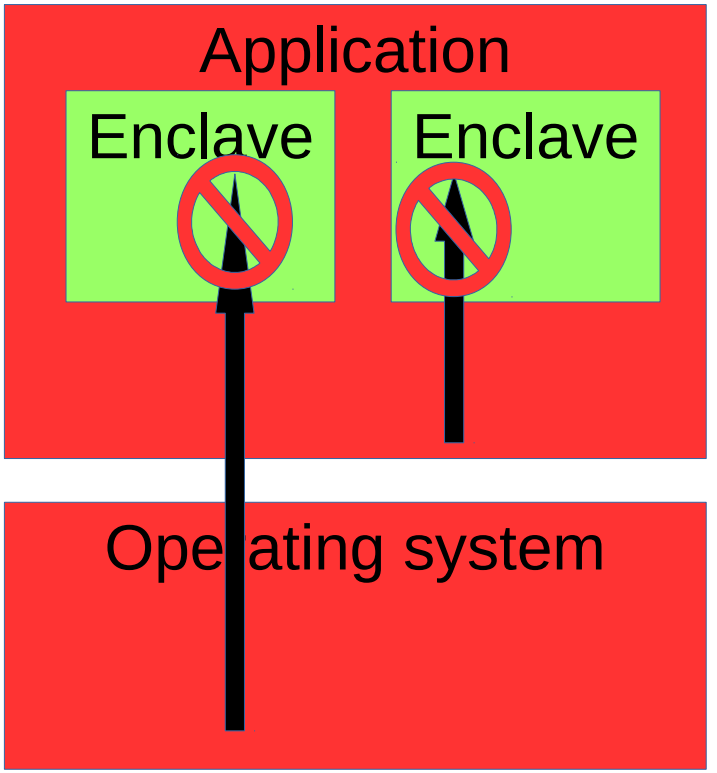
1. Take your favorite app
2. Run in SGX enclave
3. Done

1. Take your favorite app
2. Run in enclave
3. Done

Secure and fast

Why is it secure and fast?

- Reversed sandbox
- Private code & data
  - Confidentiality
  - Integrity
  - Freshness
- Defends against OS!
- HW acceleration
- Scales with CPU scaling



1. Take your favorite app
2. Run in enclave
3. Done

Secure and fast

Running unsecured/unmodified applications

System support

Performance
Convenience

Security issues

Side channels
Buffer overflows
ROP

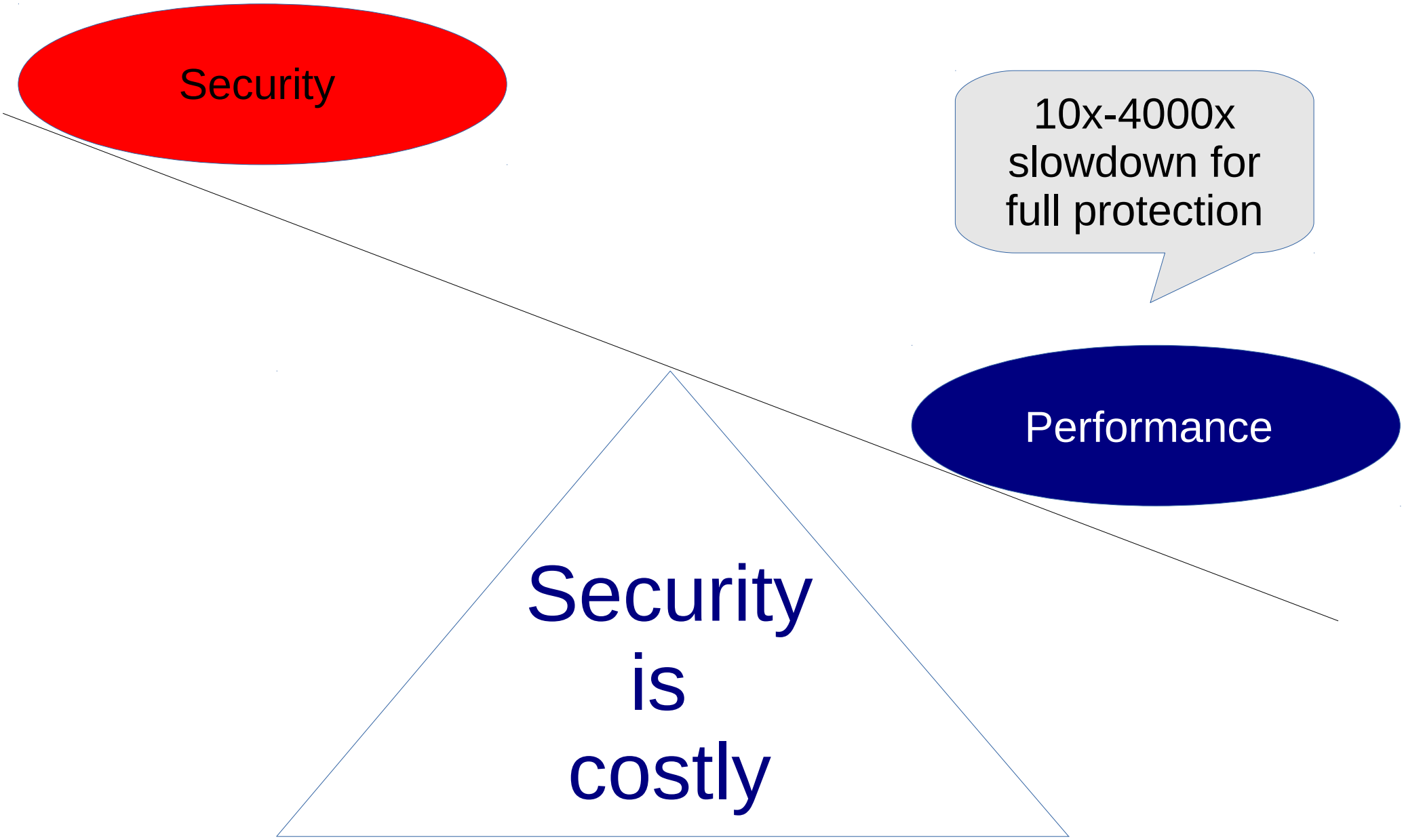
System support for zero-cost security

- Compatibility layers / LibOS
  - SCONE[OSDI16], Graphene-SGX[ATC17], Haven[OSDI14]
- Reducing huge TCB
  - Glambdring[ATC17]
  - Panoply[NDSS17]
- Performance enhancement
  - Eleos[EUROSYS17]

Hardening SGX security

- Page table attacks and mitigation
  - T-SGX[NDSS17], Leaky Cauldron [CCS17]
- Cache-timing attacks and mitigation
  - DR.SGX[Arxiv], Cloack[USENIX Sec17]
- ROP/ASLR
  - Dark-ROP[USENIX Sec17] vs. SGX-Shield [NDSS17]
- Branch predictor attacks
  - Branch shadowing [USENIX Sec17]
- Preventing buffer overflows
  - SGXBounds [Eurosys17]

So what's the problem?


Security
10x-4000x slowdown for full protection
Performance
Security is costly

The level of protection depends on:

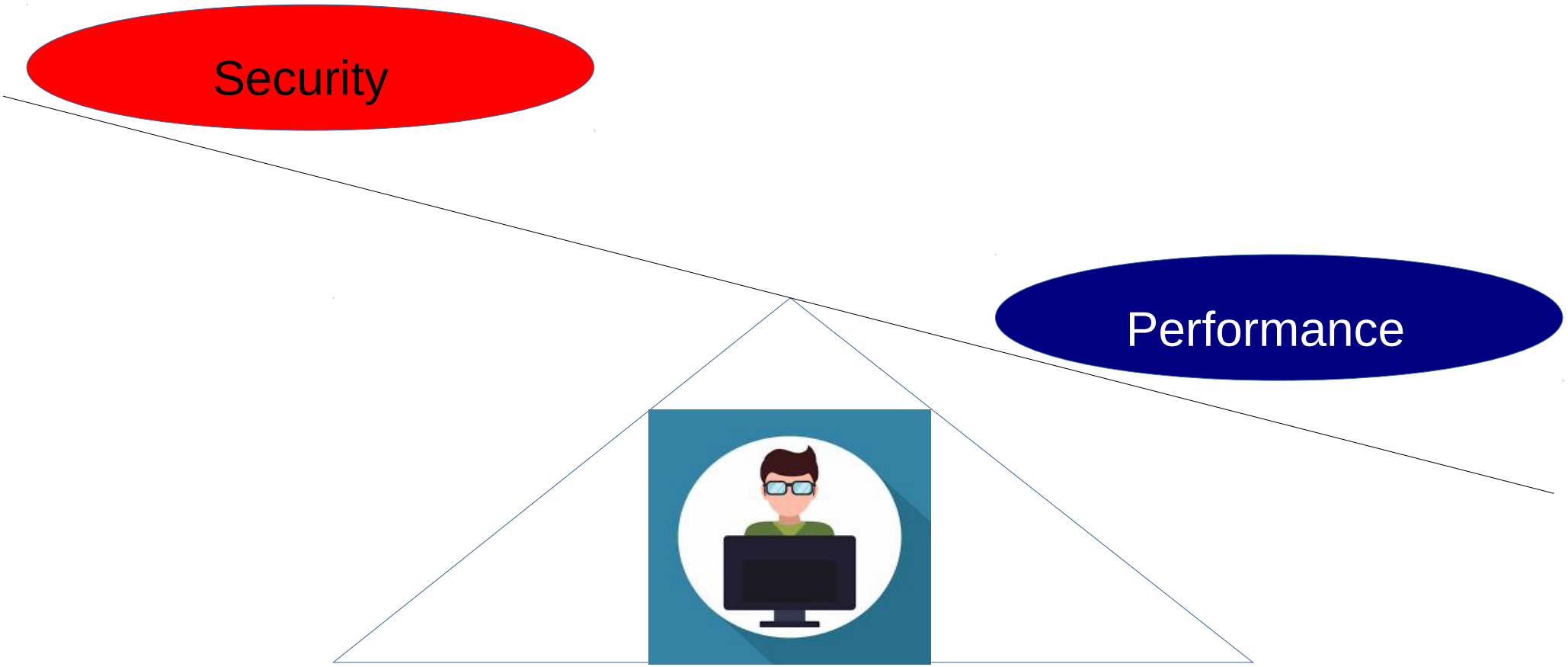
- Execution environment and expected threats
  - Public vs. private clouds
  - Side channels vs. direct attacks
  - Multi-tenant vs. exclusive use
- Operational requirements
- Tolerable performance cost

The level of protection depends on:

- Execution environment and expected threats
  - Public vs. private clouds
  - Side channels vs. direct attacks
  - Multi-tenant vs. exclusive use
- Operational requirements
- Tolerable performance cost

ISVs must support different levels in the same application!

How to support all of them at once without code modification??



Needed: adaptable security at low development cost

Unprotected Fully Protected

ZIKIT: **Z**ero-effort **I**nstrumentation tool**K**it for adaptable secur**IT**y

- Developer annotates sensitive memory regions

DONE

ZIKIT: Zero-effort Instrumentation toolKit for adaptable securITy

- Developer annotates sensitive memory regions

DONE

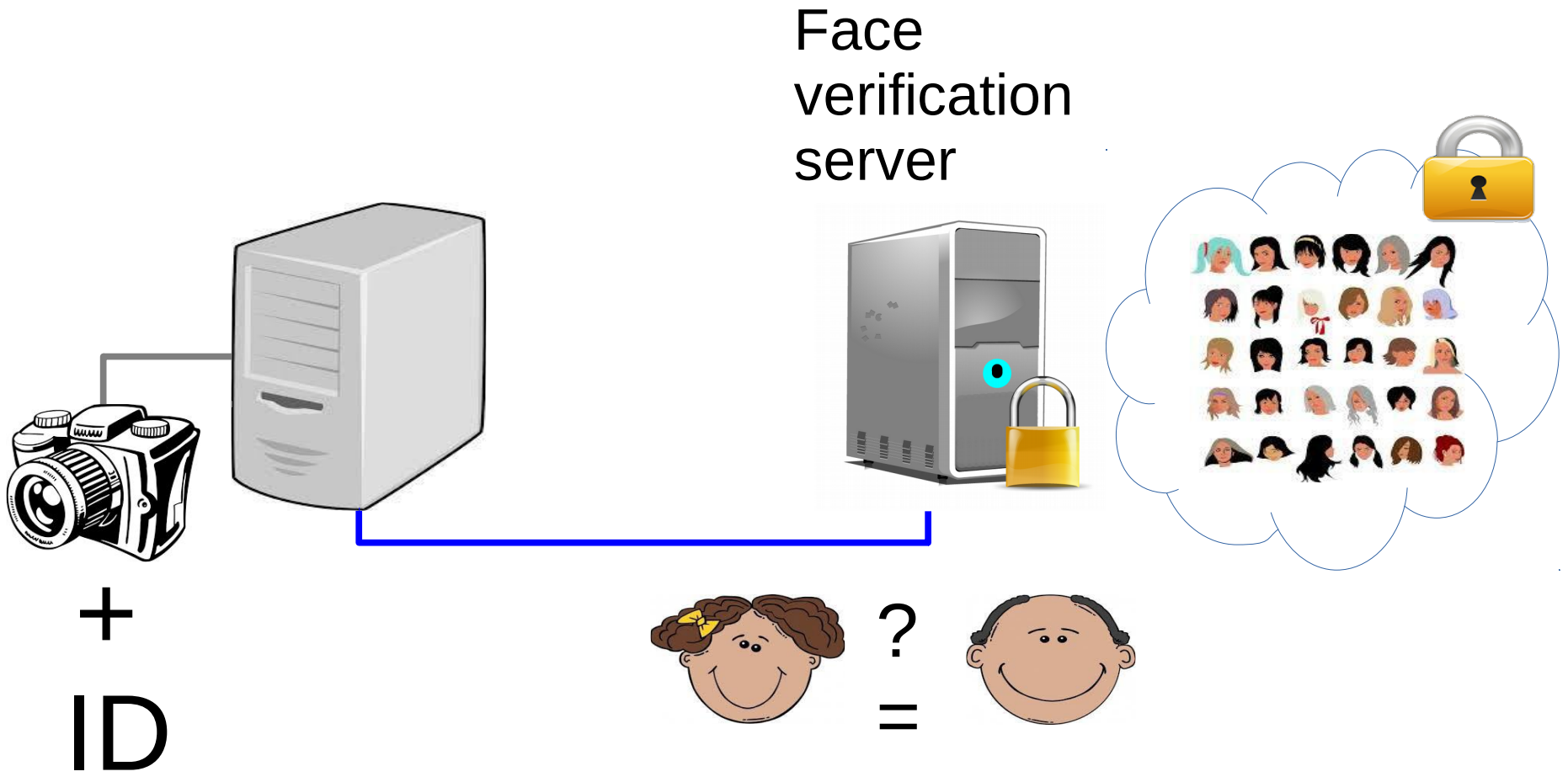
- At runtime/deployment: choose desirable protection level

Unprotected Fully Protected

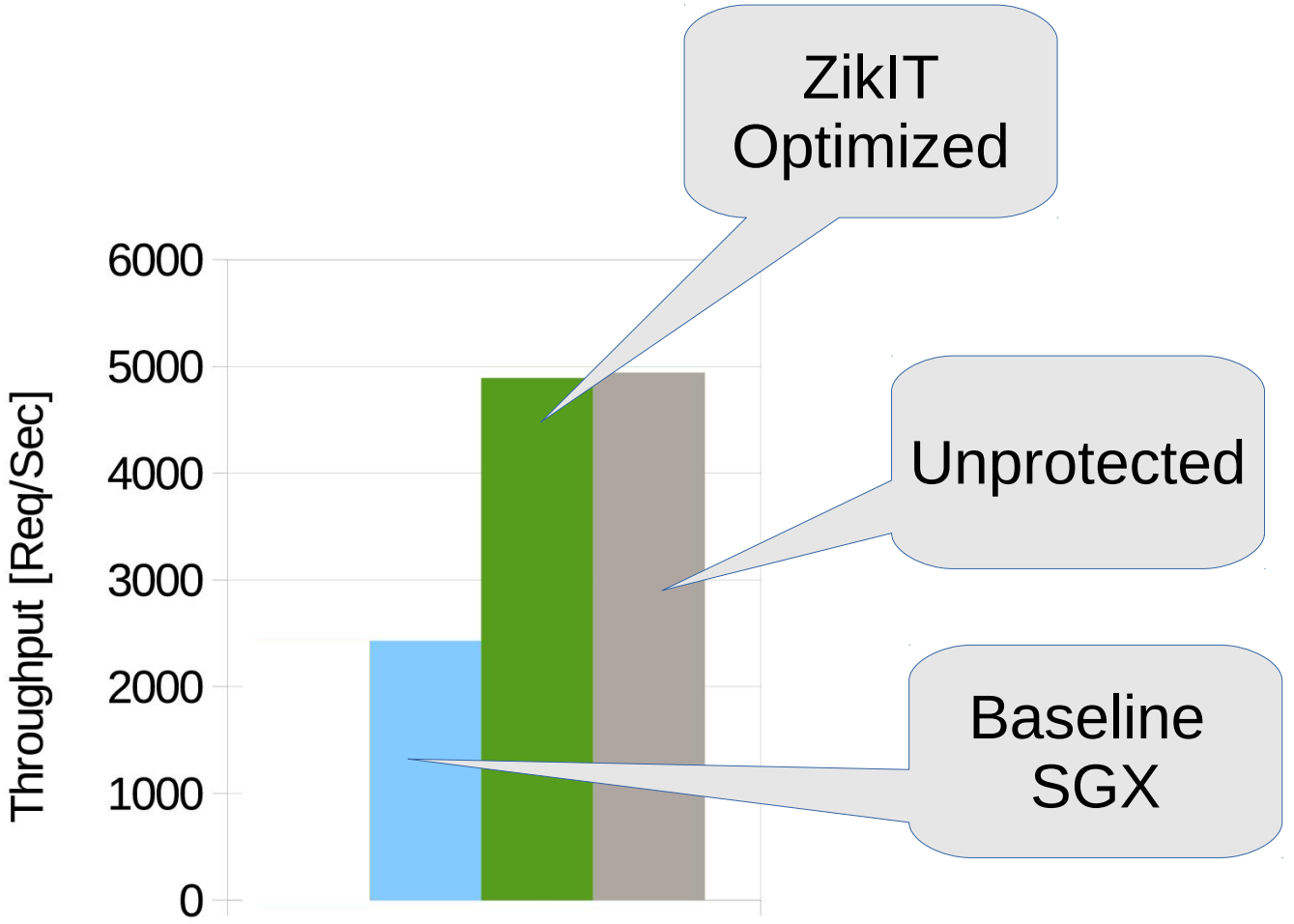
Under the hood

- Compiler-based selective hardening of data and code via static analysis
- Performance optimizations for memory-intensive SGX applications
- Pluggable modules for ORAM, bounds checking, remote communication,...

Biometric Identity validation server



Biometric Identity validation server



1. Take your favorite app
2. Compile with ZIkIT
3. Run in SGX
4. Done

Nope.. Still working on it!

Thank you!

Watch for open source code at
https://github.com/acsl-technion

mark@ee.technion.ac.il

https://sites.google.com/site/silbersteinmark