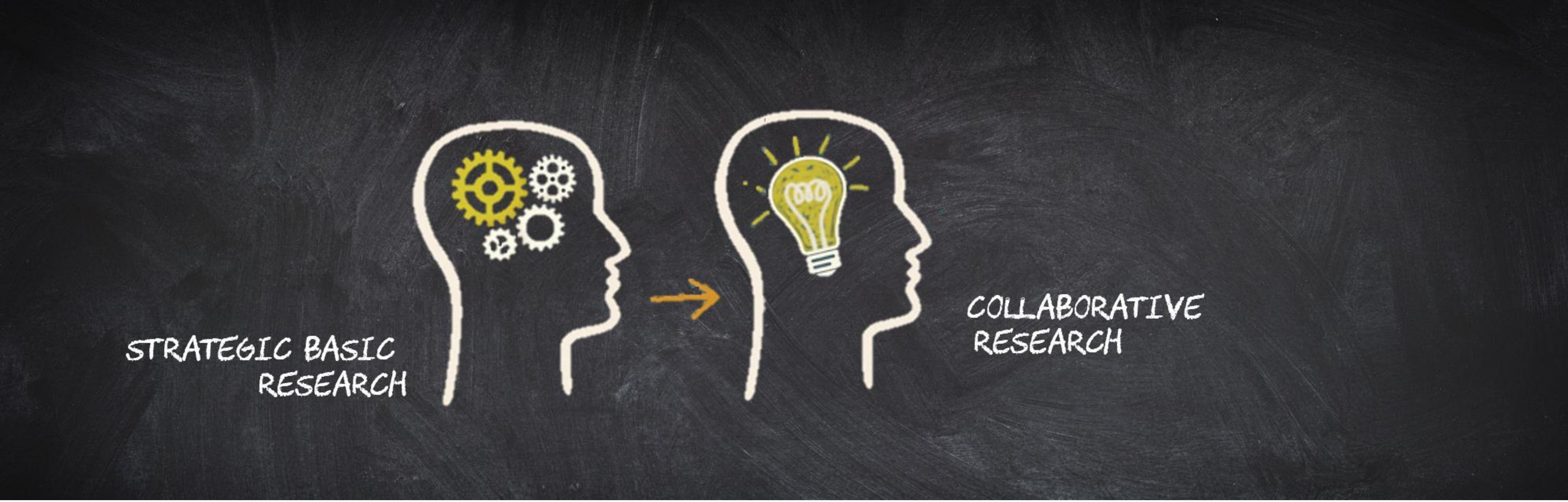


Strategic Cybersecurity Research and Support for Innovation in Industry

Bart Preneel - COSIC, KU Leuven
Wouter Joosen - DistriNet, KU Leuven

Leuven, January 31, 2020

Cybersecurity Initiative Flanders

“Top Strategic Basic Research Programme”

TRACK 01

Secure Software & Applications

TRACK 02

Security Services

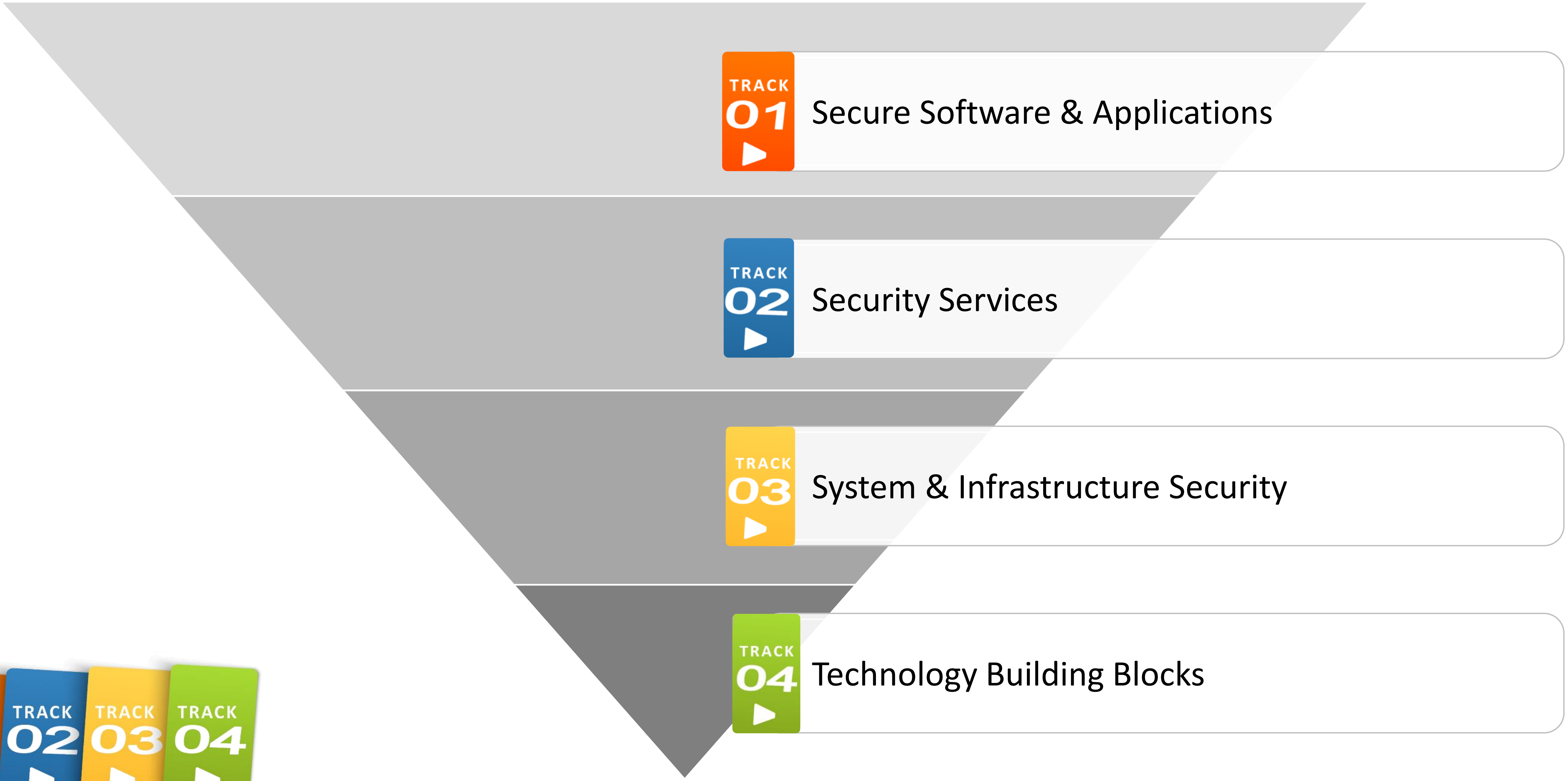
TRACK 03

System & Infrastructure Security

TRACK 04

Technology Building Blocks

(Potentially) ***different audiences*** for different research tracks



Secure Software & Applications

Security Services

System & Infrastructure Security

Technology Building Blocks

TRACK 01

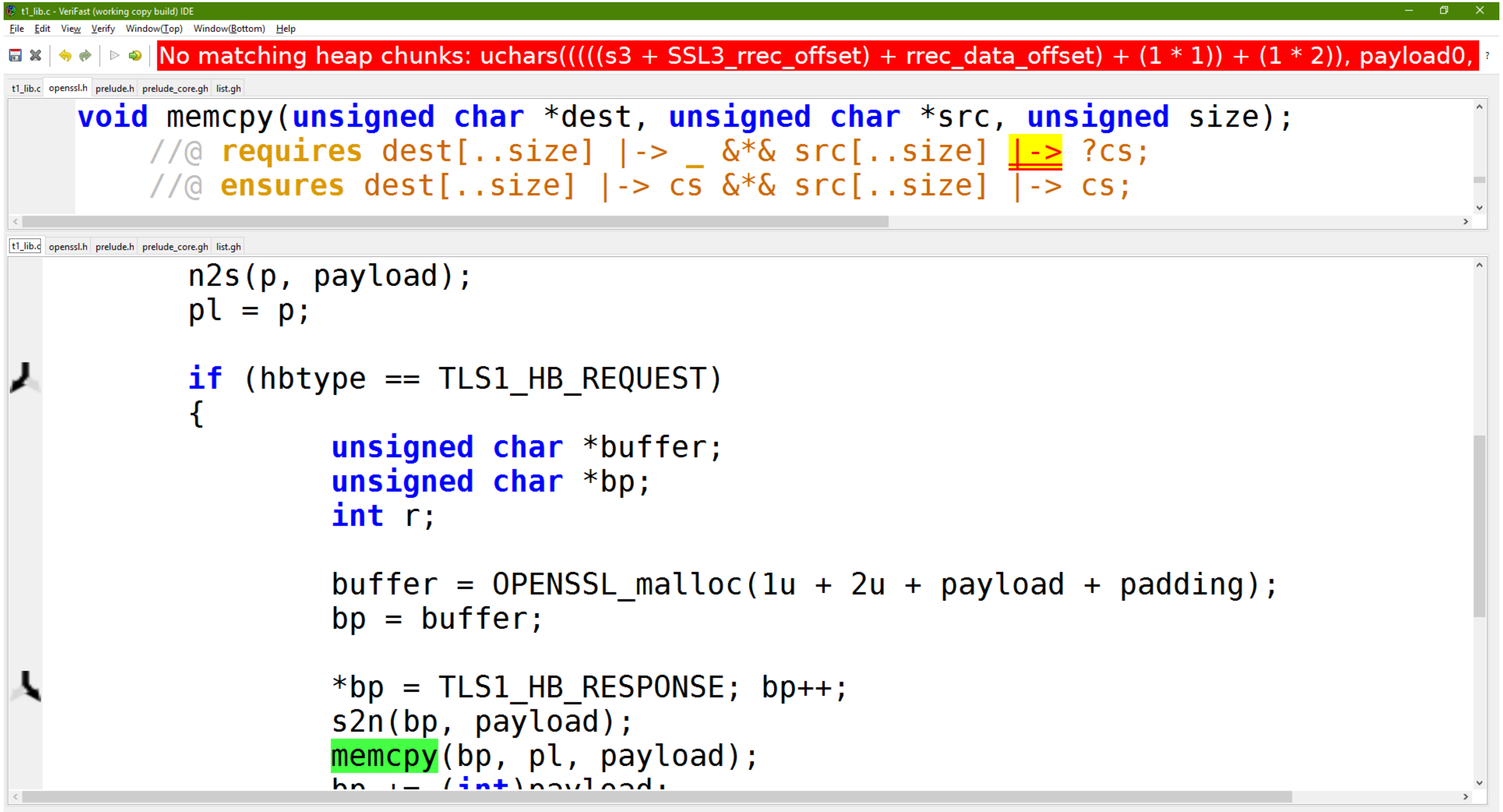
Secure Software & Applications

- THEME 1
  Secure Software Development Life Cycle (SDLC)

- THEME 2
  Program Verification and Security Testing

- THEME 3
  Secure Programming Languages & Secure Compilation

VERIFICATION ON THE HORIZON



No matching heap chunks: uchars(((((s3 + SSL3_rrec_offset) + rrec_data_offset) + (1 * 1)) + (1 * 2)), payload0,

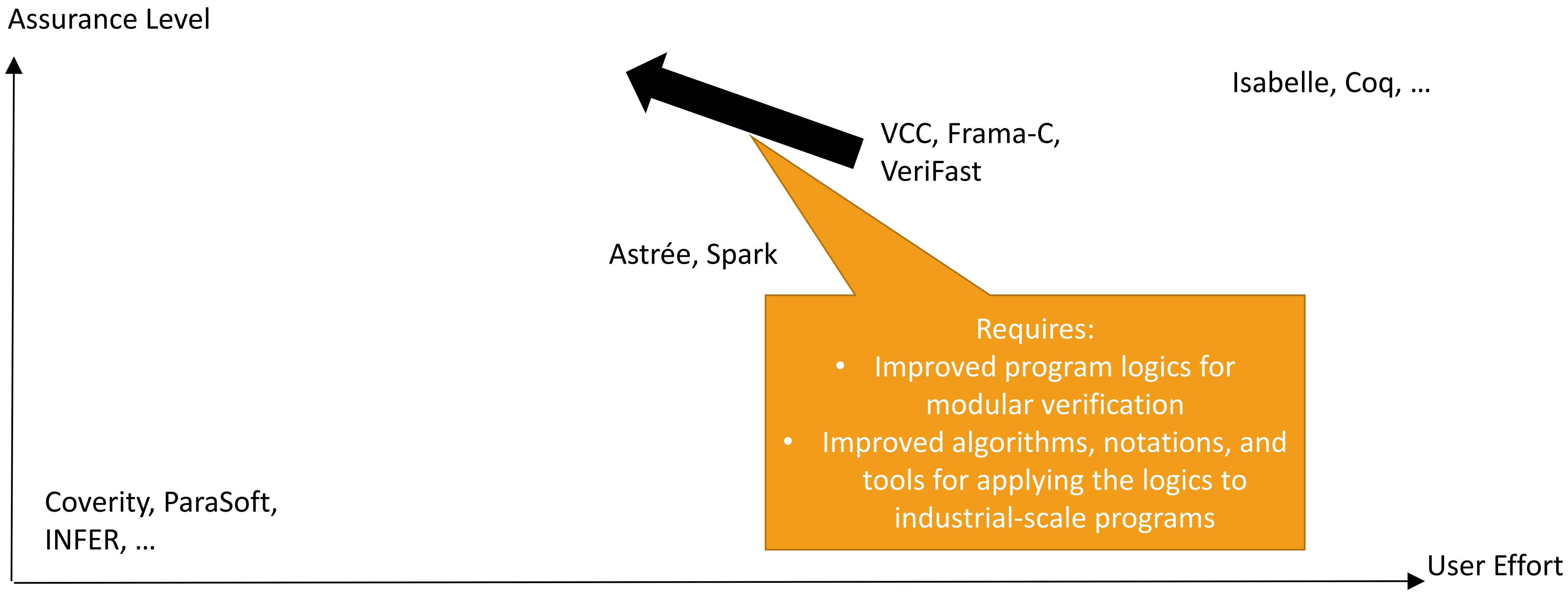
```
void memcpy(unsigned char *dest, unsigned char *src, unsigned size);
    //@ requires dest[..size] |-> _ &*& src[..size] |-> ?cs;
    //@ ensures dest[..size] |-> cs &*& src[..size] |-> cs;
```

```
        n2s(p, payload);
        pl = p;

        if (hbtype == TLS1_HB_REQUEST)
        {
                unsigned char *buffer;
                unsigned char *bp;
                int r;

                buffer = OPENSSL_malloc(1u + 2u + payload + padding);
                bp = buffer;

                *bp = TLS1_HB_RESPONSE; bp++;
                s2n(bp, payload);
                memcpy(bp, pl, payload);
                bp += (int)payload;
```

THEME 2

01

OBJECTIVE



Requires:

- Improved program logics for modular verification
- Improved algorithms, notations, and tools for applying the logics to industrial-scale programs

THEME 2

01

TRACK

02

Security Services

- THEME1
  Identity Management and Authentication

- THEME 2
  Authorization and Audit

- THEME3
  Advanced Encryption Techniques and Data Access Middleware

- THEME4
  Policy and Regulation

POLICY AND REGULATIONS

TRACK 02

Security Services

EU Council Directive Critical Infrastructures (2008)

EU Cybercrime Directive (2013)

PSD2 Directive (2015)

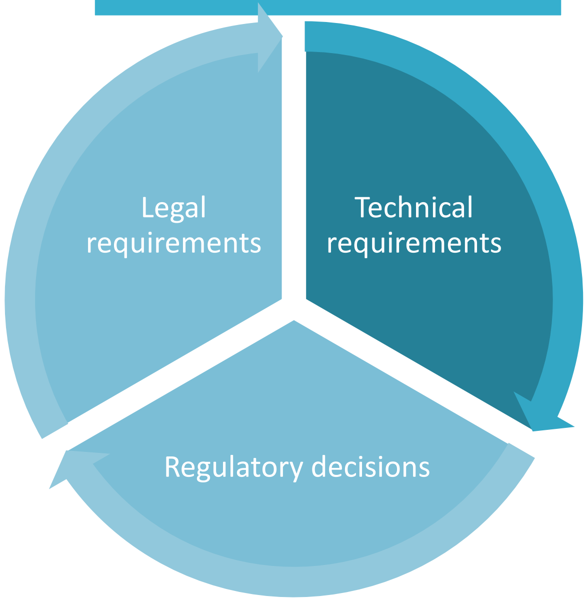
EU NIS Directive (2016)

General Data Protection Regulation (2016)

Free-flow of Non-personal Data Regulation (2018)

European Electronic Communications Code (2018)

ePrivacy Regulation (20xx?)



Directive on Open Data and PSI (2019)

Cybersecurity Act (2019)

TRACK 03

▶

System & Infrastructure Security

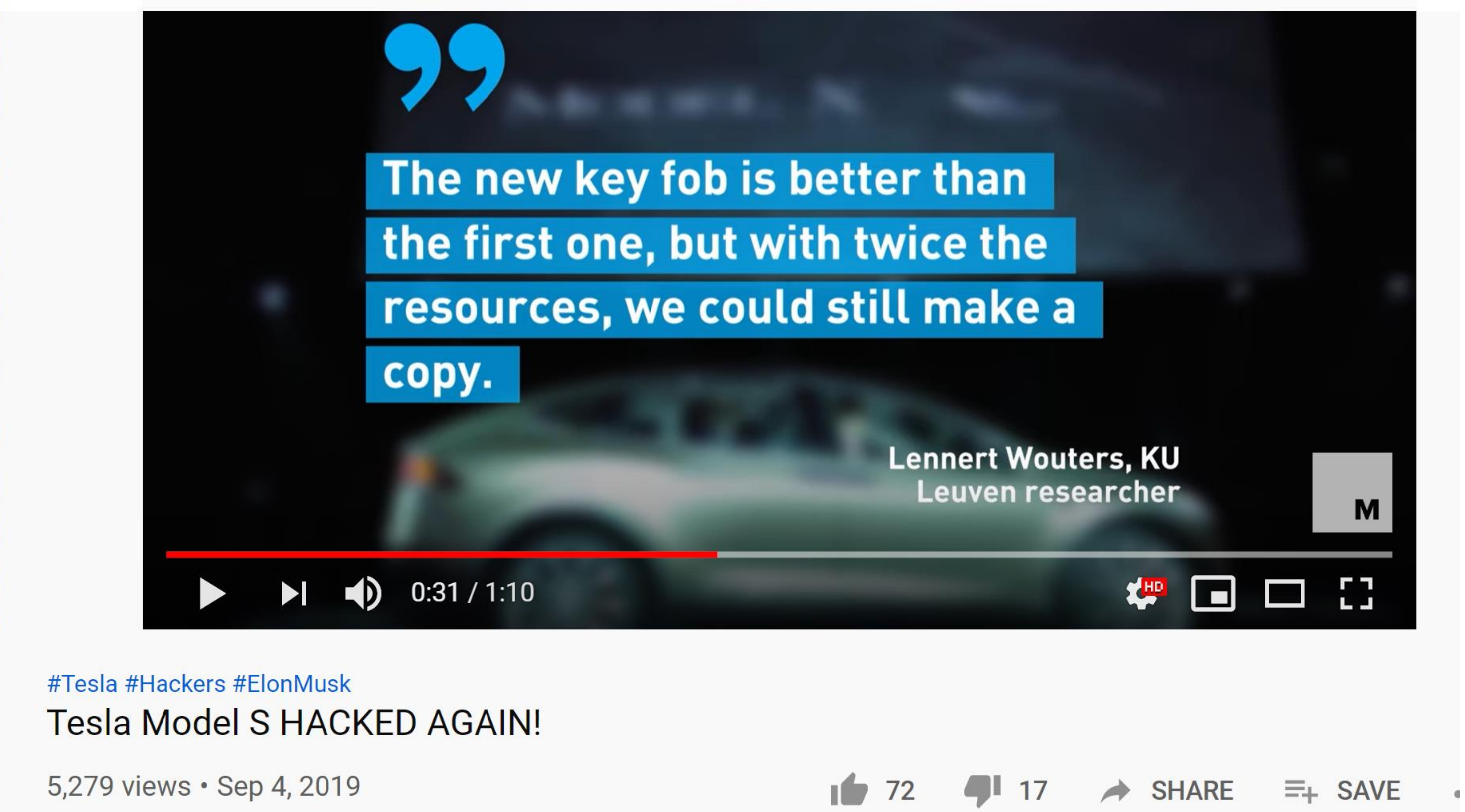
- THEME 1
  System Security
- THEME 2
  Network Security
- THEME 3
  Security Monitoring and Management

2018 Tesla Key fob hack: cloning a key fob in 2 seconds

https://www.youtube.com/watch?v=aVlYuPzmJoY
https://www.esat.kuleuven.be/cosic/fast-furious-and-insecure-passive-keyless-entry-and-start-in-modern-supercars/

2017: Responsible disclosure (12 months)
2018: new key fobs with proper 80-bit keys (DST-80)

2019: Cloning new fob takes 4 seconds
New responsible disclosure
Over the air update possible



The new key fob is better than the first one, but with twice the resources, we could still make a copy.

Lennert Wouters, KU Leuven researcher

#Tesla #Hackers #ElonMusk

Tesla Model S HACKED AGAIN!

5,279 views • Sep 4, 2019

TRACK 04 ▶

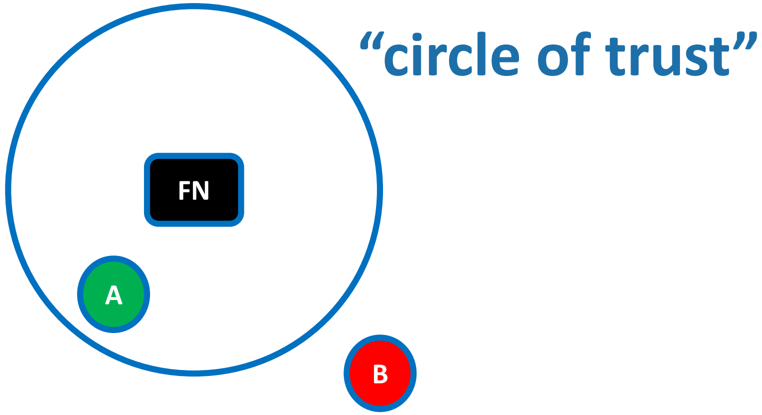
Technology Building Blocks

- THEME 1
  Secure hardware
- THEME 2
  Cryptographic algorithms
- THEME 3
  Cryptographic protocols
- THEME 4
  Secure and efficient cryptographic implementations

Secure RF distance bounding for Bluetooth

Defeating relay attacks

Relay attack Solihull



"circle of trust"

FN

A

B

01 ▶ Bart Jacobs

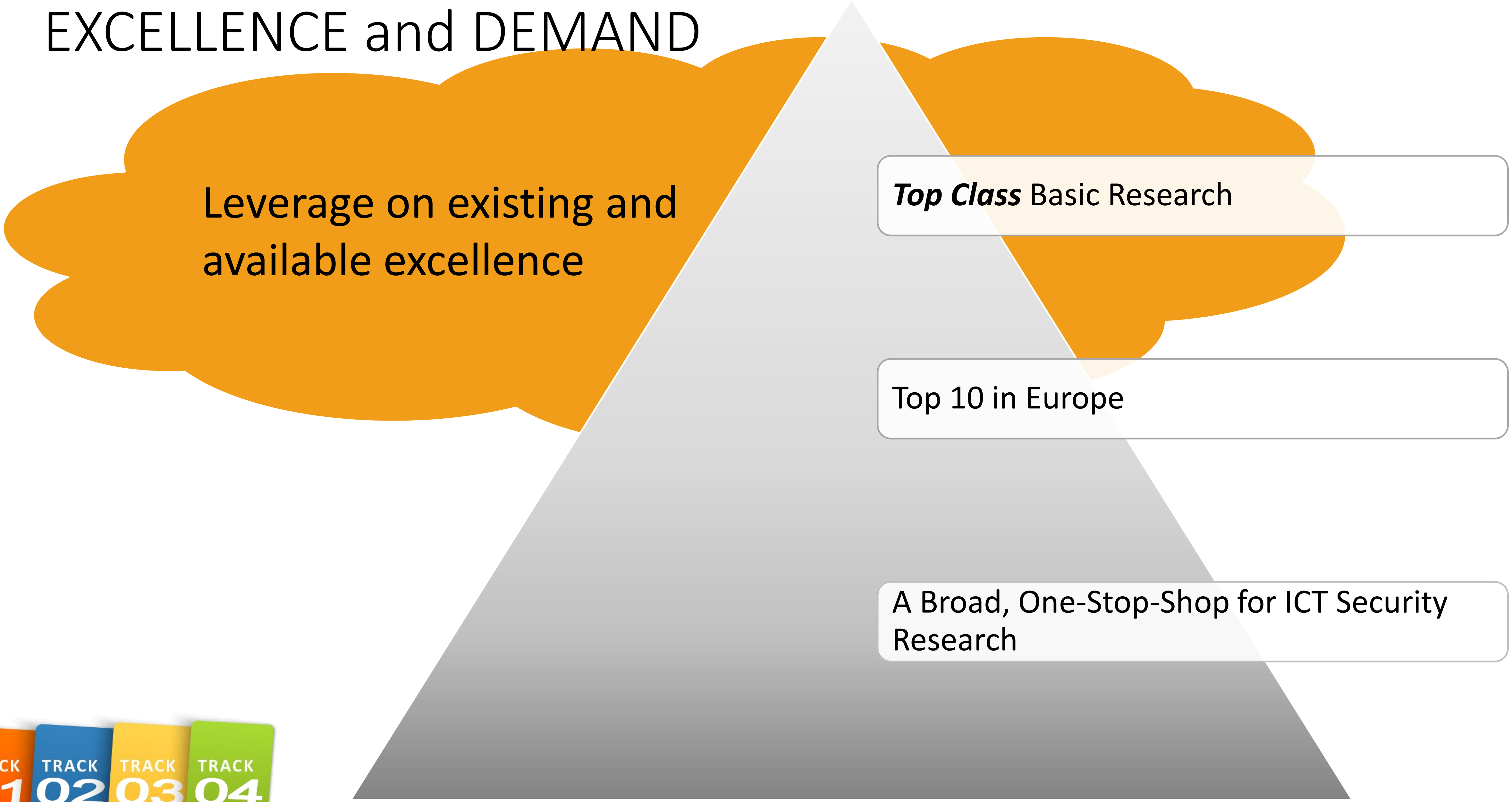
02 ▶ Frederik Vercauteren

03 ▶ Frank Piessens

04 ▶ Ingrid Verbauwhede

TRACK 01 ▶ TRACK 02 ▶ TRACK 03 ▶ TRACK 04 ▶

EXCELLENCE and DEMAND



Leverage on existing and available excellence

Top Class Basic Research

Top 10 in Europe

A Broad, One-Stop-Shop for ICT Security Research

INDUSTRY FEEDBACK
(e.g. April 2019)

INTERNATIONAL SCIENTIFIC ADVISORY BOARD (July 2019)

TRACK 01 Secure Software & Applications

Secure SDLC – Secure Software Development Life Cycle

(RA 1.1.1) Cybersecurity Requirements

(RA 1.1.2) Cybersecurity-by-Design Solutions

(RA 1.1.3) Security Analysis for Existing Applications

Program Verification

(RA 1.2.1) Formal Program Verification

(RA 1.2.2) Incremental Static Application Security Testing (SAST) for Distributed Applications

(RA 1.2.3) Efficient Runtime Application Security Protection (RASP) for Distributed Applications

Secure Programming Languages and Secure Compilation

(RA 1.3.1) Mechanically-verified Security Proofs for Capability Machine Programs

(RA 1.3.2) Specifying and Proving Security Properties of Side-Effecting Programs

(RA 1.3.3) Language-embedded Security Policies for Distributed Micro-services.

TRACK 02 Security Services

Identity Management and Authentication

(RA 2.1.1) Identity

(RA 2.1.2) Frictionless Authentication: Collaborative and Continuous

(RA 2.1.3) Privacy-preserving Identity and Authentication

Authorization and Audit

(RA 2.2.1) Enhancing Authorization Capabilities

(RA 2.2.2) Intelligent Audit

(RA 2.2.3) Synergy between Audit and Authorization

Advanced Encryption Techniques and Data Access Middleware

(RA 2.3.1) Secure Outsourced Data Processing

(RA 2.3.2) Secure Collaborative Data Processing

(RA 2.3.3) Data Access Middleware

Policy and Regulation

(RA 2.4.1) Legal Compliance Analysis

(RA 2.4.2) Policy Analysis

(RA 2.4.3) Legal Engineering Analysis

TRACK 03 System & Infrastructure Security

System Security

(RA 3.1.1) Protection Against Software-Controlled Side-Channel Attacks (on general purpose hardware)

(RA 3.1.2) Processor Extension to Support New System Security Models

(RA 3.1.3) Security and Safety In Mixed Criticality Systems

(RA 3.1.4) Diversity-based Multi-Variant Execution Mitigation Techniques for System Defense

Network Security

(RA 3.2.1) Study of Critical Internet Components and Protocols

(RA 3.2.2) Secure Communication Protocols for the IoT

(RA 3.2.3) Analysis of Protocol Implementations

Security Monitoring and Management

(RA 3.3.1) Intelligence Gathering and Identification of Security State

(RA 3.3.2) Methods and Tools for Secure Deployment

(RA 3.3.3) Detection and Response for IoT and Industrial Control Systems

TRACK 04 Technology Building Blocks

Secure Hardware: Roots of Trust Anchored into Technology Foundations

(RA 4.1.1) Developing PUFs

(RA 4.1.2) True Random Number Generators

(RA 4.1.3) Technology Solutions to Secure Circular Economy

Cryptographic Algorithms

(RA 4.2.1) Symmetric-key Algorithms

(RA 4.2.2) Public-key Algorithms

(RA 4.2.3) Proofs and Validation

Cryptographic Protocols

(RA 4.3.1) Cryptographic Protocols for Distance Bounding

(RA 4.3.2) Cryptographic Protocols Design for MPC Applications

(RA 4.3.3) Cryptographic Protocols for Blockchain

(RA 4.3.4) Cryptographic Protocols for Mix Networks

(RA 4.3.5) Security Analysis of Cryptographic Protocols

Secure and Efficient Cryptographic Implementations

(RA 4.4.1) Implementation Challenges of Post-quantum, FHE, Lightweight Crypto on Novel Compute Platforms

(RA 4.4.2) Side-Channel and Fault Attacks

(RA 4.4.3) White-Box Cryptography

KU LEUVEN

imec

COSIC

Focus

PROTECTION OF DIGITAL INFORMATION

Critical Mass in Cybersecurity

80 + members
7 professors
8 research experts/managers

Portfolio of Research Projects

30 + ongoing projects
50 + European research projects (incl. 2 ERCs)

Output related to Cybersecurity

29 PhDs since 2014

Selected Awards

AES Competition 2001
2 ERC Grant Holders
3 IACR Fellows
1 IEEE Fellow 2013
1 CNIL Award

Cybersecurity Research

Symmetric Key Cryptography
Public Key & Cryptographic Protocols
Embedded Systems Security
Privacy & Identity Management
Mobile & Wireless Security

Application Domains

Authentication
using Biometrics
Privacy technologies
Blockchain
Internet-of-Things
Automotive

Publications at Top Venues

IACR conferences: 246
Top 4 security conferences: 30
Other Core A/A* cybersecurity conferences: 29
Core A*/A cybersecurity journals: 99

Valorization

Industry training
Startups: CrypTech, nextAuth
Multiple patents
Multiple Software & Hardware Libraries

KU LEUVEN imec DistriNet

Focus

ICT Security and Distributed Systems

Critical Mass in Cybersecurity

65 + members
7 professors
7 research experts/managers (5 FTE)

Portfolio of Research Projects

30 + ongoing projects
25 + European research projects

Output related to Cybersecurity

52 PhDs since 2014

Selected Awards

USENIX 2018
DLSW 2017
CCS 2017
ACM SYSTEX 2017

Cybersecurity Research

Development of Secure Software & Applications
Secure Programming & Programming Languages
Software Engineering for Security
Advanced Verification
System Security
Authentication, Authorization & Audit
Security Analytics

Application Domains

Smart Cities
E-Health
Financial Services
Logistics
Internet-of-Things
Cloud-based Systems
Mobile & Web
Data-centric systems

Publications at Top Venues

Top 4 security conferences: 32
Other Core A/A* cybersecurity conferences: 64
Core A*/A cybersecurity journals: 14

Valorization

Industry training
Startups:
Ubizen, Qmedit, Inmanta, VersaSense, intigriti, Elimity

KU LEUVEN

imec

CiTiP

Focus

LEGAL-ETHICAL ASPECTS OF THE DIGITAL TRANSFORMATION OF SOCIETY

Critical Mass in Cybersecurity

20 + members

3 professors

1 innovation manager

Portfolio of Research Projects

35 ongoing projects

of which 26 European research projects

Application Domains

Smart Cities
E-Health
Financial Services
Media
Communications
Transport

Output related to Cybersecurity

7 PhDs since 2014

Cybersecurity Research

Compliance Research
Policy Research
Legal Engineering

Selected Awards

SWIFT Institute
Research Grant 2015

Valorization

Deliver Legal Experts
Training for Industry
Support startup activities

VUB Software Languages Lab

Focus

DESIGN, IMPLEMENT & APPLY BETTER LANGUAGES TO SUPPORT THE SOFTWARE ENGINEERING LIFECYCLE

Critical Mass in Cybersecurity

20 + members
4 professors (2 FTE)

Portfolio of Research Projects

10 ongoing projects
(4 fundamental, 6 strategic)

Application Domains

- Internet-of-Things
- Cyber Physical Systems
- Intelligent Systems
- Industry 4.0
- Big Data

Output related to Cybersecurity

10 PhDs since 2014

Selected Awards

- SANER 2016
- ECOOP 2016
- SCAM 2015
- AITO 2008

Cybersecurity Research

- Secure Programming Languages & Compilers
- Static & Dynamic Analysis of Software
- Dynamic Enforcement of Security Policies

Valorization

- Build software artifacts
- Training
- Support startup activities

UNIVERSITEIT GENT

CSL

Focus

NOVEL ARCHITECTURES AND DESIGN METHODOLOGIES,
NEW SECURITY SOLUTIONS AND SOFTWARE PROTECTIONS,
TOOLS & TECHNIQUES TO AUTOMATE DEPLOYMENT

Critical Mass in Cybersecurity

5 + members
1 professor
1 PostDoc

Portfolio of Research Projects

multiple FWO and H2020

Application Domains

Small Embedded Systems,
Mobile & other Edge Devices

Cloud & Exascale Computing

Output related to Cybersecurity

3 PhDs since 2014

Selected Awards

ICPC 2017
Maurice Wilkes 2017
OOPSLA 2017
FWO - IBM 2016

Cybersecurity Research

Mitigations in multiple attack scenarios, including man-at-the-end attacks, fault injection, time side channels & remote exploits

Design and prototyping of system-level tools such as compilers, operating systems, and runtime systems

Modelling of attacks in support of decision support systems for the users of protection techniques

Valorization

Multiple Bi-Lateral projects with IP transfer

Startup: CoScale

imec

Device Reliability & Electrical Characterization group (DRE)

Focus

FUNDAMENTAL TECHNOLOGY RELIABILITY RESEARCH

Critical Mass in Cybersecurity

12 + researchers

3 Senior Staff, Manager & Scientific Director

Portfolio of Research Projects

Support of imec programmes

4 European Projects (past 5 years)

Application Domains

Low Power Electronics
High Performance Computing
Life Sciences
Automotive
Machine Learning
Quantum Computing

Output related to Cybersecurity

7 PhDs since 2014

Cybersecurity Research

Bringing physical insight into technology related reliability degradation mechanisms

Selected Awards

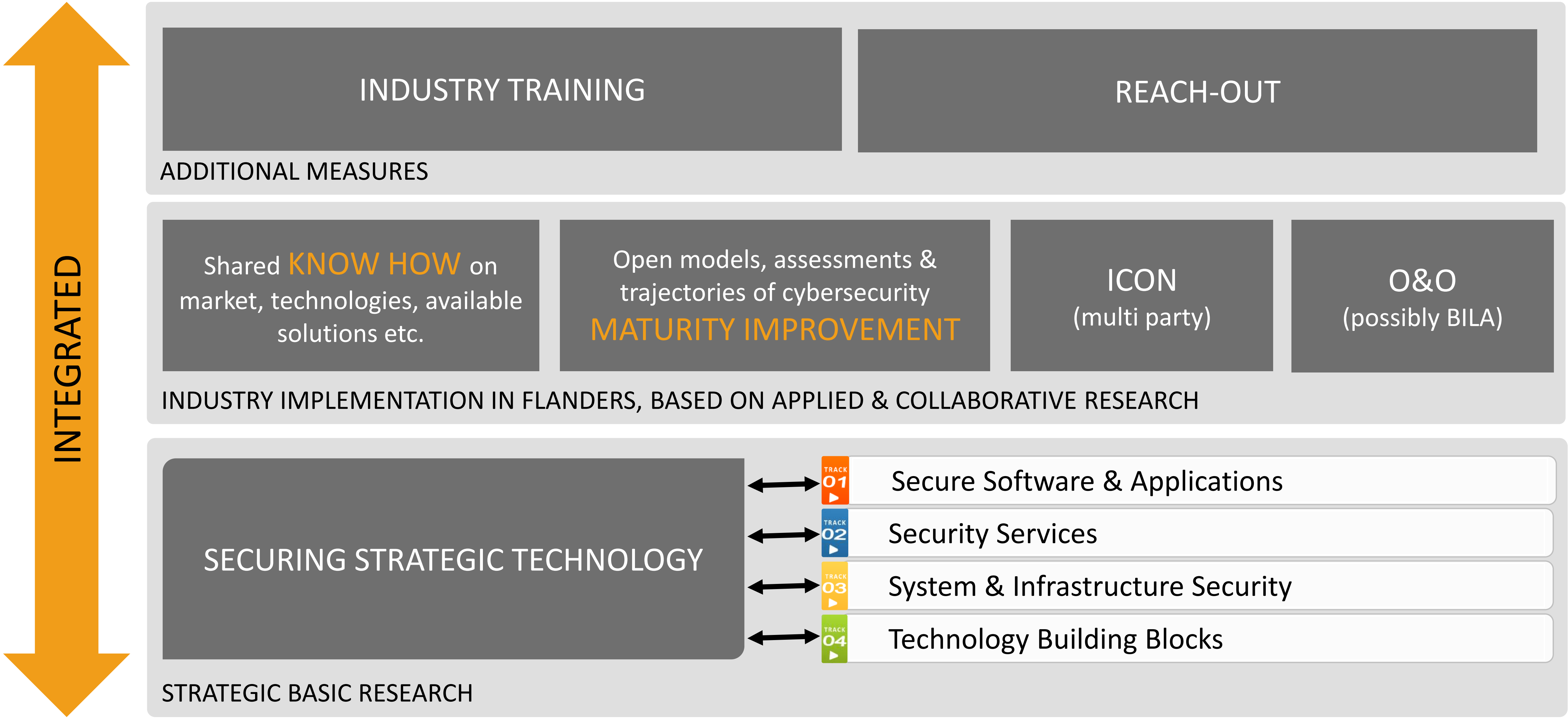
IEEE IRPS 2018
IRPS 2016
IEEE IPFA 2014
IEEE IRPS 2012

Valorization

IP transferred
to various imec partners

Proactive Support

THE OVERALL PROGRAMME – CyberSecurity Flanders



INTEGRATED

INDUSTRY TRAINING

REACH-OUT

ADDITIONAL MEASURES

Shared KNOW HOW on market, technologies, available solutions etc.

Open models, assessments & trajectories of cybersecurity MATURITY IMPROVEMENT

ICON (multi party)

O&O (possibly BILA)

INDUSTRY IMPLEMENTATION IN FLANDERS, BASED ON APPLIED & COLLABORATIVE RESEARCH

SECURING STRATEGIC TECHNOLOGY

TRACK 01 Secure Software & Applications

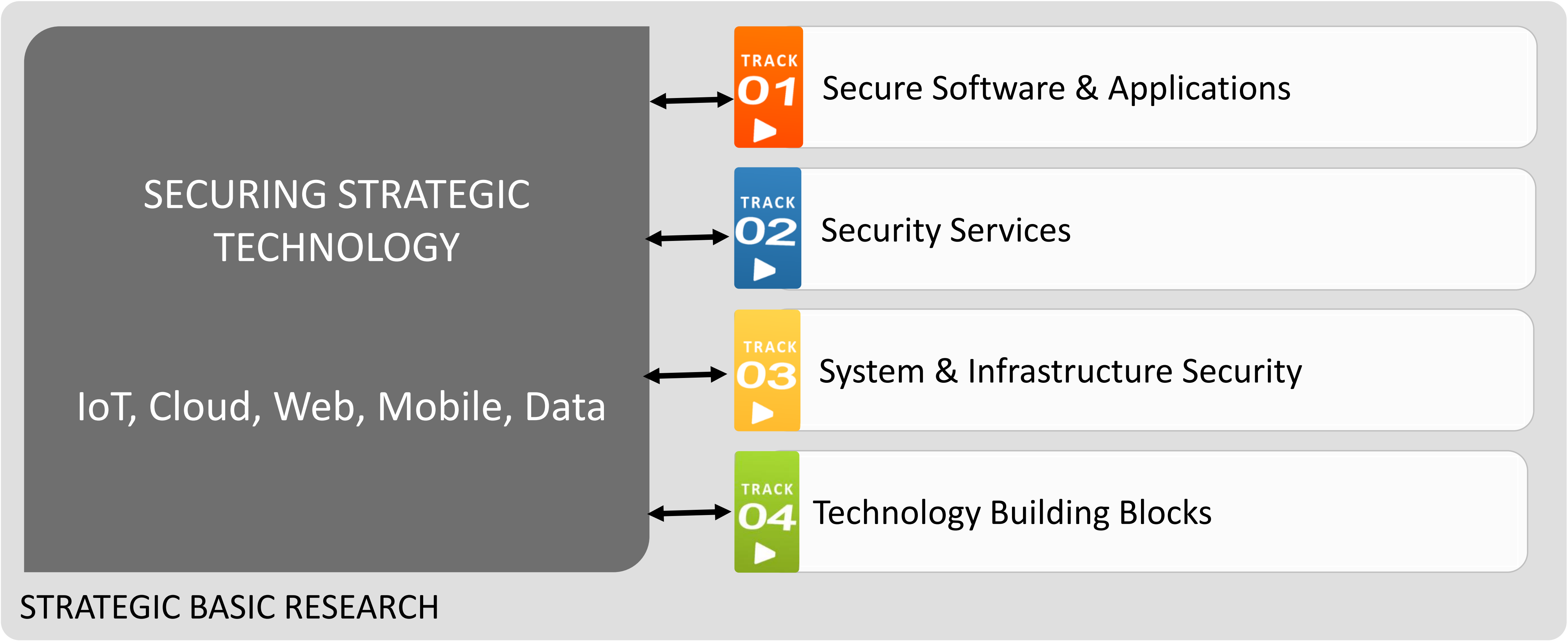
TRACK 02 Security Services

TRACK 03 System & Infrastructure Security

TRACK 04 Technology Building Blocks

STRATEGIC BASIC RESEARCH

Prototypes and environments that combine multiple results



SECURING STRATEGIC TECHNOLOGY

IoT, Cloud, Web, Mobile, Data

TRACK 01 Secure Software & Applications

TRACK 02 Security Services

TRACK 03 System & Infrastructure Security

TRACK 04 Technology Building Blocks

STRATEGIC BASIC RESEARCH

ICON and O&O

Danny De Cock, Bert Lagaisse, Sam Michiels, Svetla Nikova, Dave Singelée, Bjorn De Sutter, Coen De Roover, Peggy Valcke, Els Kindt

Danny De Cock

Bert Lagaisse

Sam Michiels

Svetla Nikova

Dave Singelée

Bjorn De Sutter

Coen De Roover

Els Kindt

COOCK

L-SEC, B-Hive, Sirris, ...

Lieven Desmet, Svetla Nikova

Lieven Desmet

Svetla Nikova

TETRA

Nele Mentens, Vincent Naessens & Stijn Volckaert

Nele Mentens

Vincent Naessens

Stijn volckaert

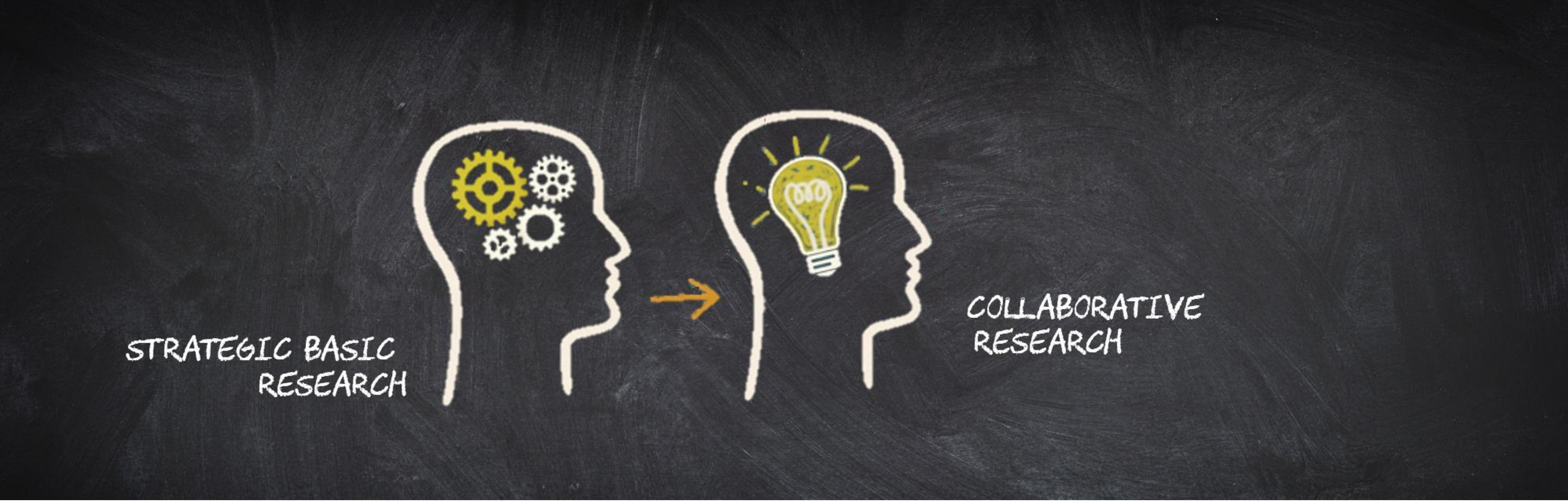
Baekeland

Bart Preneel & Wouter Joosen

Specialized Education and Industry Training

Pieter Philippaerts, Wouter Joosen, Bart Preneel

Pieter Phillipaerts



THANK YOU