



Security Forum 2007 CALIT Symposium

Information Security :
Technology and Design –
Hardware security and
e-health security

Herman E. Maes, IMEC, Leuven, Belgium

25 October 2007 : SAP Lounge Brussels, Belgium



IMEC 1984 - 2007

1984

Established by state government of Flanders in Belgium
Non-profit organization
Initial investment: 62M€
Initial staff: ~70

2007

One of the largest independent R&D organizations in its field, worldwide
Revenue (P&L) : 240M€ (includes 39 M€ grant from government)
16% government/state funding
Staff: > 1500



CALIT 2007 - Information Security 25 October 2007

Mission statement

"To perform research and development, ahead of industrial needs by 3 to 10 years, in microelectronics, nanotechnology, design methods and technologies for ICT systems"

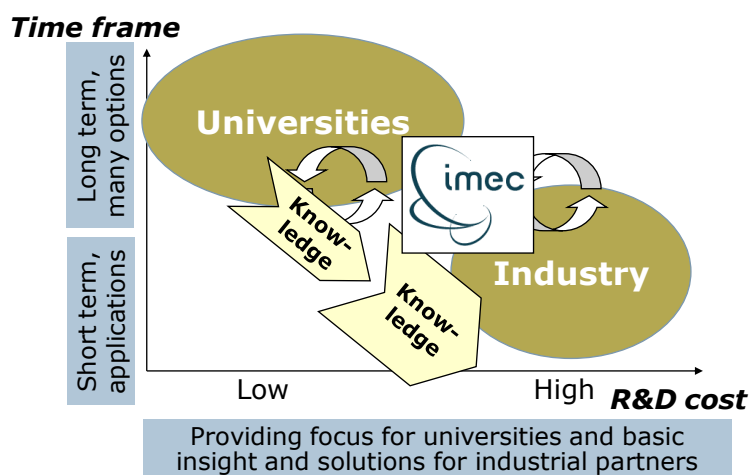
- Performance criteria:
 - **being a worldwide center of excellence**
(total contract revenue, publications, invited papers)
 - **being excellent in exploratory work**
(number of Ph.D.s, projects and publications with universities)
 - **with impact on local industry**
(new spin offs, collaborations, training)



imec

CALIT 2007 - Information Security 25 October 2007

IMEC as a "Transformer"



imec

CALIT 2007 - Information Security 25 October 2007

Center for Advanced Learning in Information Technologies (CALIT)



Center of Advanced Learning in Information Technologies (CALIT)

Platform for high-level Events and Training Programs

- ▣ visionary and interdisciplinary in nature
- ▣ complementary to most academic offerings.

What ?

- ▣ selected number of themes of high importance
- ▣ visionary symposiums, brainstorm sessions and summer schools.

Target groups

- ▣ managers
- ▣ policy-makers
- ▣ scientists
- ▣ practicing engineers.

imec

CALIT 2007 - Information Security 25 October 2007

Center for Advanced Learning in Information Technologies (CALIT)



Themes and Events in 2006 :

Convergence of sciences at nm-scale

14 and 15 September 2006 : CALIT Symposium and Workshop on 'Valorization in medicine and healthcare'

2-3 October 2006 : Biology for Engineers (Basic)

4-7 October 2006 : Bio-Sensor Technology for Engineers

Information Security

18 October 2006 : CALIT Workshop "Challenges for Information Security"

19 October 2006 : CALIT Symposium "System Security and Privacy"

20 October 2006 : L-SEC Symposium "Technology meets Business"

Heterogeneous Integration Systems

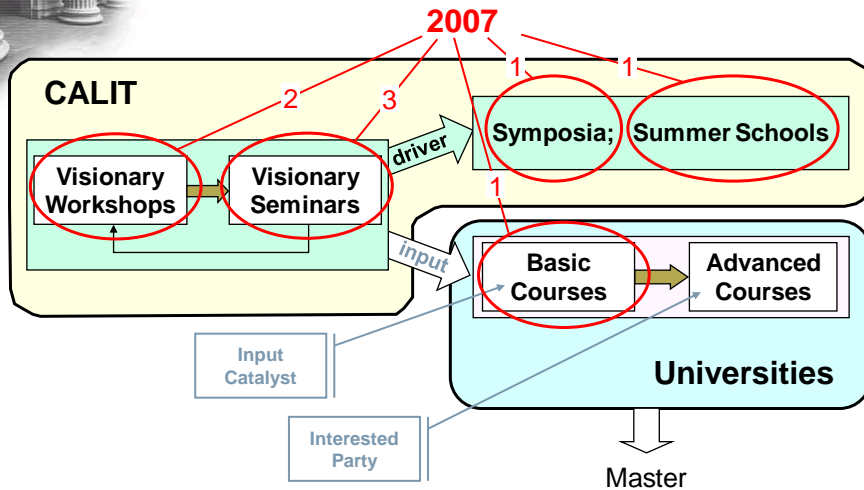
10 November 2006 : CALIT Symposium on 'Reliability in future SoCs – can Technology-Aware Design help?'

imec

CALIT 2007 - Information Security 25 October 2007

Center for Advanced Learning in Information Technologies (CALIT)

2007 : fourth year of CALIT



imec

CALIT 2007 - Information Security 25 October 2007

Center for Advanced Learning in Information Technologies (CALIT) 2007

Themes and Events in 2007 :

Convergence of Sciences at nm-scale

13 and 14 September 2007 : CALIT Symposium on "Nano meets Micro : addressing needs in Microsystem Technology for Biology and medicine using Nanotechnology"

12-13 November 2007 : Basics of Biology for Engineers

14-16 November 2007 : Bio-Sensor Technology for Scientists and Engineers

Information Security

24 October 2007 : CALIT Workshop on : Hardware and e-Health security"

25 October 2007 : CALIT Symposium on "Information Security : Technology and design solutions"

Heterogeneous Integration Systems

12 November 2007 : CALIT Workshop on "Domain specific technologies : opportunities and challenges?"

13 November 2007 : CALIT Symposium on "Can (system) design(-ers) influence technology?"

imec

CALIT 2007 - Information Security 25 October 2007

CALIT- Herman Maes 24-25 October 2007



Previous CALIT Symposia on Information Security

The first CALIT event on Information Security (IMEC, Leuven, 19 May 2005) was about "Security in embedded systems, ambient technology and beyond"

This second CALIT event on Information Security (Crowne Plaza, Brussels, 19 October 2006, embedded in the Security Forum 2006) dealt with "Systems Security and Privacy"

imec

CALIT 2007 - Information Security 25 October 2007

The 3th CALIT Symposium on Information Security (embedded in the Security Forum 2007)

Information Security: from Hardware to Applications 25 October 2007

- As we rely more and more on information system, information security touches our lives on a daily basis. In the PC world, we need to deal with malware (viruses, worms, Trojan horses and spyware), phishing attacks, botnets and SPAM. In spite of this environment, we buy things on the web, use electronic banking systems and make mobile and VOIP phone calls; these applications use sophisticated security solutions to protect us.
- As the complexity and scale of systems grow and the integration of hardware and software progresses, security solutions need to be implemented at multiple layers to offer defence in depth; the implementation of security in small embedded systems and hardware presents new opportunities but also new challenges.
- Three well known researchers introduce us to **innovative security solutions at the hardware level**: anti-counterfeiting technology, secure non-volatile memory and new low-cost security protocols for RFID tags.
- In the area of advanced applications, leading players discuss the challenges of critical components such as non-volatile memories and the issues related to remote monitoring and treatment of patients in an e-health environment.

imec

CALIT 2007 - Information Security 25 October 2007

CALIT Information Security Workshop 2007

24 October 2007
The Lodge, Leuven, Belgium
Visionary Workshop

“Information Security : Hardware security and e-Health Security”

Discussion Panels :

- Hardware Security
Moderator : Prof. Ingrid Verbauwhede
- e-Health Security
Moderator : Prof. Bart Preneel

- Conclusions of the CALIT Workshop 24.10.2007
Prof. Bart Preneel, 4.40pm

imec

CALIT 2007 - Information Security 25 October 2007

Security Forum 2007 (25.10.2007)

CALIT Track (Visionary and technology tracks)

9.00am

Opening and Introduction

*Ulrich Seldeslachts, L-Sec, Belgium
Herman Maes, IMEC, Belgium*

9.10am

SIM card and handset forensics

David Naccache, ENS, France

10.00am

Anti-Counterfeiting Technology based on Physical Unclonable Functions

Pim Tuyls, Philips Research, The Netherlands

10.50am

Coffee Break

11.05pm

How to SQUASH your data : provably Secure and Lightweight cryptography for RFID tags

Adi Shamir, The Weizmann Institute, Israel

12.00am

Lunch

1.00pm

Secure non-volatile memory : is it a new trend for the security of embedded systems?

Guido Marco Bertoni, ST Microelectronics, Italy

1.50pm

Remote monitoring of people at risk and remotely supervised treatments

Hermie J. Hermens, University of Twente, The Netherlands

2.40pm

Coffee Break

3.00pm

HPLabs Trusted Systems Lab & HP Security Office

Graeme Proudler, HP Laboratories, UK

3.50pm

Security threats on IPv6

Eric Vyncke, CISCO, Belgium

4.40pm

Conclusions of CALIT Workshop of 24 October 2007

Bart Preneel, COSIC, KULeuven, Belgium



CALIT

imec

CALIT 2007 - Information Security 25 October 2007