JESI

Joint European Security Initiative

Klaus Kinzinger, Kinzinger Automation
Alexandre Petrescu, CEA LIST

SCCT

Secure Computing Core Technology

A non-NDA Teaser

Intro

There exists a clean solution
for the problem of cybersecurity. It is

- straightforward, clear,
- complete, formally provable and thus
- qualifies for **certification** according to the highest IT security standards

JESI SCCT will supply this solution to the IoT, Industry 4.0 and critical infrastructures market. This technology will be used by everyone who builds mission critical systems of any kind.

Objectives

General purpose, fully scalable processor IP with

1. Certified and reliable **cybersecurity**
   (task level security features guaranteed by HW)

2. Certified and reliable **safety / protection** of
   - control flow – CFI (programs cannot crash)
   - memory access (smart pointers in HW)

3. Superior **energy efficiency** and performance

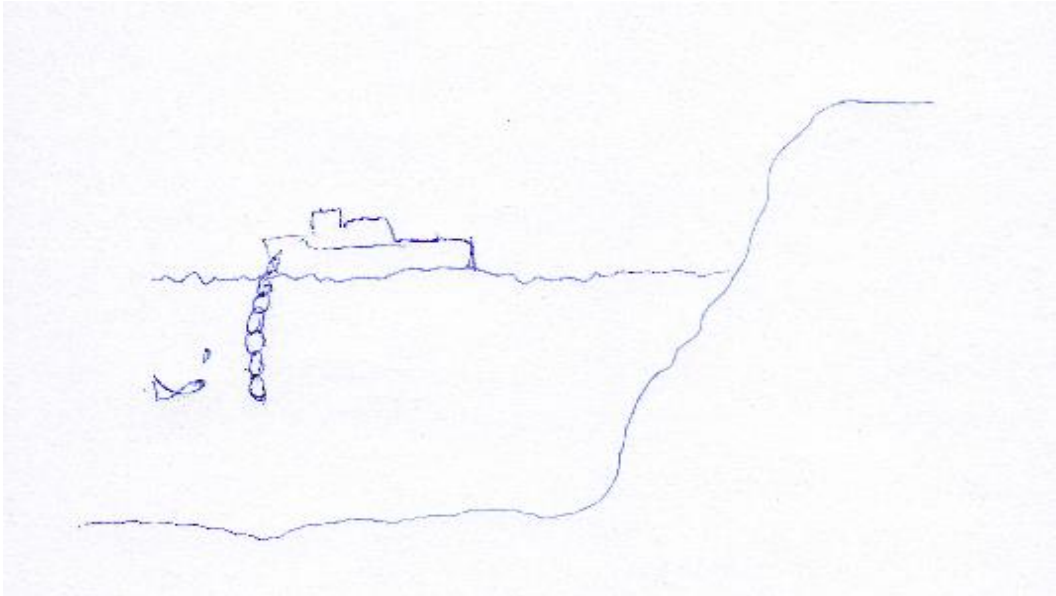
Basics

- IT security is an architectural feature and no add-on. One can not mount or reliably glue it onto hardware that by design has no support for it (von Neumann)

- A major technology leap is needed that ought to start with critical infrastructures and then should expand into the mass markets

- For economic reasons, in the mass markets energy efficiency is paramount for success

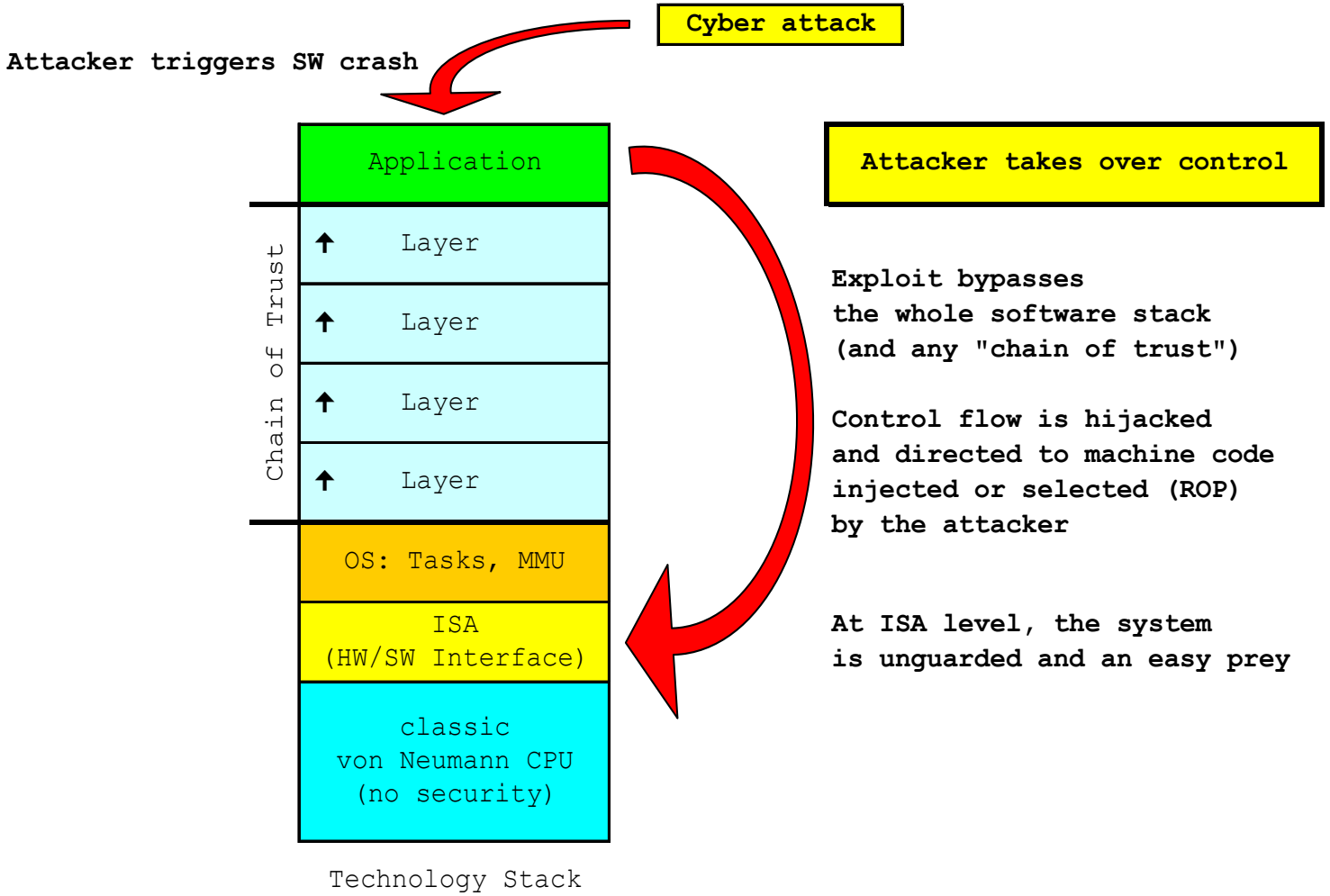
Chain of Trust ?



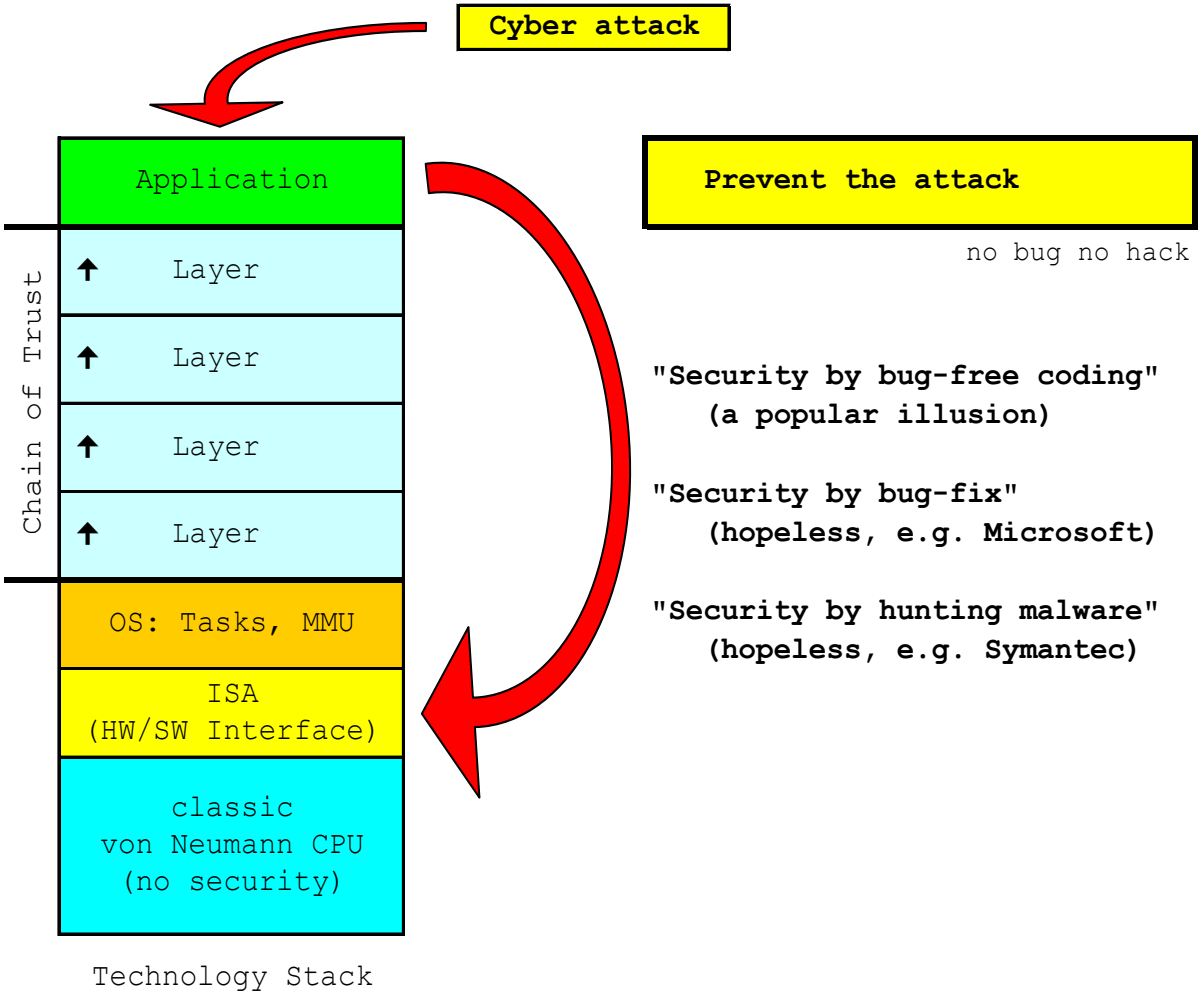
IT security can not exist
without proper hardware anchoring

It never has and never will

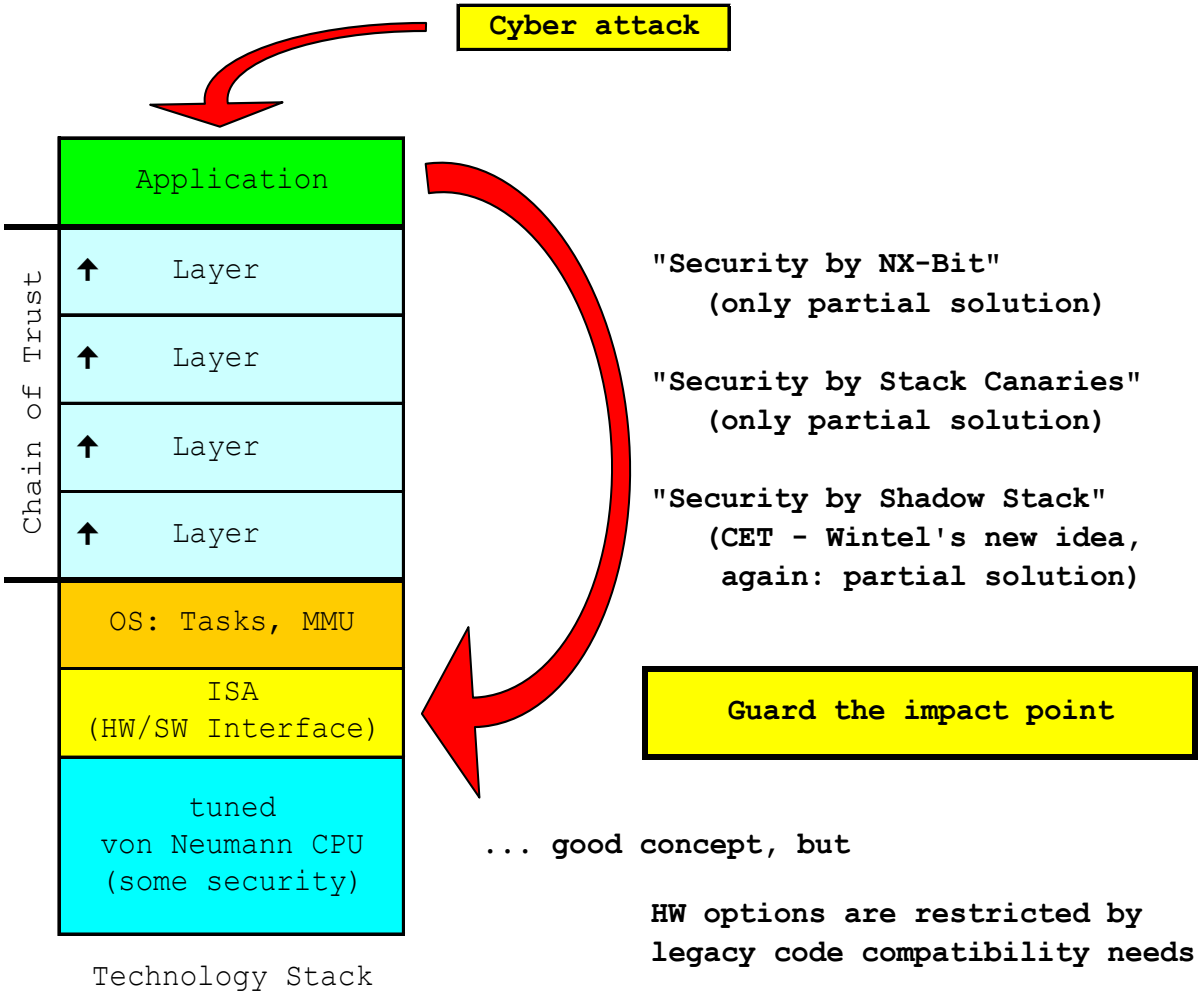
Exploit of a SW Bug



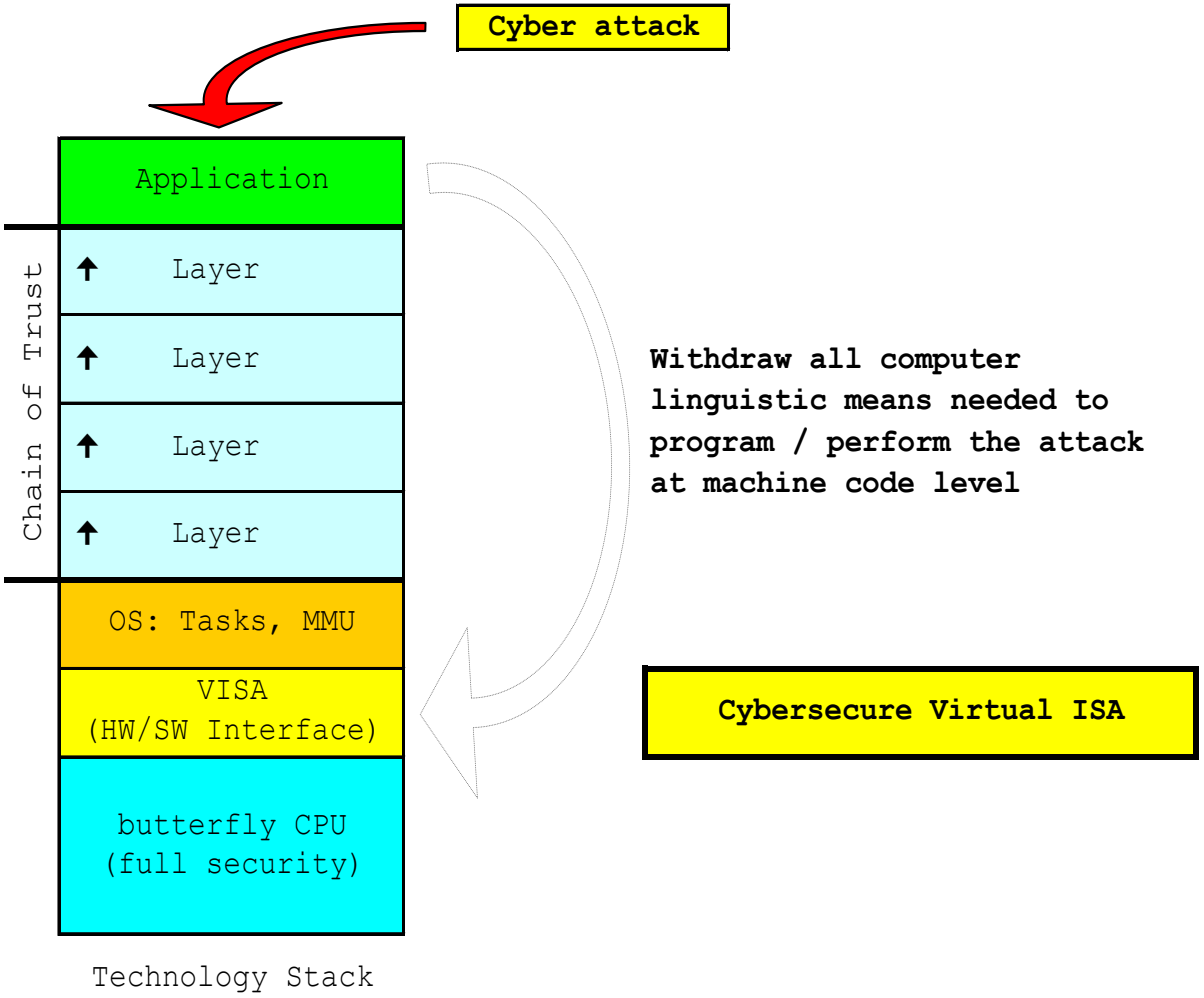
Cyberdefense – Option 1 – Quality Assurance



Cyberdefense – Option 2 – VNA Tuning



Cyberdefense – Option 3 – Secure ISA



JESI

Joint European Security Initiative

www.jesi-initiative.eu
Klaus Kinzinger, Kinzinger Automation
Alexandre Petrescu, CEA LIST
v31, February 7th, 2017

Mission – European Secure ICT Standard

JESI develops a new cybersecure processor type

Based on a solid theoretical framework, its novel computing core IP, OS components, algorithms, and communication protocols define a future **European Secure ICT Standard** providing reliable cybersecurity against

- all kinds of malware, ransomware, viruses, worms, and Trojan horses that exploit coding errors, and
- most types of backdoors and key escrow implanted into SW or HW by non-EU manufacturers

Main Use Cases

Based on the results of the JESI foundation project **SCCT** – Secure Computing Core Technology – three JESI *subprojects* implement use cases of primary interest

SVCT Secure Vehicular Communications Technology (networked environments in car / train / aircraft, and in stationary communications infrastructures)

SIAT Secure Industrial Automation Technology (Industry 4.0, IoT, "secure PLC" and so on)

SHPC Secure High Performance Computing (data center & cloud computing)

Timeline

Cybersecurity at highest JESI level is urgently needed to protect people, nations, and industries around the world from the impact of cyber espionage, sabotage, warfare, and terrorism. It is also vital for future digitalisation projects like **Industry 4.0** and **IoT**

JESI is therefore planned to deliver **ASAP**

- **April 7th, 2017 – submission to Celtic-Plus**
- June 2017 – Celtic-Plus Label
- September/October 2017 – Project start
- 30 Months – Duration. Results: prototypes

Partner per type per country per subproject

France

AKKA	IND	SVCT
Bertrandt	IND	SVCT/SHPC
CEA	RTO	SVCT
INRIA	RTO	SVCT
ESIEE	Uni	SVCT
Eurecom	RTO	SVCT
Montimage	SME	SVCT
Quirinus	SME	SVCT/SHPC
YoGoKo	SME	SVCT

Germany

Kinzinger	SME	SCCT
FZI	RTO	SCCT
TUD	Uni	SCCT
KIT	Uni	SIAT
HAW	Uni	SCCT

Spain

Ficosa	IND	SVCT
Innovalia	RTO	SVCT
Eneo	SME	SVCT
Nextel	SME	SVCT
SQS	SME	SVCT
Ikusi	SME	SVCT
UAB	Uni	SCCT/SHPC

South Korea

SW Mobile	SME	SVCT

Belgium

IMEC	RTO	SCCT
KU Leuven	Uni	SCCT

Romania

Beia	SME	SVCT

Austria

F-AR	RTO	SIAT
JKU	Uni	SCCT
Yagoba	SME	SCCT

Benefits for JESI Industry Partners

JESI is bound to cause a **major disruption** of all mission critical ICT markets because ...

ICT operators in critical application domains will run legal **liability risks** in case of damage or casualties caused by standard insecure ICT – as soon as secure solutions are available on the market they may be held legally accountable for **not** using them

For JESI industry partners, this additional legal aspect is a winning game. They will be first in the evolving high security ICT market and benefit from more than two years technology lead in the SVCT, SIAT, and SHPC domains

Call for Industry Partners

LE partners with the following profiles / roles are sought:

- Automotive, train, avionics manufacturers or their component suppliers, e.g. SEAT, Bosch, Thales, Airbus
- Industrial automation suppliers with specific interest in Industry 4.0 and IoT, e.g. Siemens, Bosch, ABB
- Industry partners looking for strategic investment into an European ARM-like technology IP provider

Events / Website / Coordinators

Events

- Regular telephone conference for partners and newcomers each second Friday 10am - 11:30pm CET
- Next **SCCT telco presentation & tech discussion** on Tuesday 28th 2 - 5 pm CET (**NDA** is required for this event, please ask the coordinators)

Website

- cloud.kinzinger.com:
  JESI presentation, documents, member forum

JESI coordinators, preliminary:

- Alexandre Petrescu, alexandre.petrescu@cea.fr
- Klaus Kinzinger, kinzinger@kinzinger.de