RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

Trusted Computing for Embedded Systems - Challenges in a Changing World

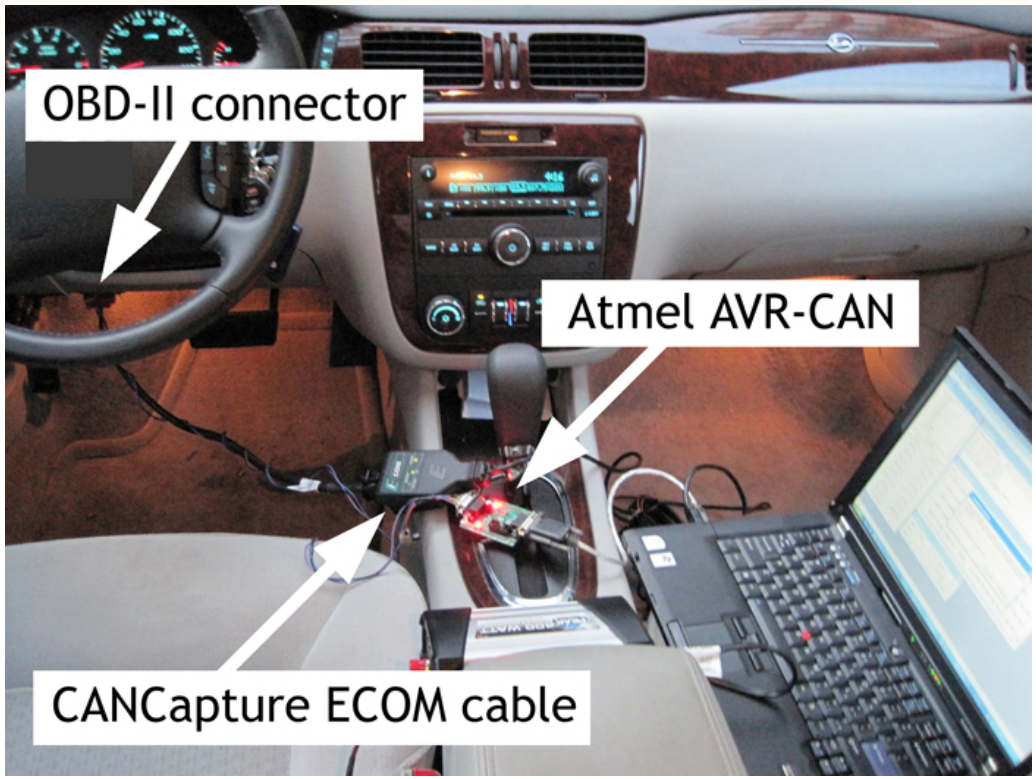
Joerg Borchert
Infineon Technologies

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

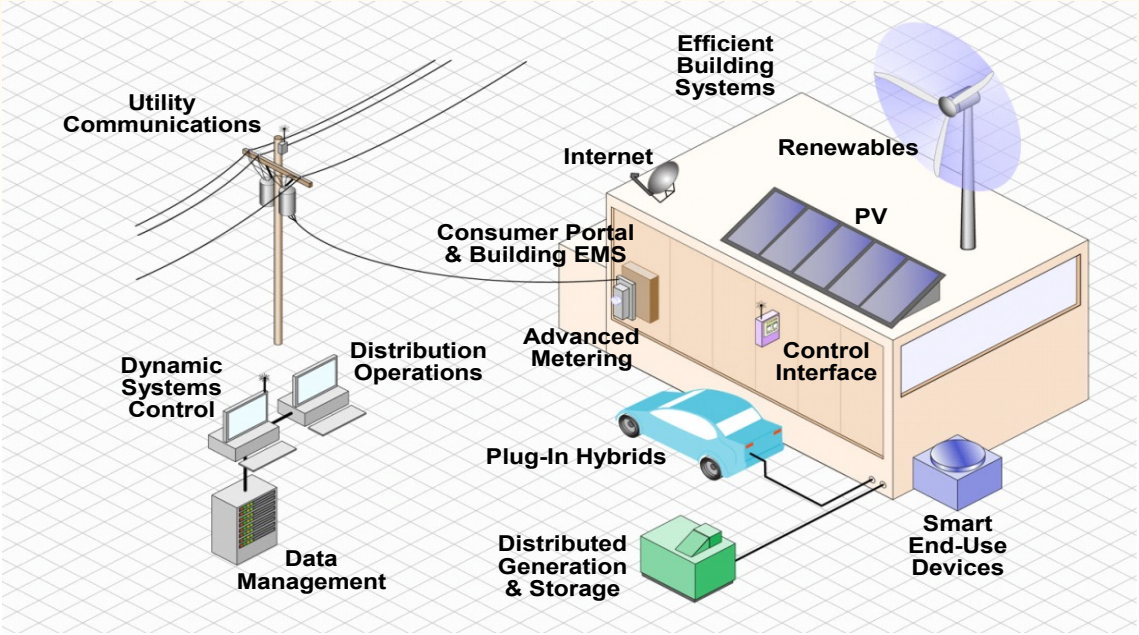
Agenda

- **Rising threat**
  - **Embedded systems at risk**
  - **Lessons from computing ecosystem**
- Counterstrategies
  - Understanding attacks
  - Learning from biology
- Evaluating risk

Embedded Systems at Risk: Hacking into Autos



Embedded Systems at Risk: Attacking the Smart Grid



- Threats from:
  - Connectivity, upgradability
  - Cost pressure

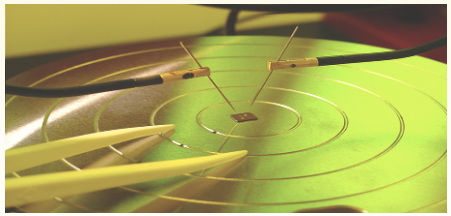
Lessons from the PC Ecosystem

- Networks…the unavoidable risk
- Traditional defenses revolve around
  - Access control
  - Monitoring traffic
- Next level defense built on “root of trust”
  - Trusted Execution only valid with security hardware (i.e., TPM)

Agenda

- Rising threat
  - Embedded systems at risk
  - Lessons from computing ecosystem
- **Counterstrategies**
  - **Understanding attacks**
  - **Learning from biology**
- Evaluating risk

3 Classes of Hardware Attack

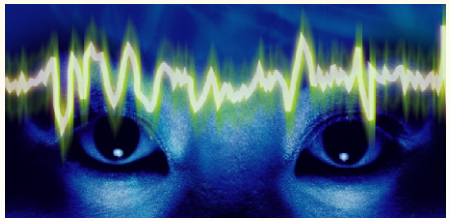


Manipulating

Development:
Months

Execution:
Days
> 100.000 €

Example:
Microprobing



Observing

Development:
Days

Execution:
Hours
> 10.000 €

Example:
Power Analysis

Semi-Invasive

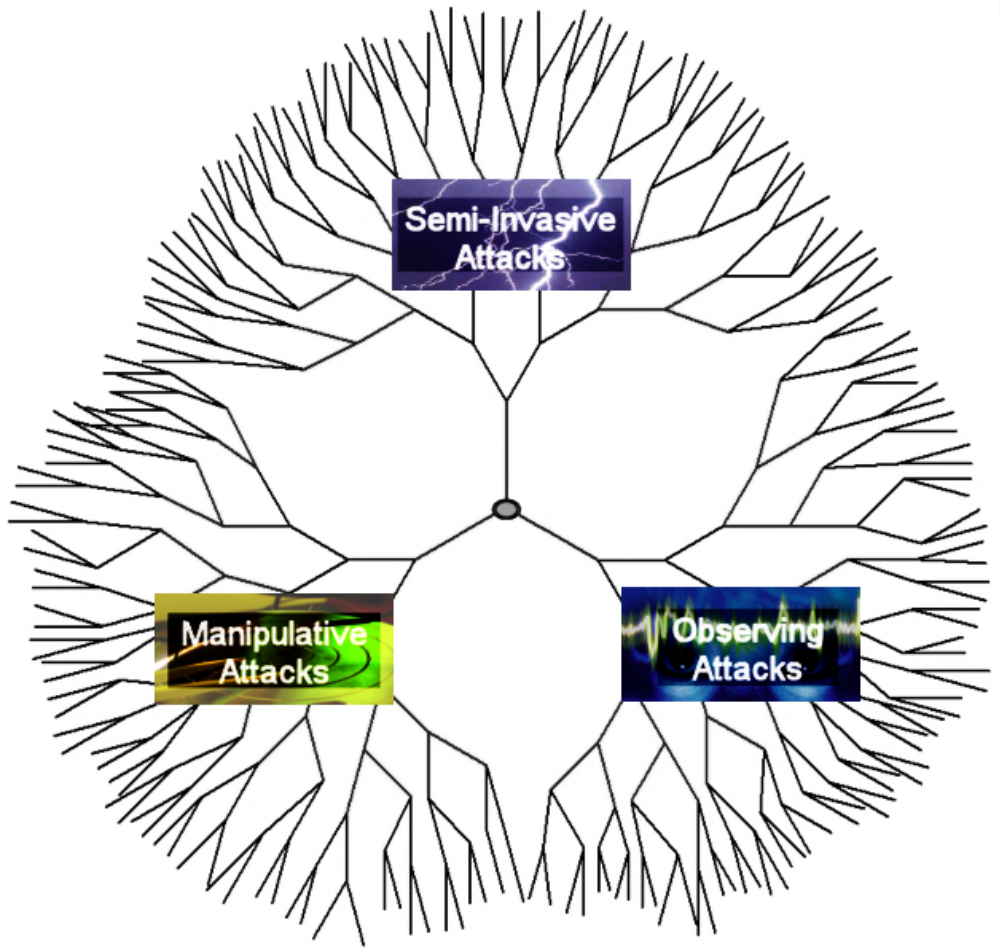
Development:
Months

Execution:
Minutes
> 100 €

Example:
Spike Attack

The attack classes require different investments and expertise. This also divides the groups of attackers from amateurs to professionals.

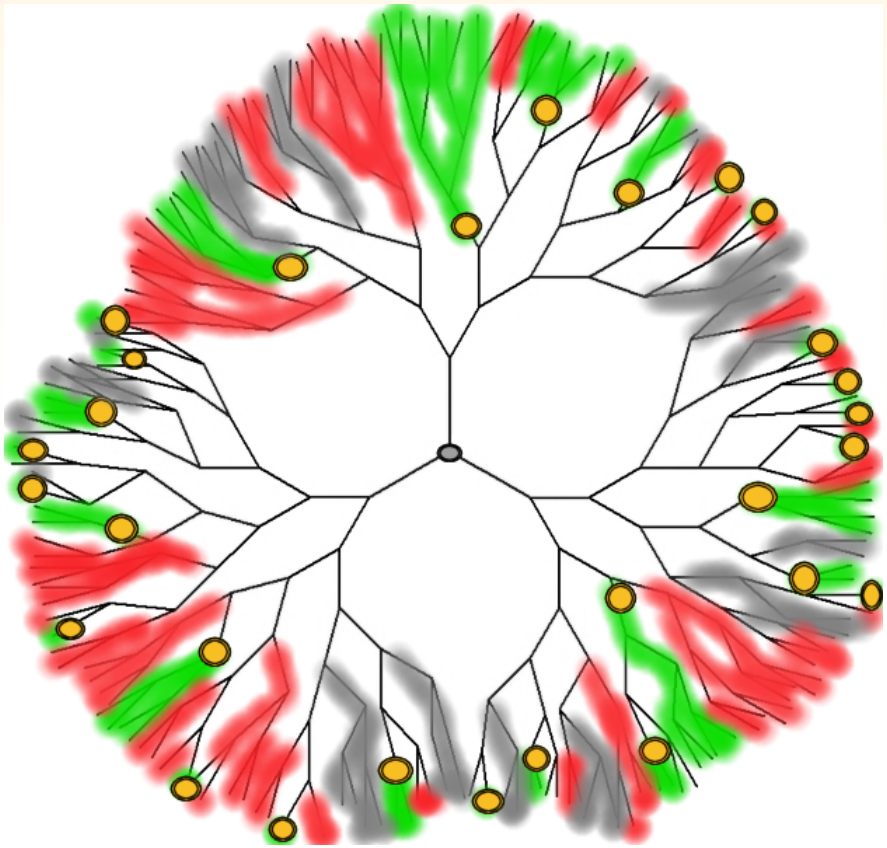
Analyzing Attack Classes



- Each attack class has unlimited # of scenarios
- Evolution of attacks is constant

Conventional Defense: Scenario Focused

RSA CONFERENCE CHINA 2012



Countermeasure

Protected

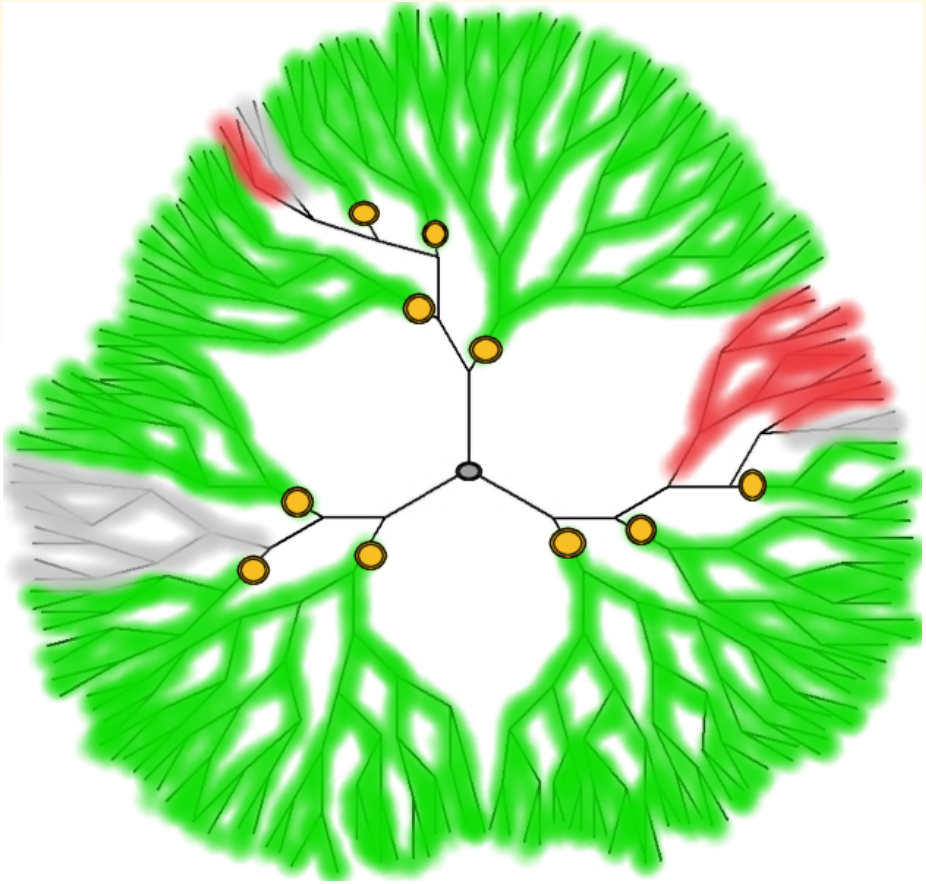
Not Protected

Not Tested, Unknown

Typical countermeasures target only small attack subsets.

Many countermeasures are needed, many weaknesses remain.

New Defense: A Comprehensive Approach



Countermeasure

Protected

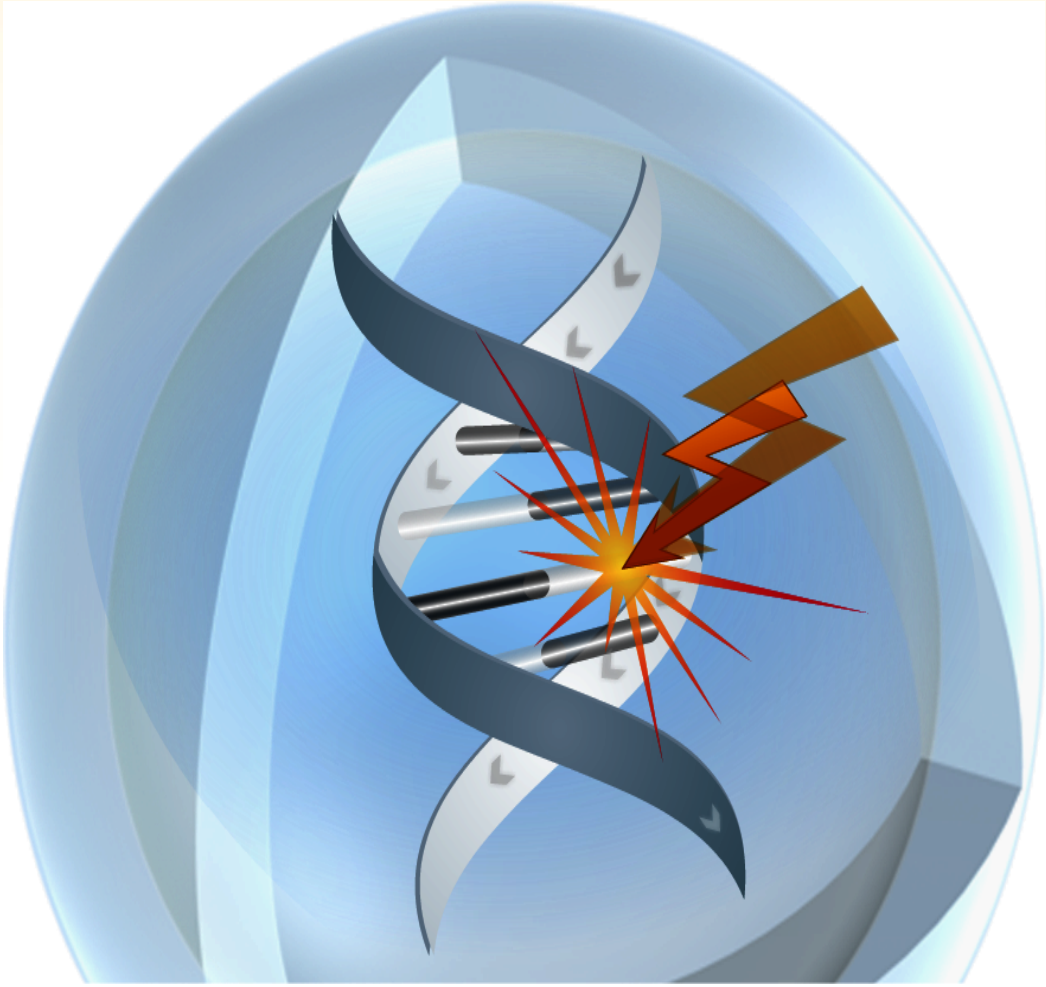
Not Protected

Not Tested, Unknown

Comprehensive countermeasures target complete attack groups.

Fewer countermeasures are needed, risks can be easily evaluated.

Security Inspired by Biology



- Cells act as secure computers with robust defense to manifold attacks
  - Protected data storage and processing
- Security IC can be emulate natural mechanisms
  - Self checking
  - Fully-encrypted processing

Key Hardware Security Concepts

- Complete shift from analogue to digital security
- Consider entire attack classes, not millions of single attack variants
- Integral security is comprehensive and must not hinder functionality
- Rely on detection of effects instead of detection of cause
- Secure products must be rugged
- Security must be easy to use

Agenda

- Rising threat
  - Embedded systems at risk
  - Lessons from computing ecosystem
- Counterstrategies
  - Understanding attacks
  - Learning from biology
- **Evaluating risk**

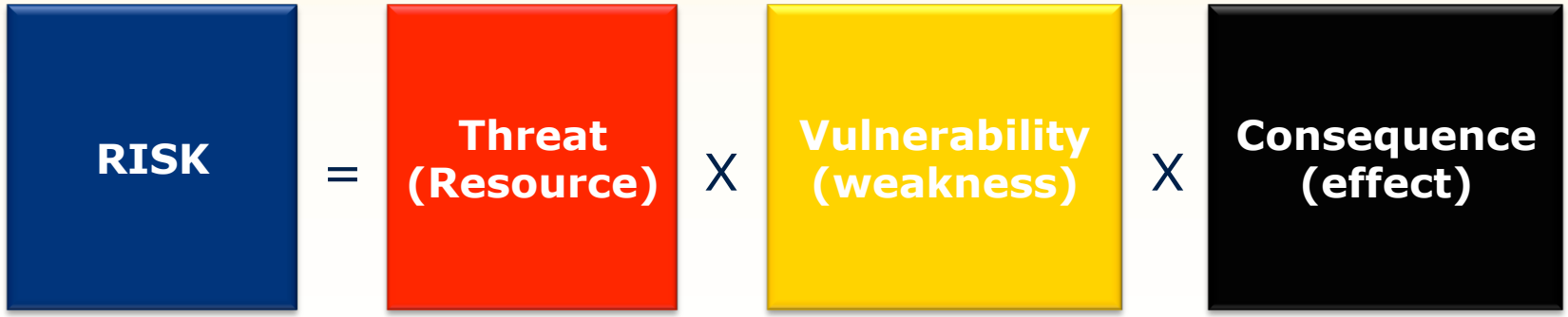
Building Defenses: Organizational Issues

- Cost
- Outsourcing, distributed responsibility
- Design philosophies

The Cost of Security: Calculations

RSA CONFERENCE CHINA 2012

Risk Analysis



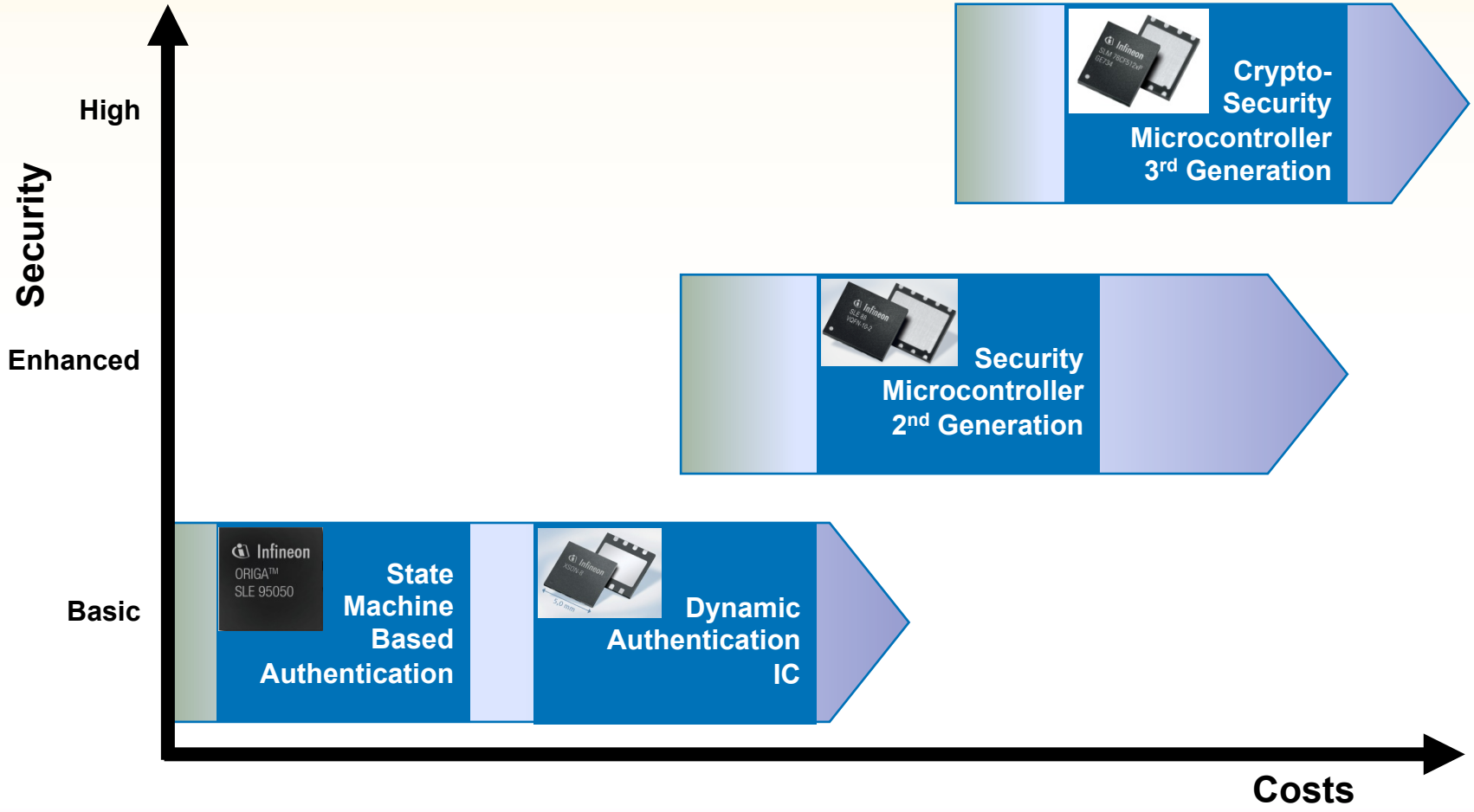
Economics

Investment in Security is an Insurance

Risk Based Options

- Software Security
  - Virtualization
  - Sandbox Models
- Hardware Security
  - Trusted Execution Environment
  - Security IC as Root of Trust

Hardware-based Security: Investment



Security Root of Trust

- The Security IC
  - Establishes an expectation of behavior
  - Cryptography is a method but not sole purpose
- Attestation is the foundation for trust. Attest before we:
  - release the memory encryption key
  - allow it on the corporate network
- The security IC uses cryptographic means for attestation and identity

Role for Standards

- Standard hardware Root of Trust is basis for successful worldwide deployment
  - Global market gains confidence in system integrity
- Trusted Computing Group provides structure to establish international standard
  - Building from work on PC TPM to define hardware security for embedded systems

Summary

- Embedded systems are valuable targets for attack
- Principles of trusted computing can be applied to embedded systems
- Countermeasures should work on complete classes of attacks, not only on specific single attack scenarios
- Paradigm shift from analog to digital security is necessary for long-living security
- Security Controllers with fully encrypted data path and full error detection are a reality today as root of trust
- Security in HW and SW is an insurance case from an economics viewpoint

Thank You

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012