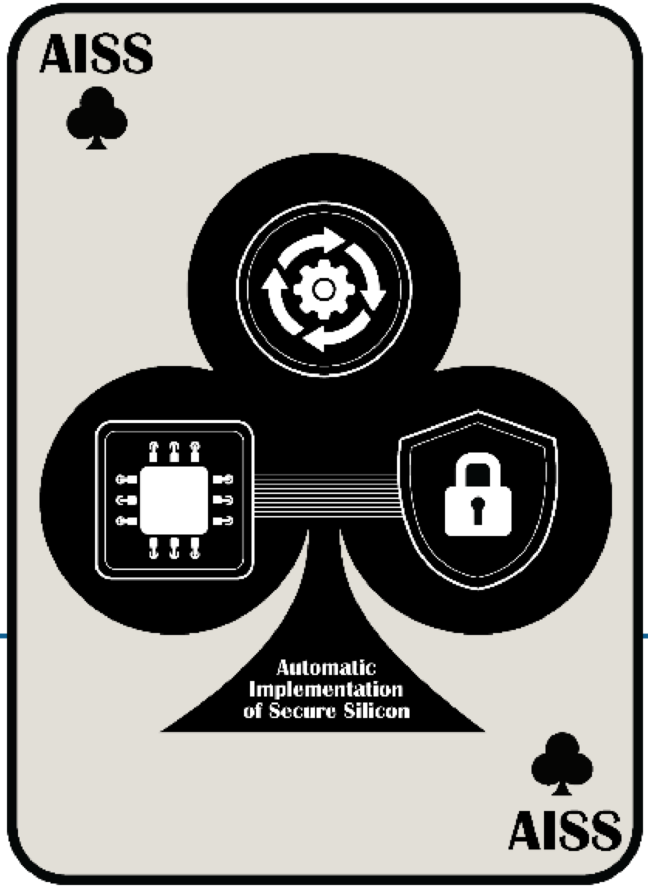


AISS Overview

Serge Leef

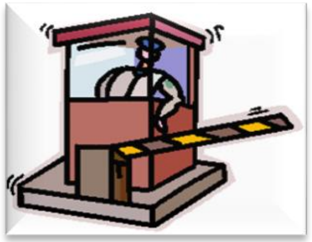
ISART

Aug 11, 2020

Goal

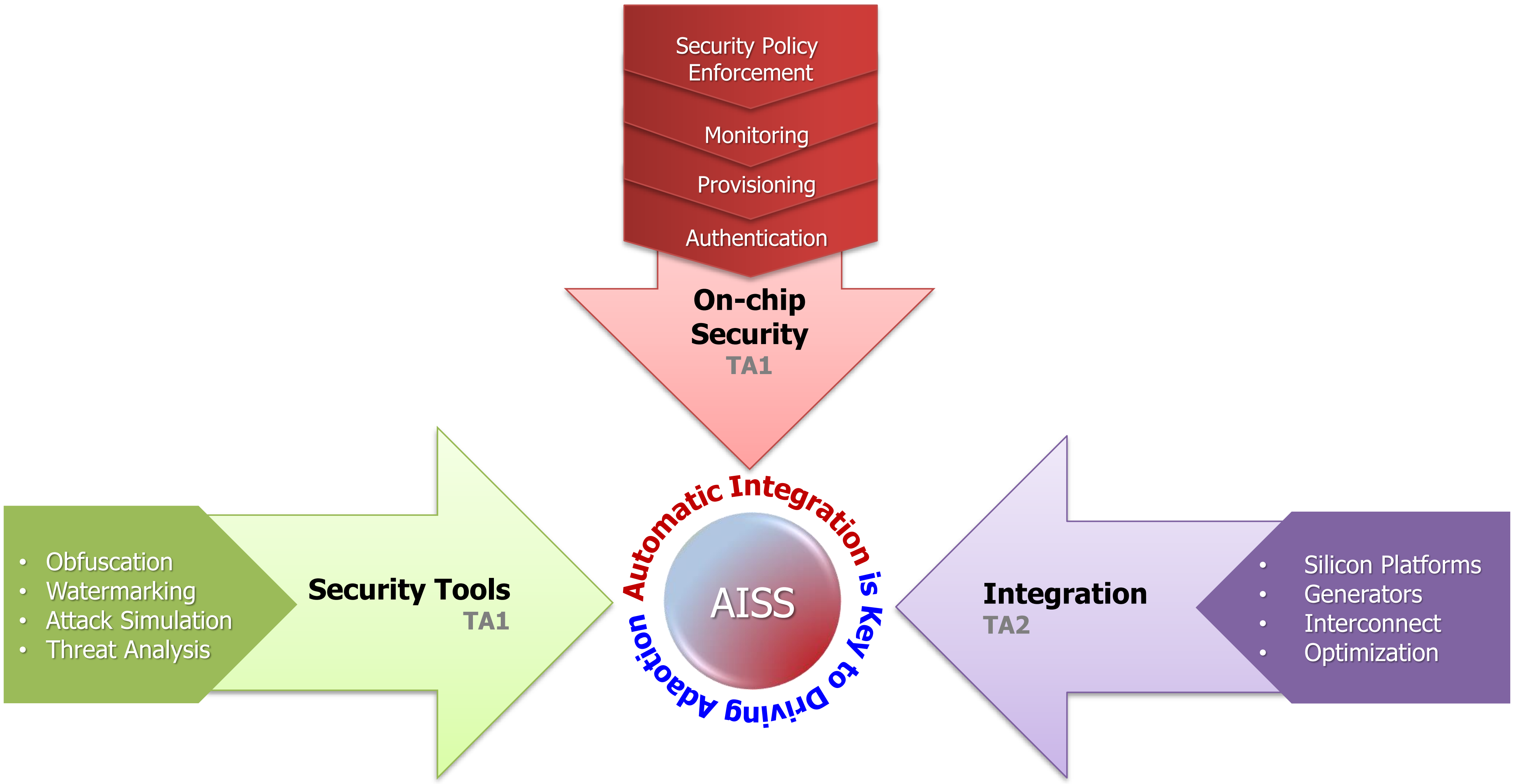
Automate inclusion of scalable defense mechanisms into chip designs to enable security vs. economics optimization

Cost and Complexity of Attack Resistance Mechanisms →

Source: shutterstock.com

AISS: Program Structure



AISS Will Democratize Chip Security through Automation

Attack Surface Based Reference Model

Software

Hardware Software Interface

Hardware

Moving Target (I20)

- Substantial efforts are on-going in the software community

In Progress (SSITH)

- Alteration of system behavior based on software-accessible points of illicit entry that exist due to hardware design weaknesses or architectural flaws

AISS Focus Areas

- **Side Channel** – extraction of secrets through physical communication channels other than intended (assumption: attackers are able to "listen" to emissions)
- **Reverse Engineering** – extraction of algorithms from an illegally obtained design representation (assumption: attackers have access to design files)
- **Supply Chain** – Cloning, counterfeit, recycled or re-marked chips represented as genuine (assumption: attackers can manufacture perfect clones)
- **Malicious Hardware** – insertion of secretly triggered hidden disruptive functionality (assumption: attackers successfully inserted malicious function(s) into the design)

Security Strategies by Company type

Huge merchant semiconductor companies *(Intel, Broadcom, Qualcomm…)*

- See the critical need and have large expert teams to create custom solutions

Reduce Effort

Mid-size semiconductor and system companies *(NXP, Cisco, Nokia…)*

- Recognize problems but lack expertise and sufficient economic motivation

Defense contractors *(Honeywell, NG, Lockheed…)*

- Possess deep, but limited, expertise (craft) unevenly applied to specific chips

AISS TARGET AREA

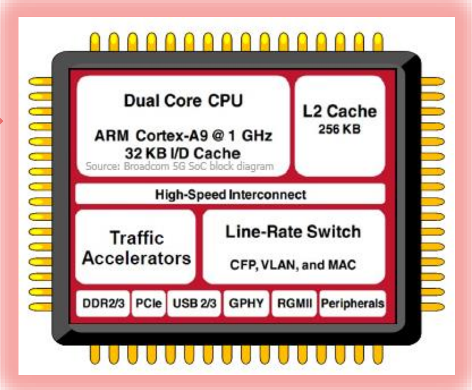
Reduce Cost

System integrators *(Ring, Fitbit, August…)*

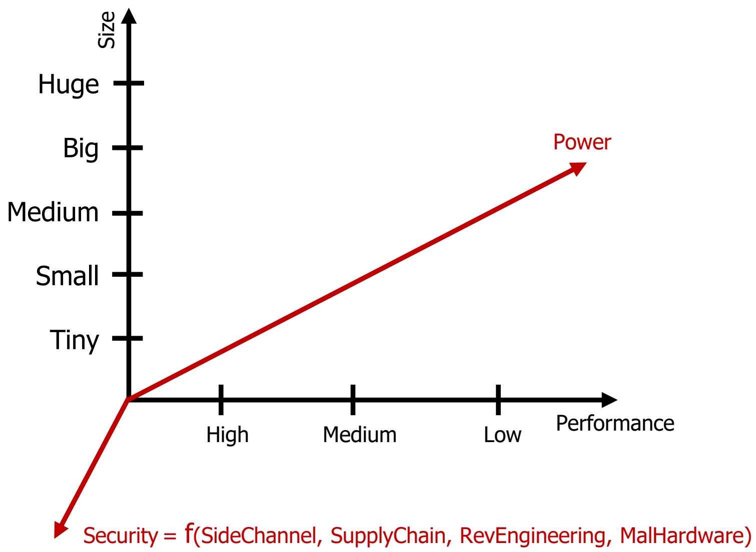
- No interest due to time-to-market focus and lack of in-house competency

Long Term EDA Dream: **System Synthesis**

<u>System</u> synthesis & optimization



1. Σ(a***Performance**, b***Size**)
2. Σ(a***Performance**, b***Size**, c***Power**)
3. Σ(a***Performance**, b***Size**, c***Power**, d***Security**)
4. Σ(a***Performance**, b***Size**, c***Power**, {d***SideChannel**, e***SupplyChain**, f***RevEngineering**, g***MalHardware**})



Key challenges:

- *Quantification of security*
- *Rapid estimation of attack resistance*
- *Multi-dimensional optimization*

(source: Broadcom)

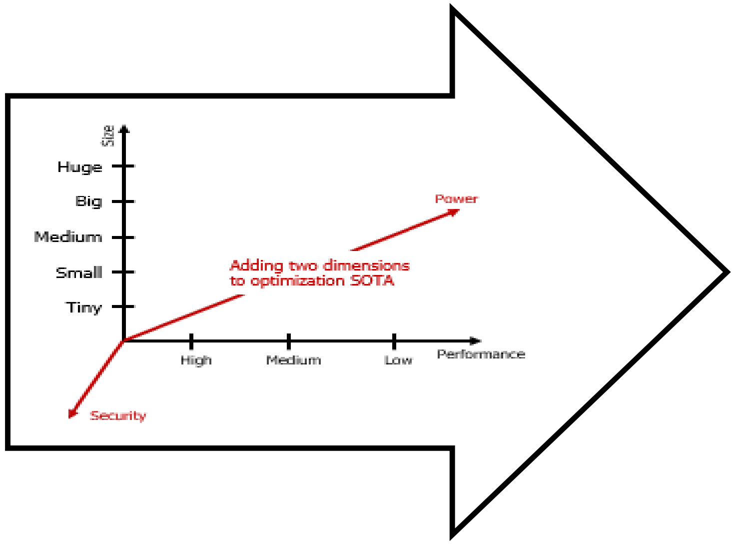
AISS: Optimized Composition

- User selects a platform and supplies a cost function with size, performance, power and security goals to guide combinatorial optimization to find **best architectures** which are presented to the user for assessment and selection

Design: "Power Doors/Windows ECU"

Platform (Automotive Control)

- Performance = 2
- Size = 9
- Power = 3
- Security = 3
  - Supply Chain = 7
  - Side Channel = 2
  - Reverse Engineering = 5
  - Malicious Hardware = 1



Combinatorial Optimization explores HUGE solution spaces (billions), but requires rapid estimation of "goodness"

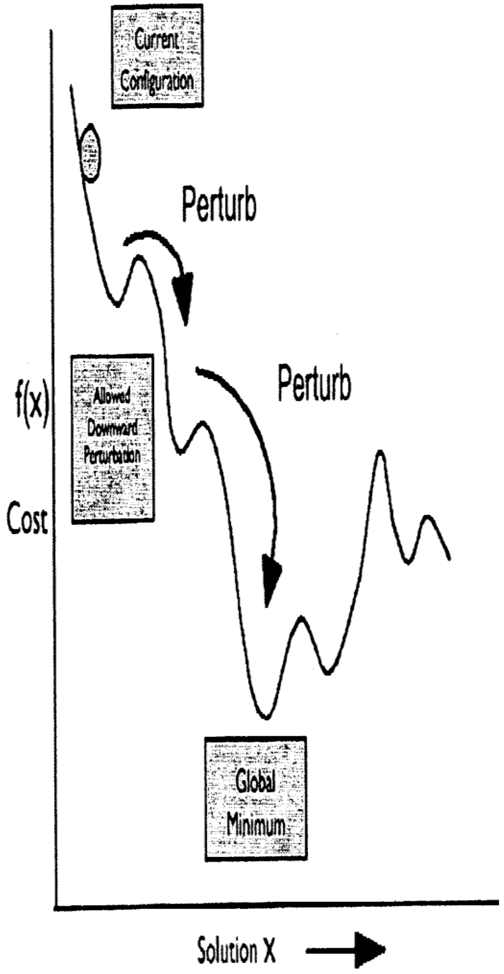
Performance and *Size* estimators are well understood and incorporated in modern tools

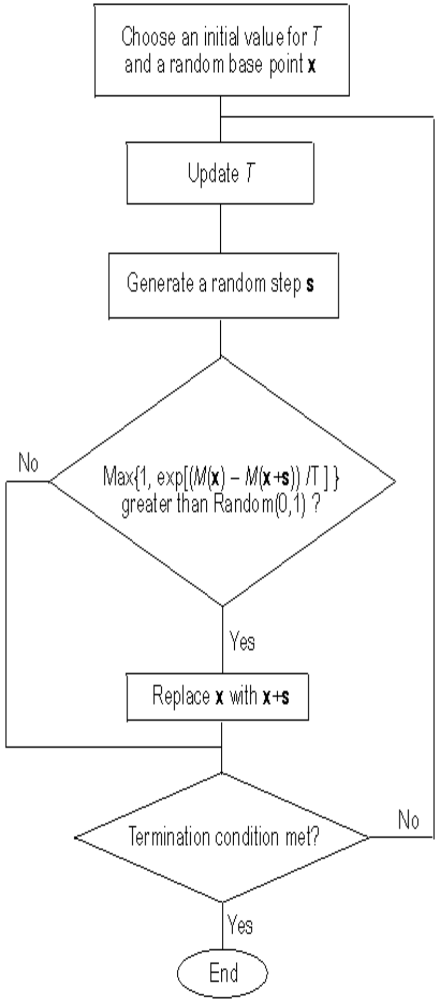
AISS will drive discovery of rapid estimation of **power** and **security**

$$f(a,b,c,d) = \Sigma(a*\mathbf{Performance},\ b*\mathbf{Size},\ \underbrace{c*\mathrm{Power}}_{\text{estimate}},\ \underbrace{d*\mathrm{Security}}_{\text{estimate}})$$

AISS: Optimization Cost Functions

$$f(a,b) = \sum (a*\textbf{Performance},\ b*\textbf{Size})$$





Cost Function Examples

Application	Perf.	Size	Power	Security
Lawn Sprinkler	2	7	9	1
Engine Control	6	5	1	3
Guided Projectile	5	1	9	7
Network Router	9	5	1	8
Mobile Phone	7	9	9	7
Smart Watch	3	6	9	3

Security Cost Function Expansion

Application	Side Channel	Reverse Eng'g	Supply Chain	Malicious Hardware
Lawn Sprinkler	1	1	9	1
Engine Control	1	7	5	2
Guided Projectile	3	9	5	9
Network Router	9	7	8	9
Mobile Phone	8	9	9	6
Smart Watch	6	8	9	1

Source: The 80s

Point: *Technology for 2-dimensional optimization has been around for ~40 years* www.darpa.mil