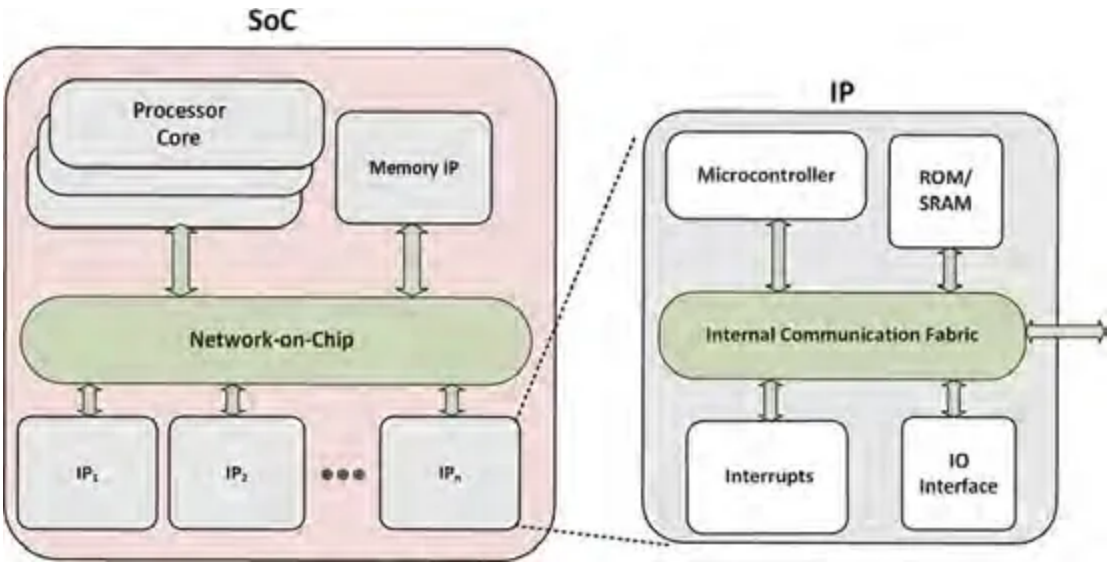
System-On-Chip (SoC) — Security Design And Modelling

Vedant Ghodke · Follow
Published in Security Risks In Systems-On-Chip (SOCs)
5 min read · Mar 30, 2021

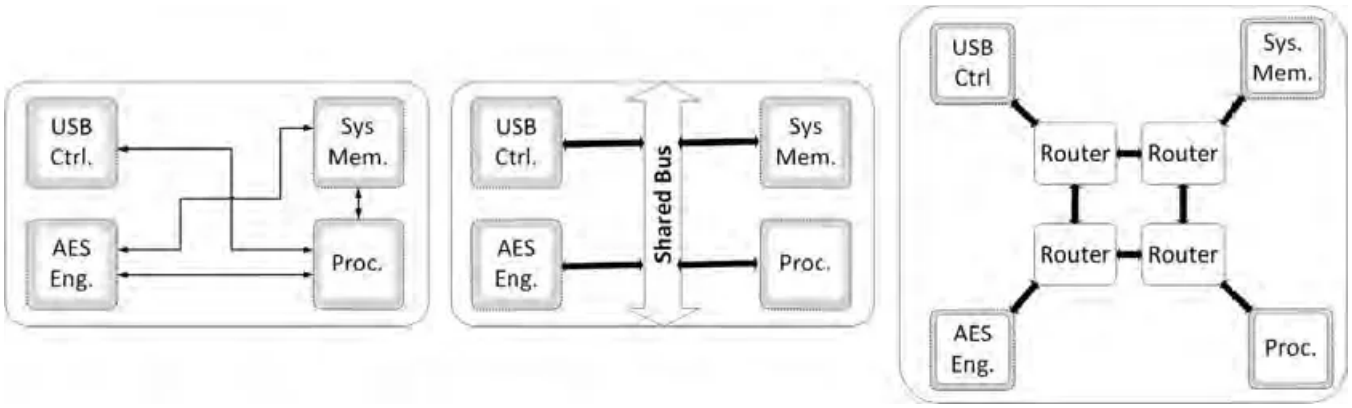
Vedant Ghodke, 30th March

In modern computing systems, the hardware and software stack coordinate with each other to implement the system functionality. The previous researches have focused on security issues of the hardware itself, and have not covered another important aspect of hardware security that concerns providing an infrastructure for secure software execution. In particular, the role of hardware in protecting the assets stored in a chip or PCB (as discussed in An Overview — Systems-On-Chips (SOCs) And Their Security Risks) from malicious software have not been described in detail.

Similarly, protection of the data/code of one application from another potentially malicious one, has not been addressed. The hardware needs to support security against software attacks, considering all levels of the software stack, from the operating system to application software. These attacks can be mounted through either functional or side-channel vulnerabilities. In this article, we will discuss various scenarios of software-induced attacks on hardware and possible countermeasures.



A modern SoC architecture that consists of multiple IP blocks connected by an interconnect fabric.



SoC architecture with Point-to-point interconnects, shared bus interconnects, Network-on-chip interconnects.

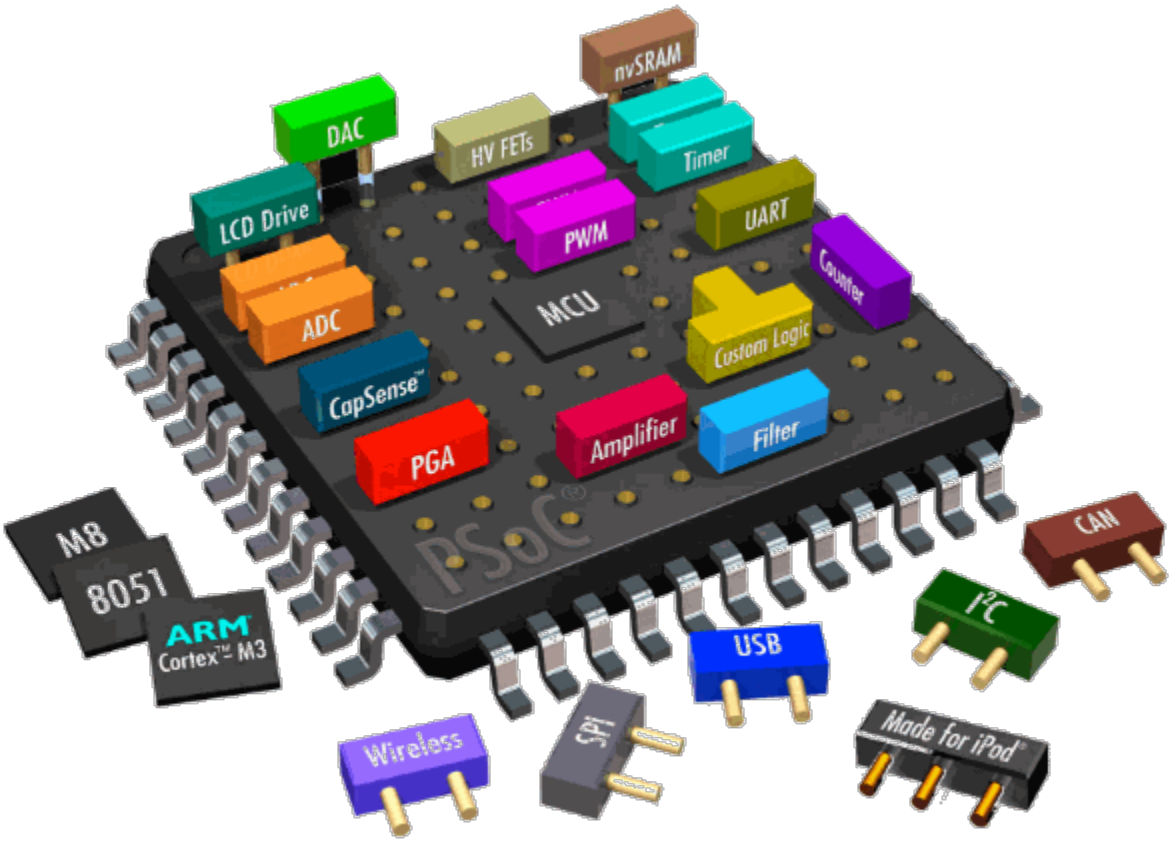
SOC Security Requirements

In this section, I will give an introduction to the security requirements SoC designers need to consider. These requirements are determined based on potential adversaries and attack vectors at different stages of the SoC life cycle.

Assets In SoC

SoC assets can be broadly defined as system-critical and security-sensitive information stored in the chips. With computing devices being employed for several highly personalized activities (for example, shopping, banking, fitness tracking, and providing driving directions), these devices have access to a large amount of sensitive, personal information, which must be protected from unauthorized or

malicious access. In addition to personalized end-user information, most modern computing systems contain highly confidential collateral from the architecture, design, and manufacturing, such as cryptographic and digital rights management (DRM) keys, programmable fuses, on-chip debug instrumentation, and defeature bits. It is crucial to our well-being that data in these devices are protected from unauthorized access and eventual corruption. Hence, security architecture, that is, a mechanism to ensure the protection of sensitive assets from malicious, unauthorized access, constitutes a crucial component of modern SoC designs.

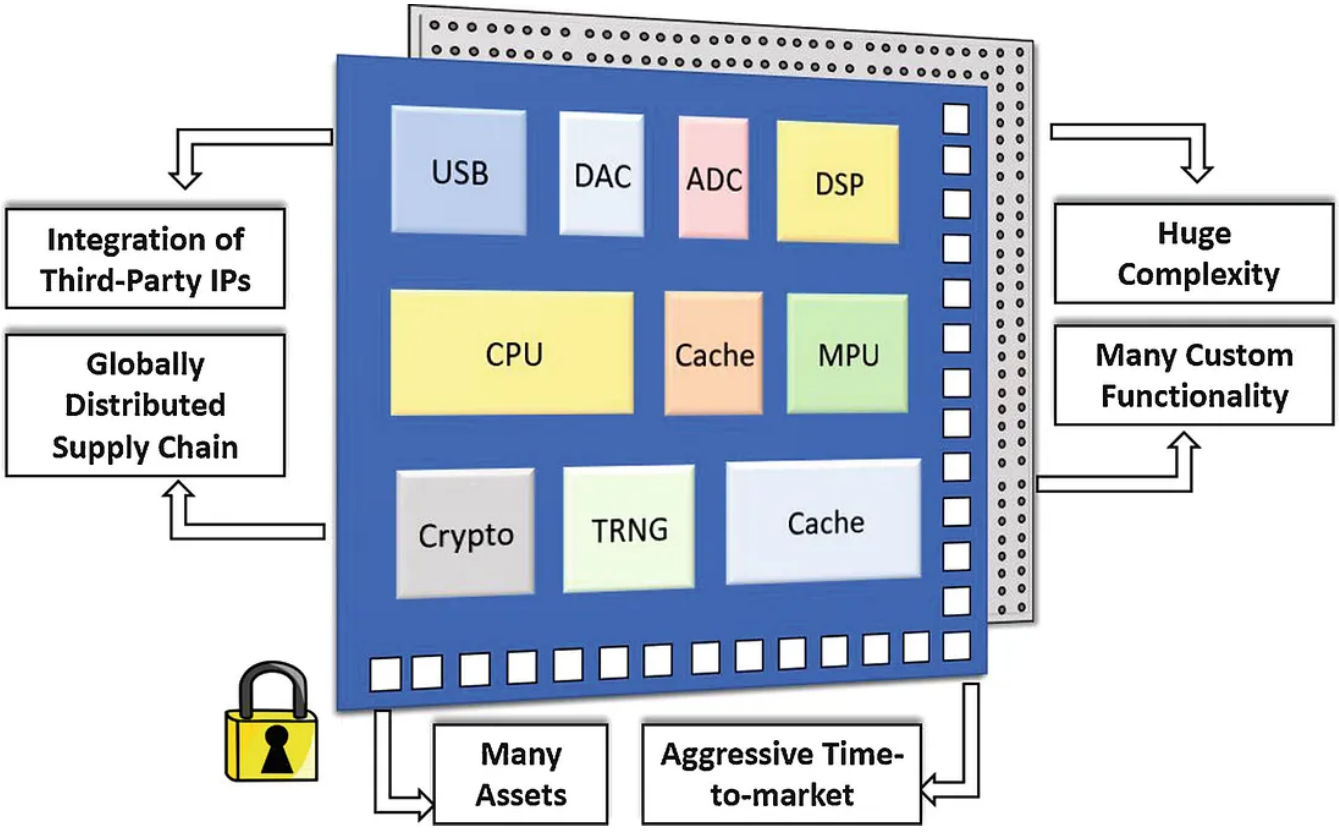


Assets used in System-On-Chip Design

Adversarial Model

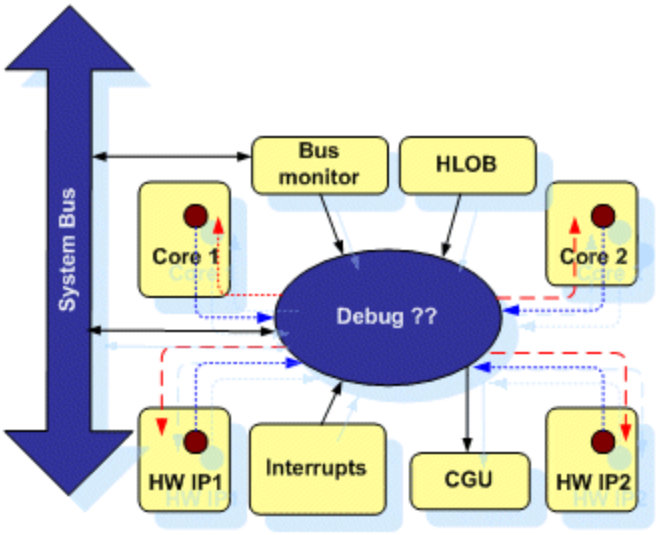
To ensure that an asset is protected, the designer needs comprehension of the power of the adversary. The effectiveness of virtually all security mechanisms is critically dependent on how realistic the model of the adversary is. Conversely, most security attacks rely on breaking some of the assumptions made regarding constraints on the adversary. The notion of the adversary can vary, depending on the asset being considered. For example, in the case of protecting DRM keys, the

end-user would be an adversary, whereas the content provider (and even the system manufacturer) may be included among adversaries in the context of protecting the private information of the end-user.



SoC Security Vulnerabilities Showing The Need For An Adversarial Model

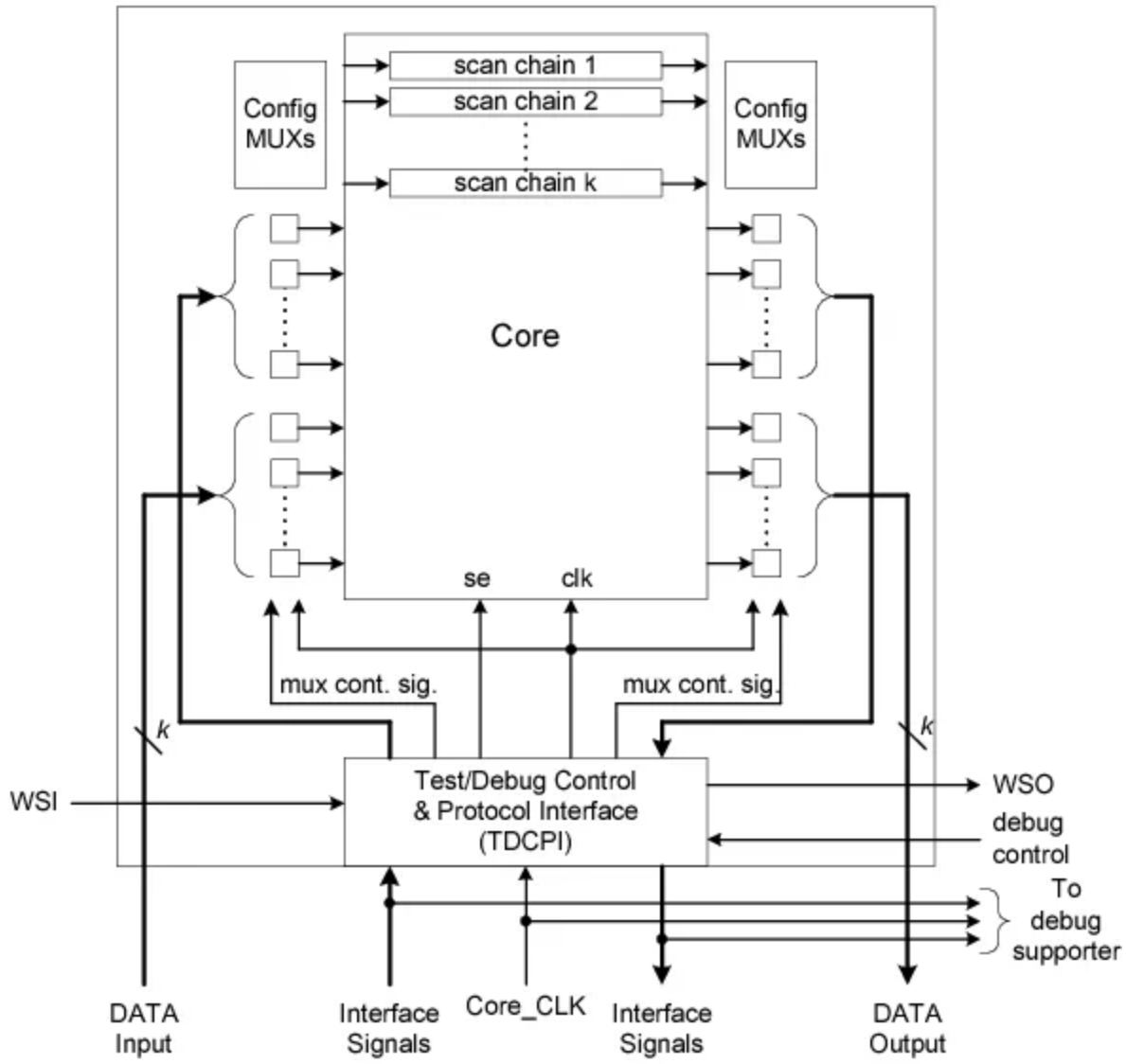
Rather than focusing on a specific class of users as adversaries, it is more convenient to model adversaries corresponding to each asset, and define protection and mitigation strategies with respect to that model. Defining and classifying the potential adversary is a creative process. It needs various considerations, such as whether the adversary has physical access, and which components they can observe, control, modify, or reverse engineer.



Debug Infrastructure For Multi-Core SoC

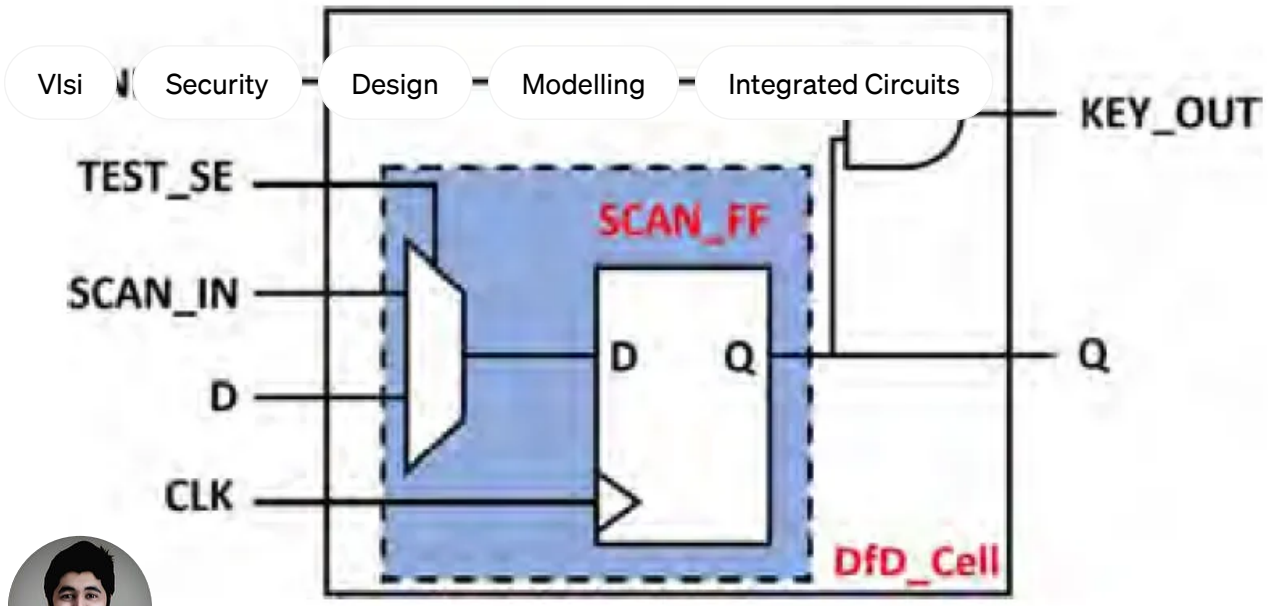
Design-For-Debug Methodology

Security requirements for SoCs often represent a conflict with **Design-For-Test (DFT)** and **Design-For-Debug (DFD)** infrastructure. DFD refers to on-chip hardware for facilitating post-silicon validation of a chip's functional and security properties. A key requirement for post-silicon validation is the observability and controllability of internal signals during silicon execution. DFD in modern SoC designs includes facilities to trace critical hardware signals, dump contents of registers and memory arrays, patch microcode and firmware, and to create user-defined triggers and interrupts. To reduce the risk of an adversary snooping on data flowing through debugging infrastructure (for example, from a crypto IP to a processor IP), data should be protected using standard cryptography primitives.



Design-For-Debug (DFD) Architecture

In the case of off-chip key generation for the SoC, the key bits must be protected from the potential snooping from other IPs, especially any untrusted IP. This can be achieved by creating a security-aware test and debug infrastructure, which involves commensurate modification to local test/debug cells of an IP that effectively blocks other IPs from observing key bits.



Follow

Modified scan cell to allow for secure key transfer by masking the output with the INHIBIT signal

Written by Vedant Ghodke

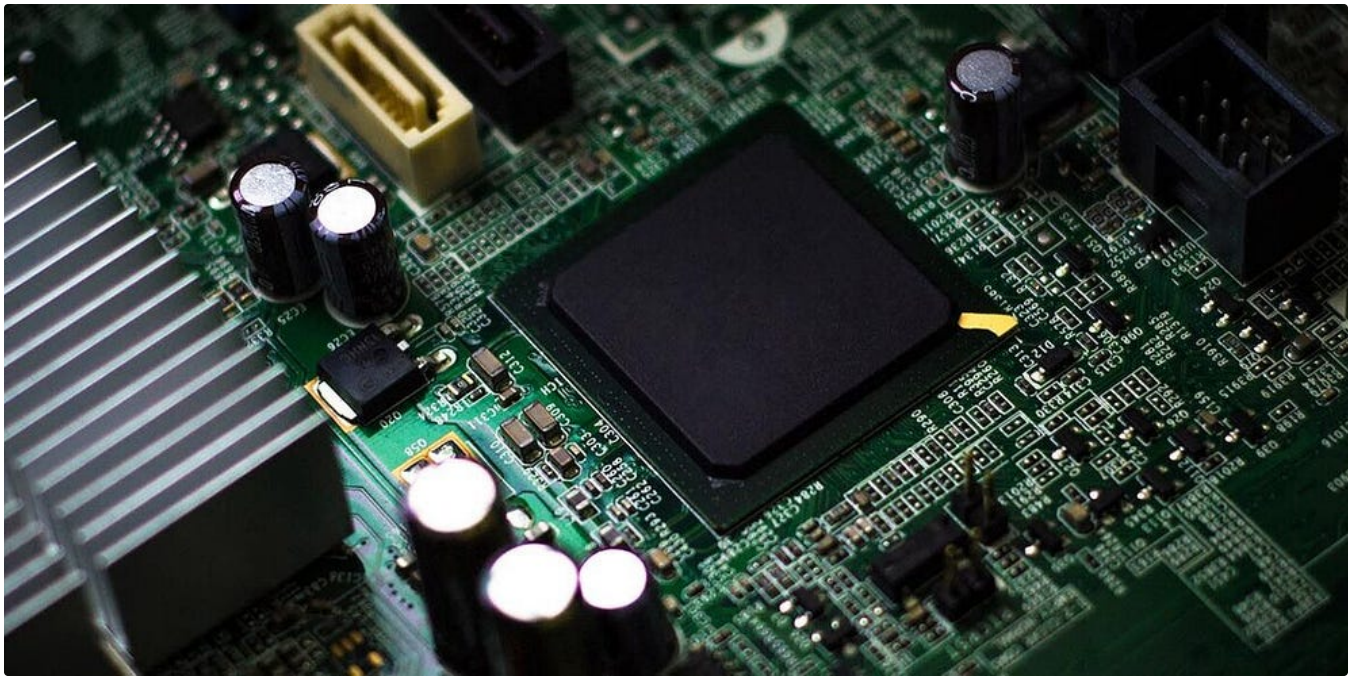
8 Followers · Editor for Security Risks In Systems-On-Chip (SOCs)
Solutions Engineer (Security) at Cisco

With the knowledge of the above SoC Security Requirements, we will be looking at SoC Security Policies to prevent the hardware and firmware vulnerabilities thus preventing unauthorized access to assets called the access control. Such access control can be defined by confidentiality, integrity, and availability (CIA) requirements. The goal of a security policy is to map the requirements to *"notionally"* design constraints that must be met by IP integrators, or SoC integrators, to develop protection mechanisms.

More from Vedant Ghodke and Security Risks In Systems-On-Chip (SOCs)

After all, what can actually be inferred is the ability to weigh out these disadvantages and educate ourselves on the mentioned security vulnerabilities and their causes, and perhaps try and propose state-of-the-art techniques to avoid any such security mishaps!

Stay well, stay safe and stay updated!

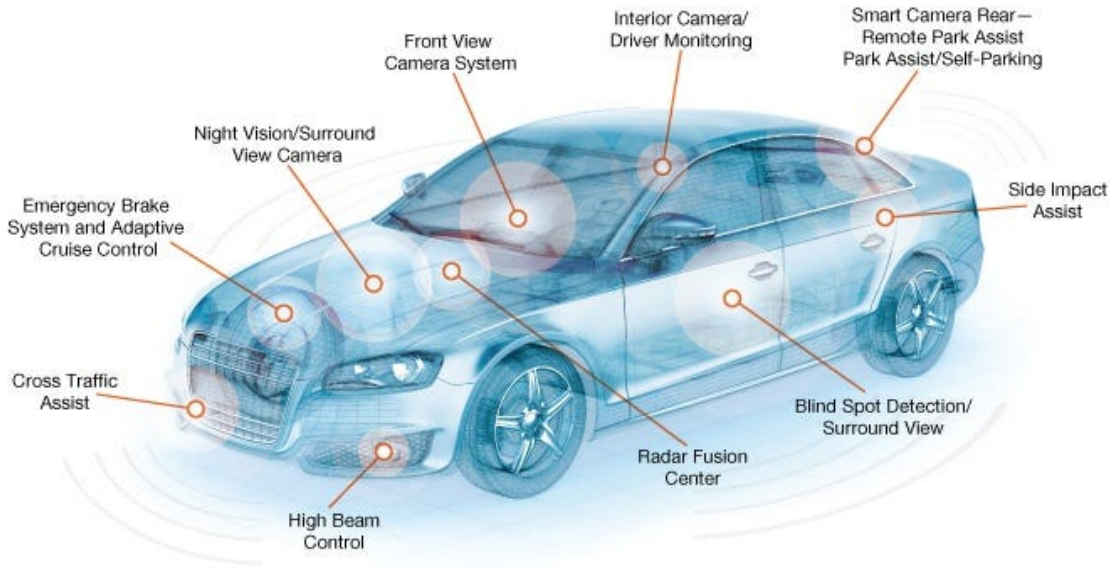


Vedant Ghodke in Security Risks In Systems-On-Chip (SOCs)

An Overview — Systems-On-Chips (SOCs) And Their Security Risks

Vedant Ghodke | 25th February, 2021

4 min read · Feb 26, 2021



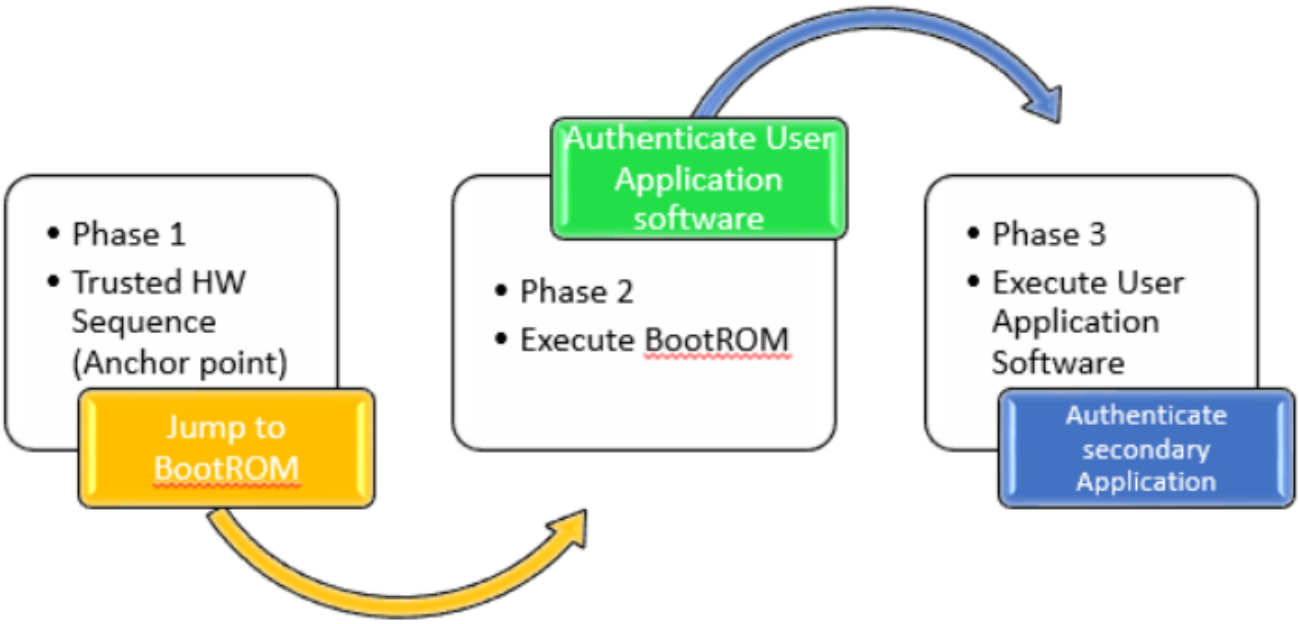
Atharvadeshpande in Security Risks In Systems-On-Chip (SOCs)

Safety & security architecture for automotive SOCs

The automotive industry is changing rapidly to address the stringent requirements for safety and security of vehicular systems...

5 min read · May 28, 2021

132

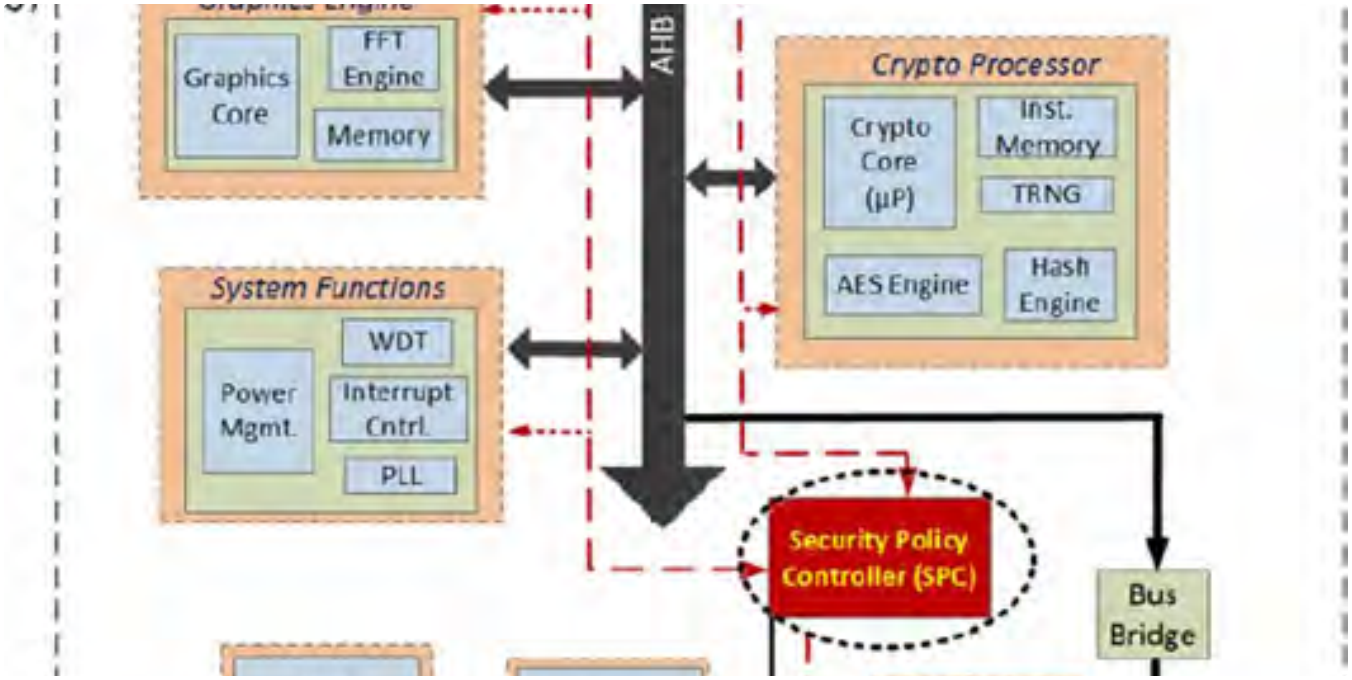


Atharvadeshpande in Security Risks In Systems-On-Chip (SOCs)

Secure the SoCs

In the era of Internet-of-Things (IoT), security has become one of the most vital parts of a System-on-Chip (SoC). Secured SoCs are used...

4 min read · Mar 26, 2021



Vedant Ghodke in Security Risks In Systems-On-Chip (SOCs)

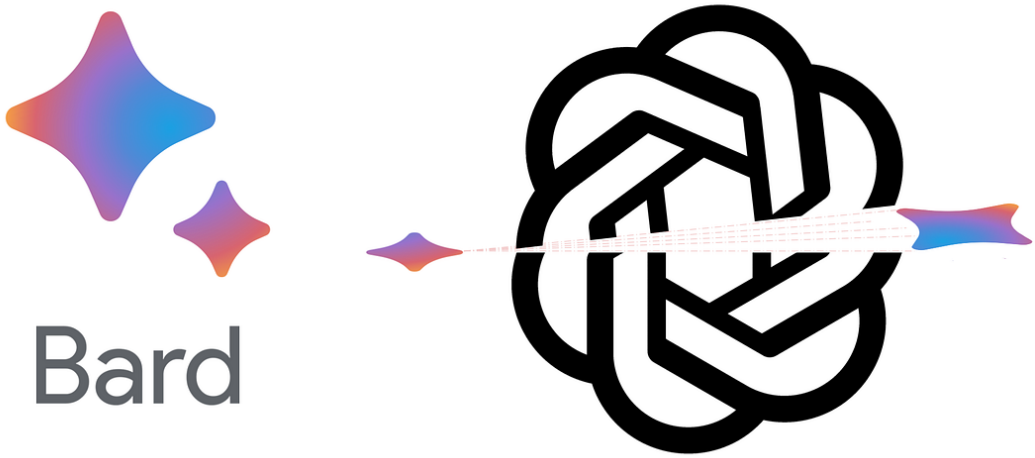
System-On-Chip (SoC) Security Policy Enforcement

Vedant Ghodke, 30th May

3 min read · Jun 7, 2021

Recommended from Medium

103



AL Anany

The ChatGPT Hype Is Over — Now Watch How Google Will Kill ChatGPT.

It never happens instantly. The business game is longer than you know.

· 6 min read · Sep 1

18.1K 550

Unbecoming

10 Seconds That Ended My 20 Year Marriage

It's August in Northern Virginia, hot and humid. I still haven't showered from my morning trail run. I'm wearing my stay-at-home mom...

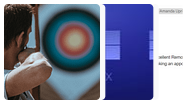
· 4 min read · Feb 16, 2022

69K 992

Lists

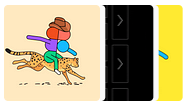
Stories to Help You Grow as a Designer

11 stories · 375 saves



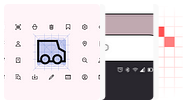
Interesting Design Topics

203 stories · 223 saves



Figma 101

7 stories · 270 saves



Icon Design

30 stories · 146 saves

Barack Obama

What I'm Reading on the Rise of Artificial Intelligence

Earlier this week, President Biden issued an executive order on artificial intelligence — a breakthrough technology that has the power to...

2 min read · 6 days ago

10.8K

234

FadinGeek

Top 20 mobile apps which nobody knows about...

In the vast ocean of mobile applications, some remarkable gems often go unnoticed. While popular apps dominate the headlines, there are...

6 min read · May 28

5.8K 143

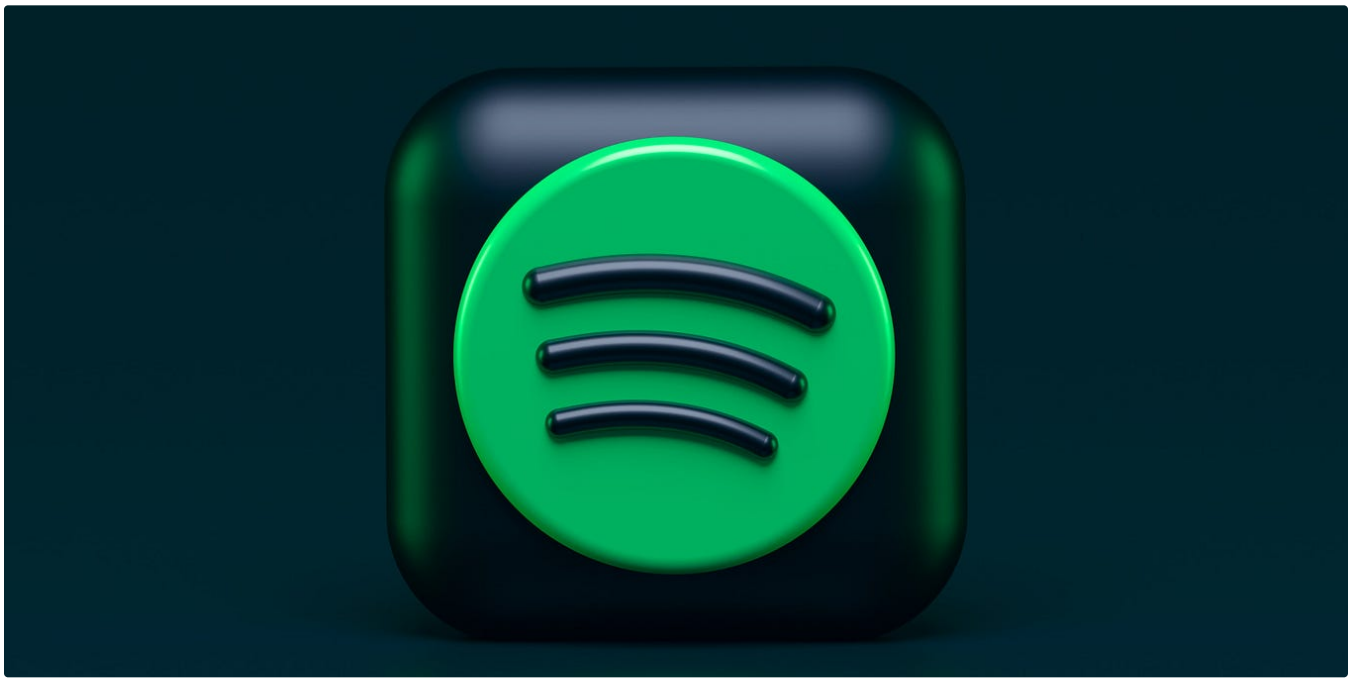
Vaishnav Manoj in DataX Journal

JSON is incredibly slow: Here's What's Faster!

Unlocking the Need for Speed: Optimizing JSON Performance for Lightning-Fast Apps and Finding Alternatives to it!

16 min read · Sep 28

7.9K 106



Scott-Ryan Abt in Pitfall

Bye Bye, Spotify

And see ya later, all you subscription services in my little empire

· 4 min read · Aug 20

15.2K 363

See more recommendations