Testing beyond spec for product security assurance

Author: Rachana Maitra
Senior Principal Engineer, Corporate SDL
Marvell Technology Inc.

Date: November 7, 2024

Agenda

1. Motivation for product security testing
2. Challenges of product security testing
3. Marvell’s approach to addressing the challenge
4. Strategy and tools for product security testing
5. Conclusion

Motivation for product security testing

Marvell Charter

*Move, store, process and **secure** the world's data with semiconductor solutions*

Product Security practice at Marvell

- ❑ **Proactive – Security development lifecycle (SDL)**

Design-in product security measures and validate implementation before production release

- ❑ **Reactive – Product security incident response team (PSIRT)**

Investigate vulnerability reports post-production and urgently mitigate consequences

Industry imperative to continually improve proactive measures

- ❑ Severity and impact of security incident post-production
- ❑ Growing sophistication of bad actors
- ❑ Ever evolving threat landscape

Challenges of product security testing

Commitment for holistic defense

- ❑ Security must be built into product definition
- ❑ Both IP and system level threats must be considered
- ❑ Layers of defense with HW/FW must be implemented

Unbounded potential for threat

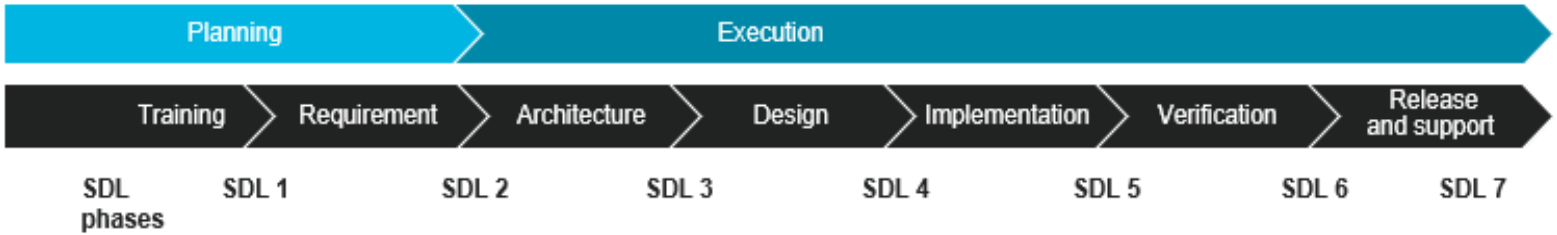
- ❑ Need strategies beyond conventional methods
- ❑ Test parameters need to go beyond spec
- ❑ Need to re-affirm defense with phase appropriate coverage

Ever evolving threat landscape

- ❑ Threat modeling may need to be retriggered, if threat landscape changes
- ❑ Security testing scope may need to be revisited, if design changes
- ❑ Tools may need to change to keep up with growing sophistication of bad actors

Marvell's approach to addressing the challenge

- ❑ Integrated SDL into Product Lifecycle (PLC), prioritizing product security testing
- ❑ Acknowledged the difference from conventional testing, continually improving strategies
- ❑ Adopted shift-left strategy in testing, ensuring robust testing pre- to post-silicon

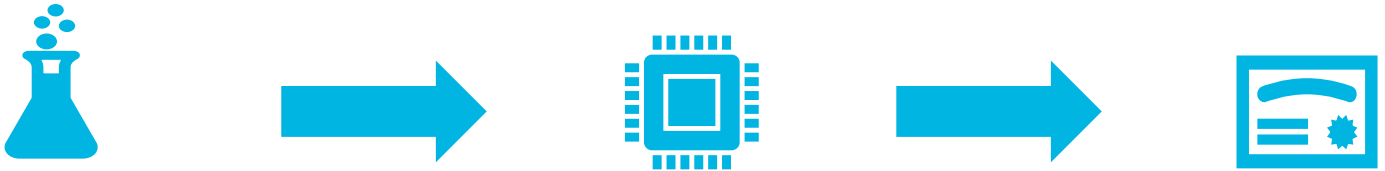


SDL process minus product security testing defeats the whole purpose

Guilty until proven innocent!

Strategy for product security testing

Looking beyond functional correctness & performance targets



Enhance security coverage

- **Functional testing**
- **Silicon characterization**

Test with specialized tools

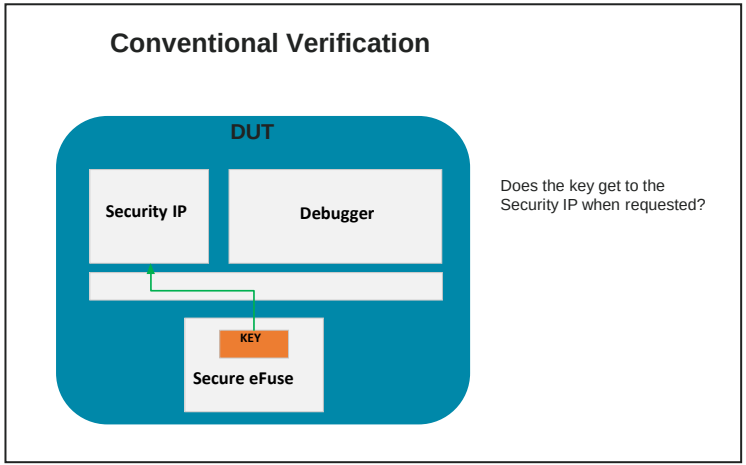
- **Tools with security specific lens**
- **Automated tools, enhanced with AI**

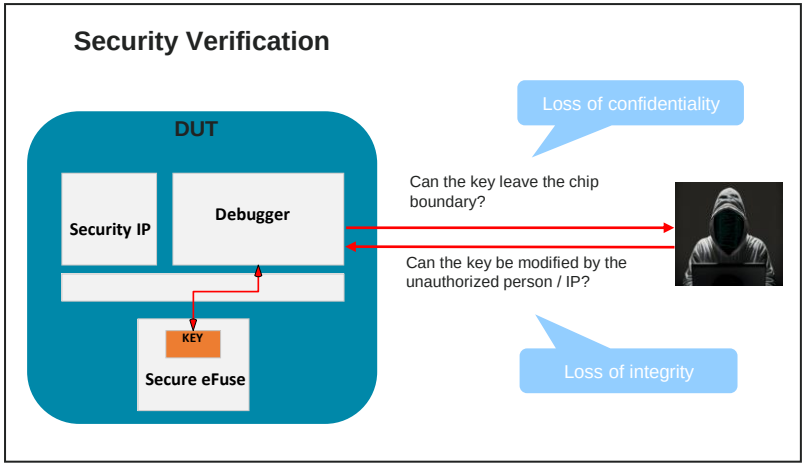
Certify by external

- **Security consultants**
- **Compliance labs**

Difference from conventional testing

Looking for what should not happen





- Who should not be able to grant access
- Who should not be able to access
- Where data should not go
- What should not be accessible

Product security testing coverage assurance

Thinking like a hacker

Assuring coverage of the three core security principals

CIA: Confidentiality, Integrity, Availability following STRIDE*

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

*Concept developed by Microsoft, widely used for modeling threats to system

Security sensitive coverage prioritization

Ensuring functional and silicon robustness per specification

- IP and block level stress of all security sensitive critical assets and interconnects
- Prioritization of negative conditions (error detection features) at all security boundaries
- System level stress of threat model with random input (HW and FW fuzz testing)
- Silicon characterization of all components enlisted in threat model across PVT spec

Coverage addition beyond spec

Covering security loop-holes hidden within functionally clean design!

- ❑ Invalid input (don’t care logic) coverage in directed and random testing
- ❑ Iterative stress of negative conditions (error detection features) beyond use case limits
- ❑ Threat model characterization on silicon beyond silicon PVT spec

Silicon characterization down to failure

Debugging all failures within and beyond spec!

Example PVT SHMOO DATA (3 runs: all pass = green, all fail = red, random fail = yellow)

SPI NOR Standard (Reads ID, performs erase/Write/Read/Compare over voltage shmoo)

DUT ID		VDD_SOC (mV)																																				
clkdiv	Temp (C)	580	590	600	610	620	630	640	650	660	670	680	690	700	710	720	730	740	750	760	770	780	790	800	810	820	830	840	850	860	870	880	890	900	910	920		
2	100			3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3		
4	100			3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3		
2	85			0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3		
4	85			0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3		
2	25			0	0	0	0	0	0	0	0	0	0	0	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3		
4	25			0	0	0	0	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3		
2	0			0	0	0	0	0	0	0	3	3	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	3		
4	0			0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	3	3	3	3	3		
2	-10			0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
4	-10			0	0	0	0	0	0	0	0	0	3	3	3	3	3	3	3	3	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		

Inclusion of specialized tools and services

Partnering with industry experts

Tools from specialized suppliers

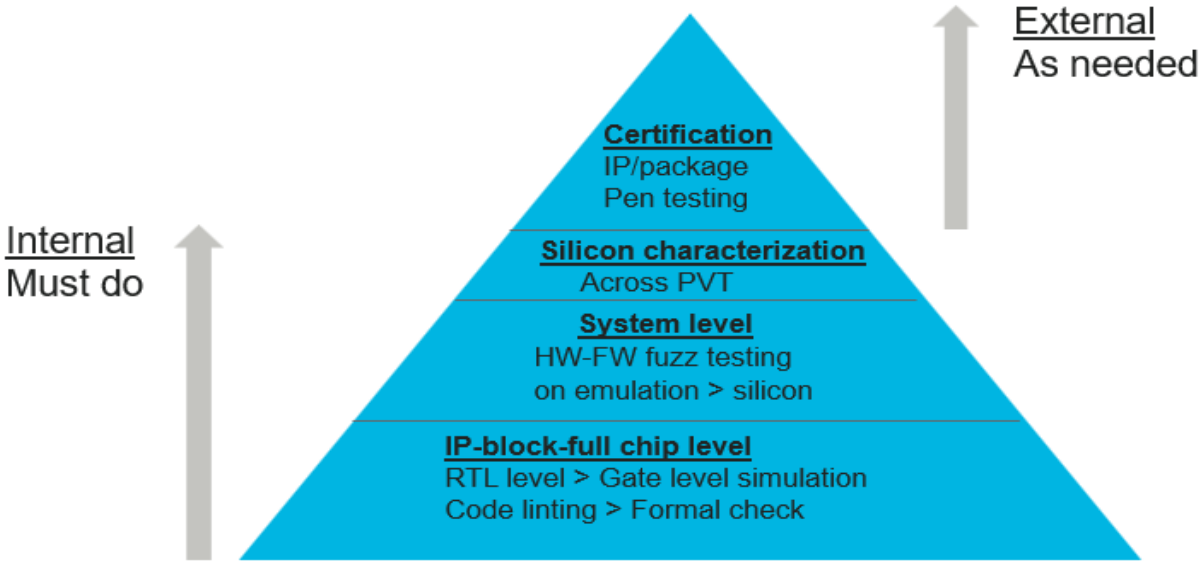
- ❑ Static lint tool for detecting security rule violations in RTL code
- ❑ Formal tool for detecting potential vulnerability in IP connectivity
- ❑ Dynamic tools for data leak or SCA or FIA vulnerability analysis at IP/block/system level

Service from specialized suppliers

- ❑ Closed or gray box penetration testing (testing by ethical hackers)
- ❑ IP certification (Ex: NIST)
- ❑ Chip/package level certification by specialized labs

Security testing pyramid

Layering verification/validation from coding to production release



Conclusion

Product security assurance is a top priority for Marvell!

Marvell's commitment

- ❑ Proactively assure product security adhering to industry best practices for security development lifecycle
- ❑ Continually improve strategy and toolset for robust product security verification/validation
- ❑ Partner with industry to evolve technology for product security assurance against growing sophistication of threats

References

1. IEEE-HOST 2024 paper by Professor Prabhat Mishra and Ankur Srivastava: Hardware Security and Trust verification

2. Article by Anders Nordstrom (Principal Engineer – Cycuity) on Data leak and timing side channel attack: Timing is of the Essence in Hardware Security

3. Course on Fault injection attack: https://course.ece.cmu.edu/~ece749/docs/faultInjectionSurvey.pdf

4. Articles on threat modeling:
   a. https://en.wikipedia.org/wiki/STRIDE_model
   b. https://www.synopsys.com/content/dam/synopsys/sig-assets/whitepapers/wp-threat-modeling-decoded.pdf

Appendix
Acronyms

SCA	Side Channel Attack
FIA	Fault Injection Attack
IP	Intellectual Property
RTL	Register Transfer Level
DUT	Device Under Test
HW	Hardware
FW	Firmware
PVT	Process-Voltage-Temperature
AI	Artificial Intelligence
NIST	National Institute of Standards and Technology

Disclaimer

- Product security can never be 100% guaranteed
- Marvell representative should be contacted for product specific implementation of security verification/validation strategy

MARVELL

Thank You

Essential technology, done right™