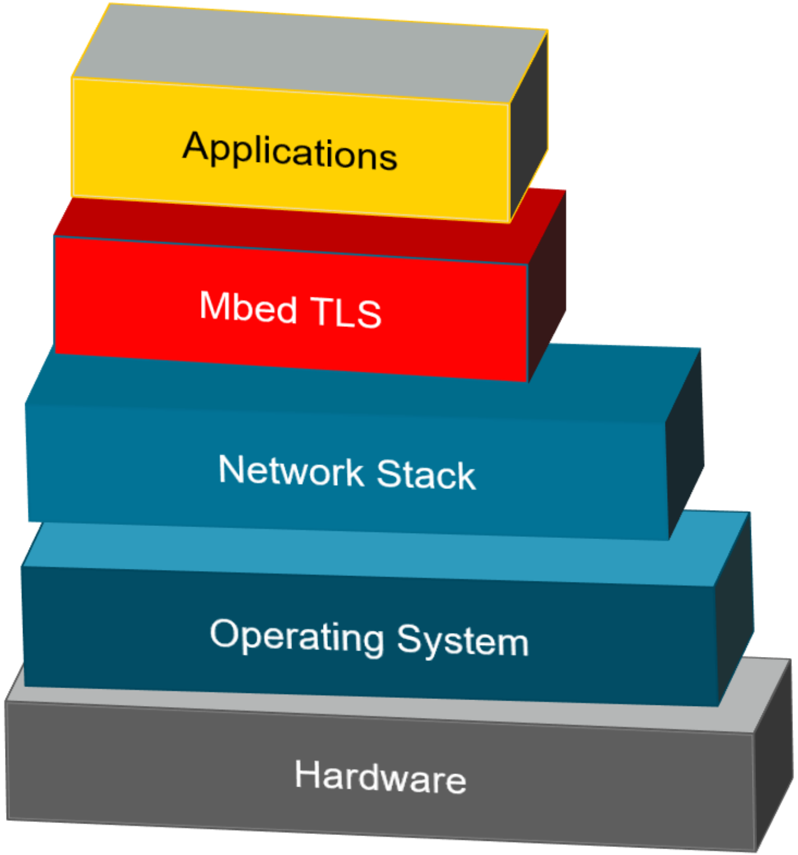
Mbed TLS Workshop

TrustedFirmware
.org

Some Context...



Applications

Mbed TLS

Network Stack

Operating System

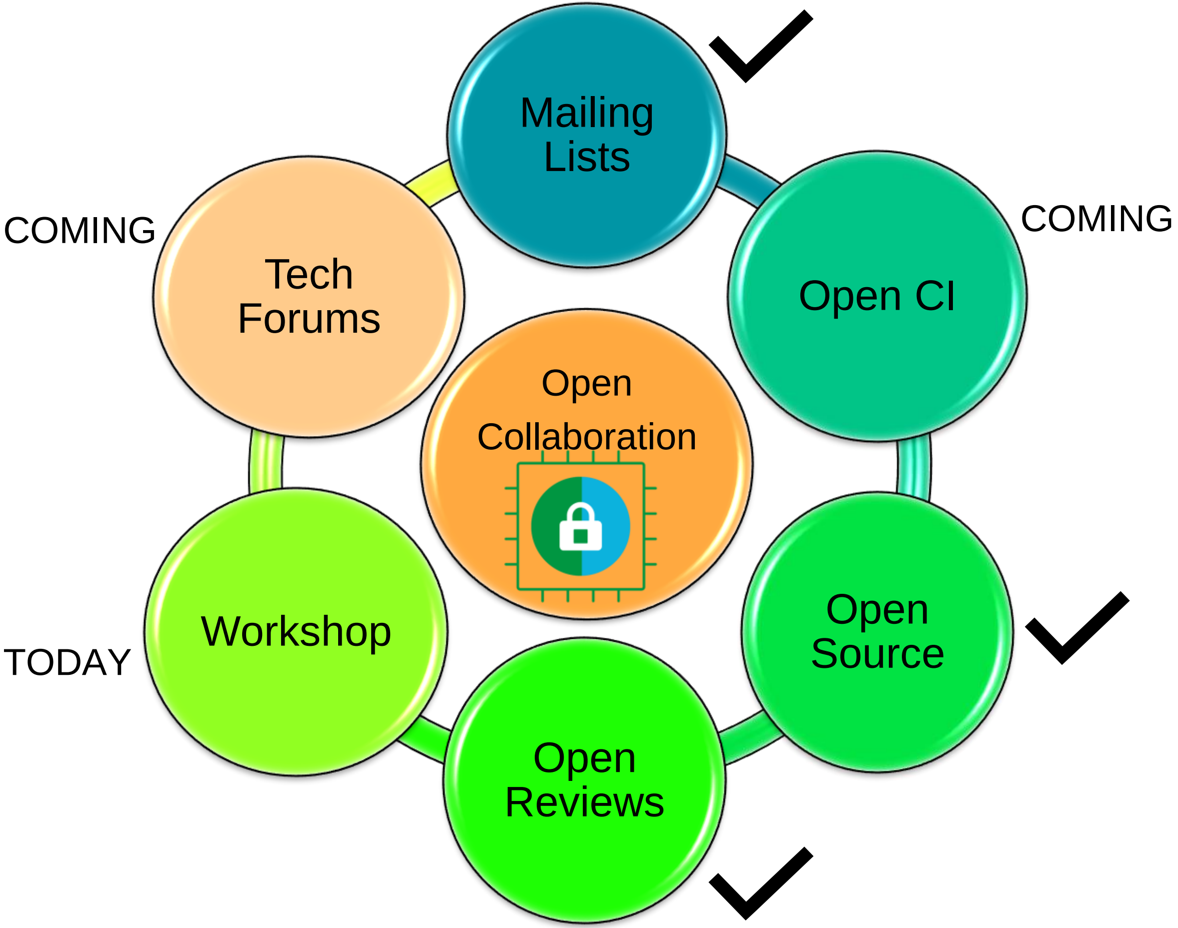
Hardware

Mbed TLS

Transitioned to TrustedFirmware.org

- *Ecosystem Ownership*
- *Community Driven*
- *Open Collaboration*
- *Increased Arm Investment*

The Virtuous Circle Of Collaboration!



Workshop Objectives

- Building a collaborative Mbed TLS community

- Discuss Recent and Upcoming Work

Notes

- Agenda posted in the chat
- Active participation from attendees
  - Unmute anytime to ask/discuss **OR**
  - Use the chat
- Remain on Mute if not speaking
- Workshop is getting recorded for anyone who can’t attend the workshop.
- Not an opportunity to ask to do more ☺, but to solve problems jointly

Agenda

Topic	Time (in GMT)
Welcome	2.00 – 2.10pm
Constant-time code	2.10 – 2.30pm
Processes - how does work get scheduled?	2.30 – 2.50pm
PSA Crypto APIs	2.50 – 3.20pm
PSA Crypto for Silicon Labs Wireless MCUs - Why, What, Where and When	3.20 – 3.50pm
Break	
Roadmap, TLS1.3 Update	4.10 – 4.30pm
Mbed TLS 3.0 Plans, Scope	4.30 – 5.00pm
How do I contribute my first review and be an effective Mbed TLS reviewer	5.00 – 5.30pm
Open Discussion	5.30 – 6.00pm

TrustedFirmware
.org

Mbed TLS, PSA Crypto

■ Released ◆ Development ● Adv. Planning ⬢ Concept

Complete ■	CY2020 Q4 ◆	CY2021 Q1 ⬢	CY2021 Q2 ⬢	CY2021 Q2+ ⬢
	PSA Crypto 1.0 Update existing APIs	PSA Crypto 1.0 Support Missing APIs	PSA Crypto 1.0 Productize	PSA Crypto 1.1
Unified PSA Driver Interface[c] Specification	Unified PSA Driver Interface[c] APIs	Unified PSA Driver Interface[c] More APIs, Test Driver		
		Mbed TLS3.0 Preparation	Mbed TLS3.0 Preview	Mbed TLS3.x Deprecation of legacy APIs, Cleanup, Use More PSA Crypto APIs Mbed TLS4.0 Remove legacy APIs, Fully Use PSA Crypto APIs
	Threat Model PSA Crypto		Open CI Phase1	Threat Model Mbed TLS
				TLS1.3 Limited Support

Mbed TLS

- Welcome more contributions, reviewers & maintainers
- Engage in the mailing list (mbed-tls@lists.trustedfirmware.org)

Let’s Build Security Collaboratively