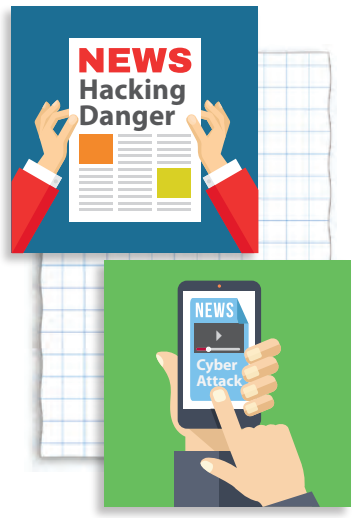


Securing Embedded Systems

Systems are at risk with software-only security

A *Root of Trust* is needed

Root of Trust is a set of functions that control a cryptographic processor

Fact: Software can be hacked by software

Fact: Hardware can be made to be robust against attacks

Fact: Hardware and software combined are much more secure

Hardware Security

Without a Trusted Platform Module

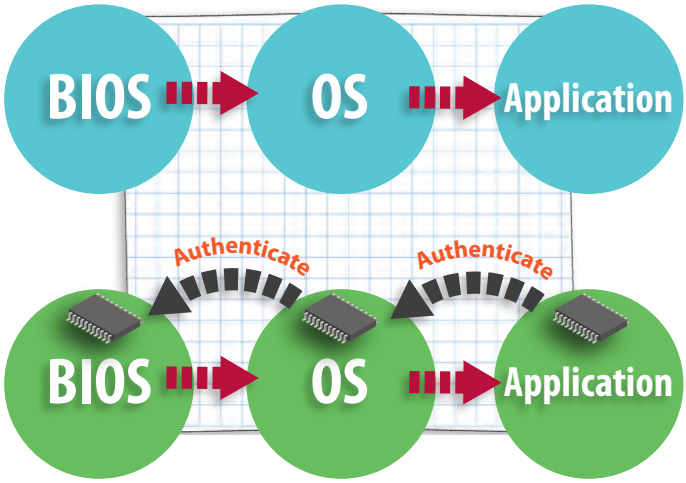
Systems boot and start executing. There is no validation at any boot stage.

This system and connected systems are at risk

With a Trusted Platform Module

The secure boot starts from a trusted source and each successive state is authenticated.

A chain of trust is created

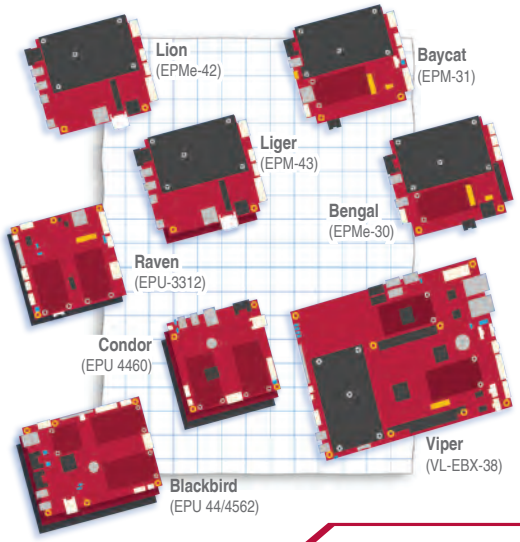


A Trusted Solution

A TPM chip provides a Root of Trust

- It enables a static root of trust measurement
- It assures that keys and secrets are only available when appropriate
- It solves the "where do we put the encryption key" problem

VersaLogic products with TPM



12/07/17