seL4 & Agile and Resilient Embedded Systems (ARES)

Douglas Schafer

AFRL Information Directorate, September 23, 2019

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

Challenge

- Highly complex & connected
- Multi-vendor; Intellectual property
- Procurement and funding

Source: https://www.flickr.com/photos/grantwickes/13836611563

Source: https://www.af.mil/News/Photos/igphoto/2000398487/

Source: https://www.flickr.com/photos/35703177@N00/8722357151//

Source: https://commons.wikimedia.org/wiki/File:ClearFog-base.jpg

Source: https://www.navy.mil/management/photodb/photos/180929-N-SU448-0062.JPG

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

ARES and seL4

To a high technology readiness level:

- Design-in embedded system software cybersecurity and resilience
  - Decouple computing layers
  - Integrate and protect 3rd party applications

- Address three pillars of cybersecurity by developing capabilities aligned with Cyber Survivability Attributes (CSA) [1]
  - Protect, Mitigate, Recover

- Implement and demonstrate feasibility meeting needs of Air Force weapon systems

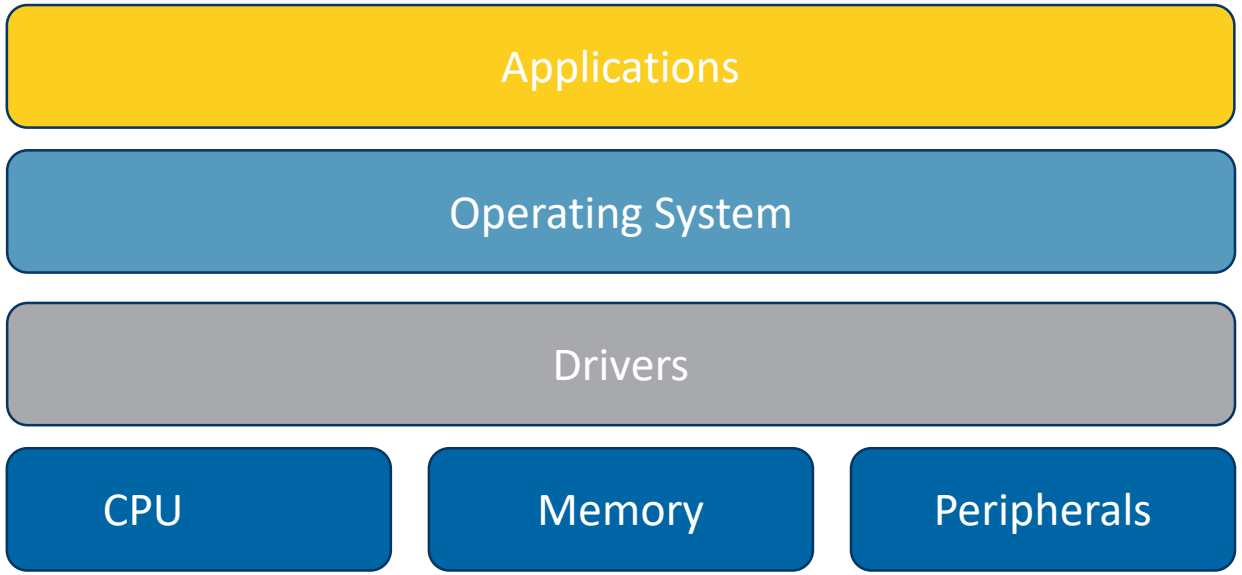
1 United States Air Force Systems Security Engineering Guidebook, 8 May 2018, v1.3

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

ARES Architecture & Software Development

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

Current SW Environment



Security posture, in general:

- Tightly coupled
- Unsecured communication
- Lack of partitioning*
- Lack of interface control
- Lack of monitoring and response

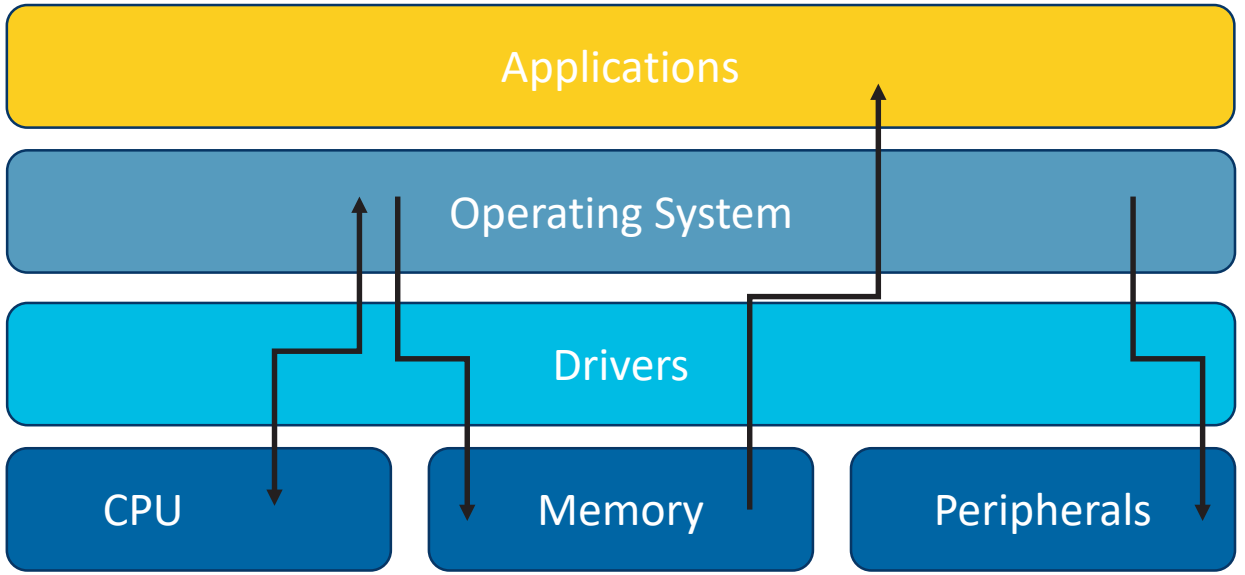
*Some systems implement commercial software separation kernels.

Significant cost in time, complexity, and funds to modify

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

Current SW Environment

Image source: https://www.google.com/search?q=cyber+attack



Notional depiction for illustration only

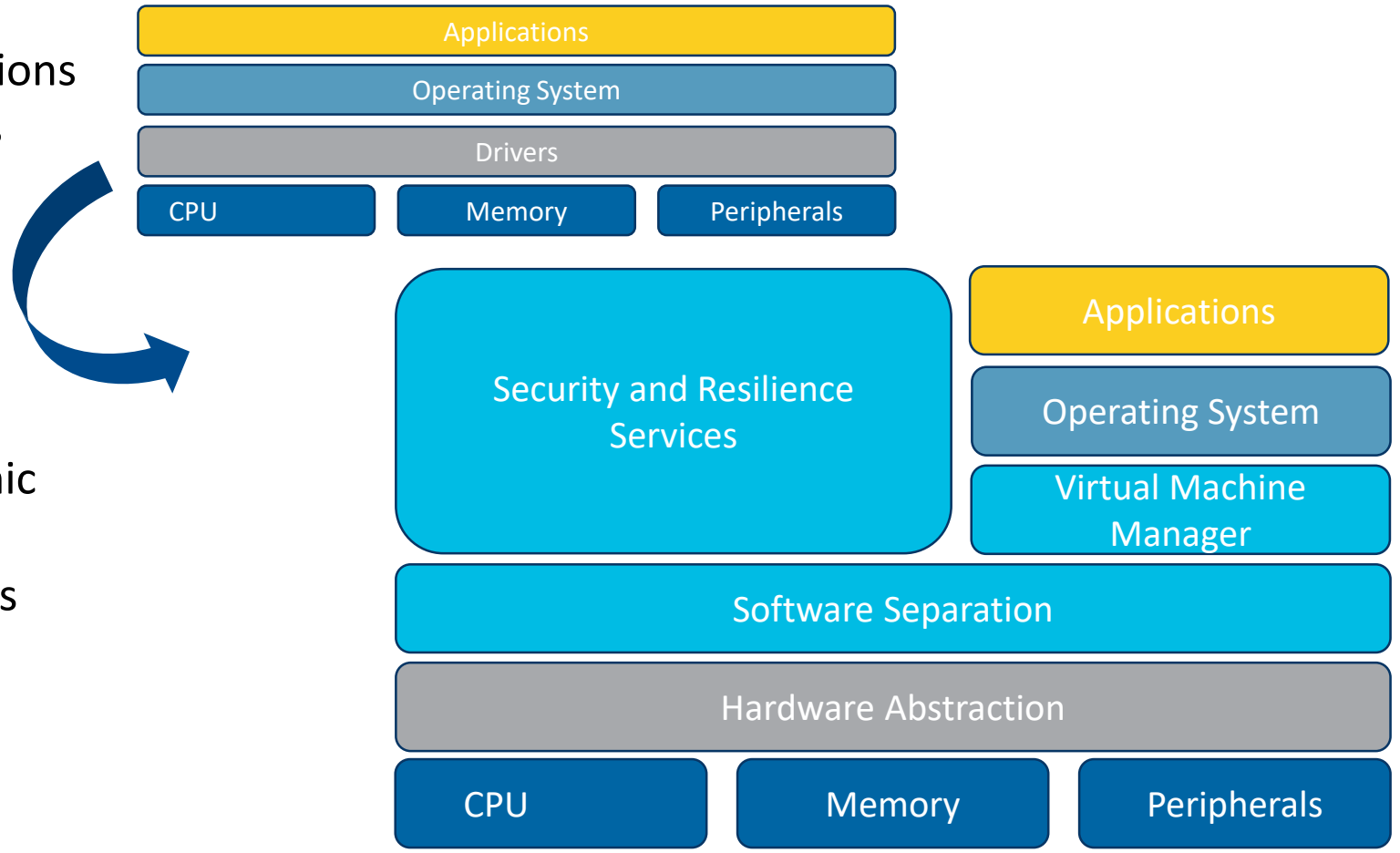
No controls on memory access, processes, interfaces, or boundaries.
So, how to protect and assuredly operate mission applications?

Attacks result in unchecked accesses and adversarial freedom of maneuver

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

ARES SW Environment

- Fully isolates and controls applications
- Restricts permissions and accesses
- Protects and monitors
  - Processes & memory
  - Interfaces
  - Information in-transit (confidentiality & integrity)
- Secures communication via dynamic encryption
- Enforces specified rules and polices



Addresses susceptibilities & monitors behaviors

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

Complete SW Development

- 64-bit, multi-core SW separation microkernel (seL4)
- Common library support and driver development
- Secure Virtual Machine Manager hosting multiple, concurrent virtual machines
- Interprocess Communication encryption/Dynamic Key Management
- Process and memory introspection
- Successful integration of small unmanned system flight and autopilot applications
- Successful testing against cyber attack classes

In-test

- Integration of industry flight management and control system
- Implementation within industry-grade small unmanned system flight module
- Flight and cyber assessment testing

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

Our Journey

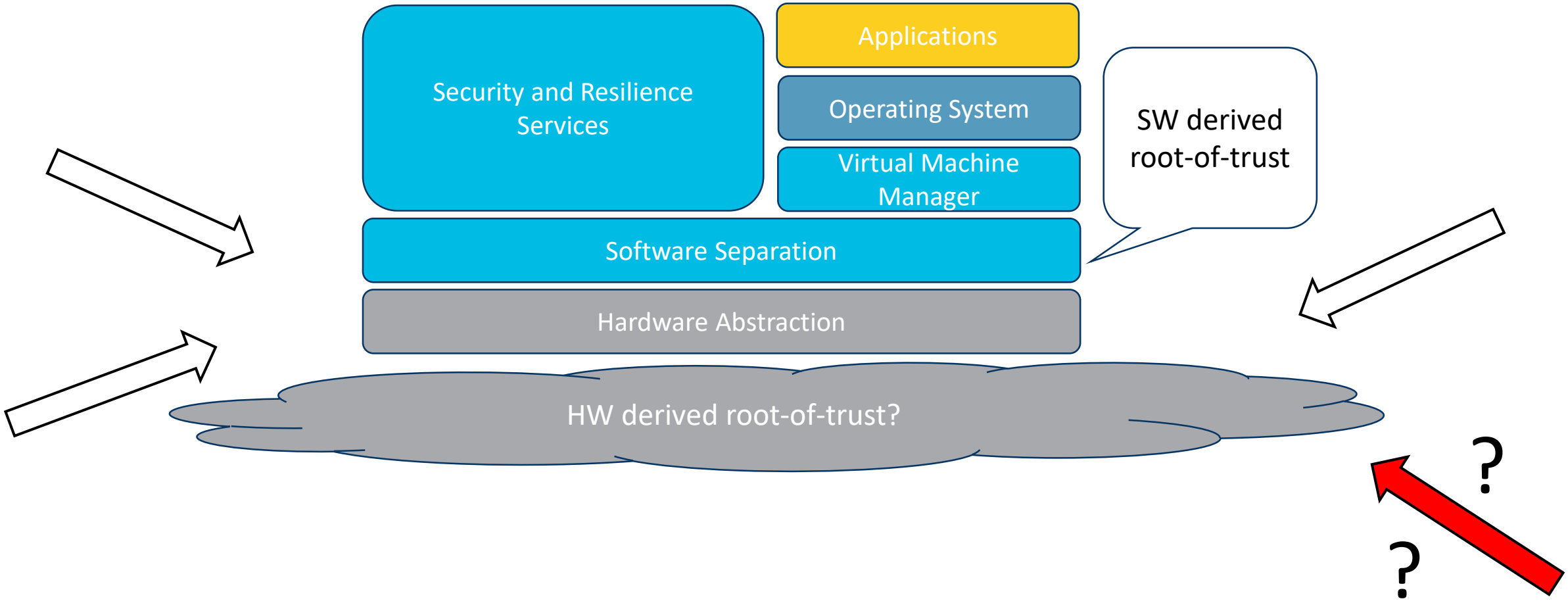
- Hangar Tests
- Anechoic Chamber
- Outdoor Navigation Signals
- Outdoor sUAV Test Range
- Fixed Wing Laboratory
- And now……

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

What's Next

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

Trusted Systems



DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

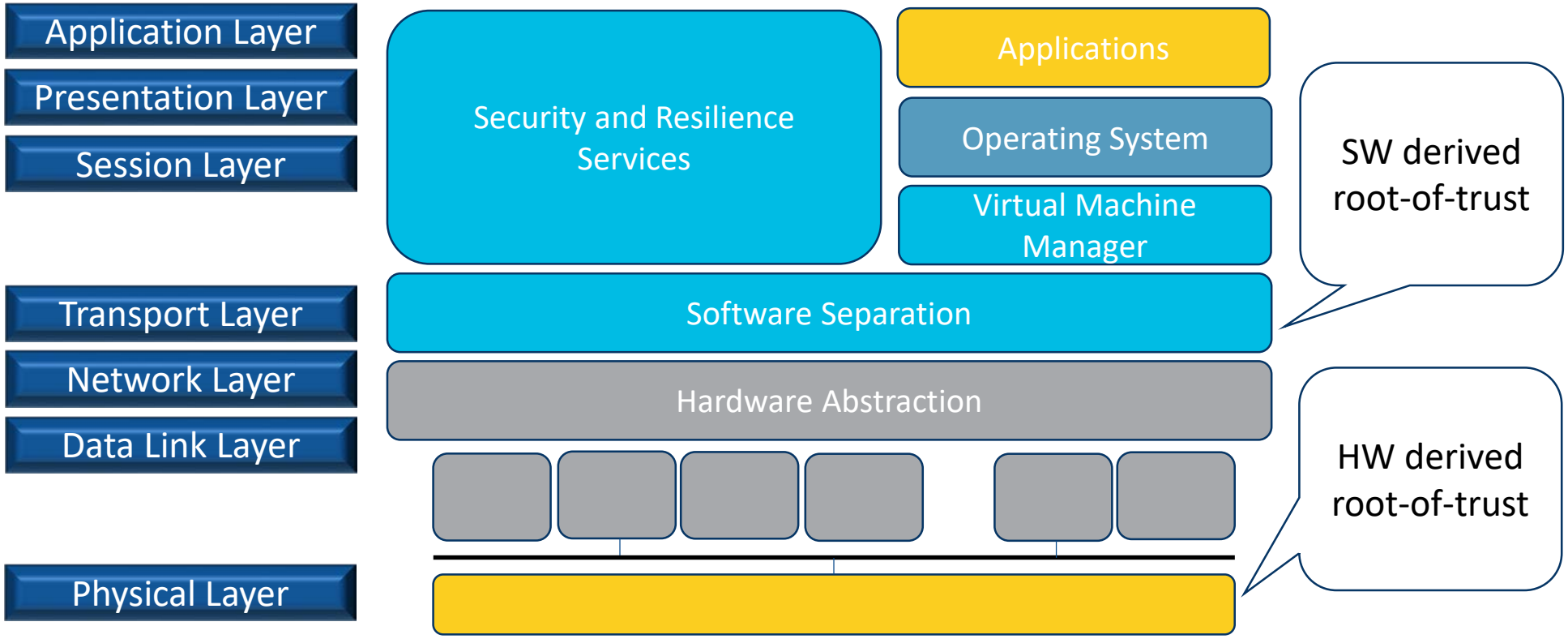
Principles for Trustworthy Systems

Derived from Dr. Neumann 2004; Saltzer/Schroeder 1975 + Kaashoek 2009

- Sound conceptual total-system architectures with realistic implement ability and composition/layered assurance
- Hierarchically layered assurance
- Intentional use; small trusted computing base
- Make security & resilience transparent

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

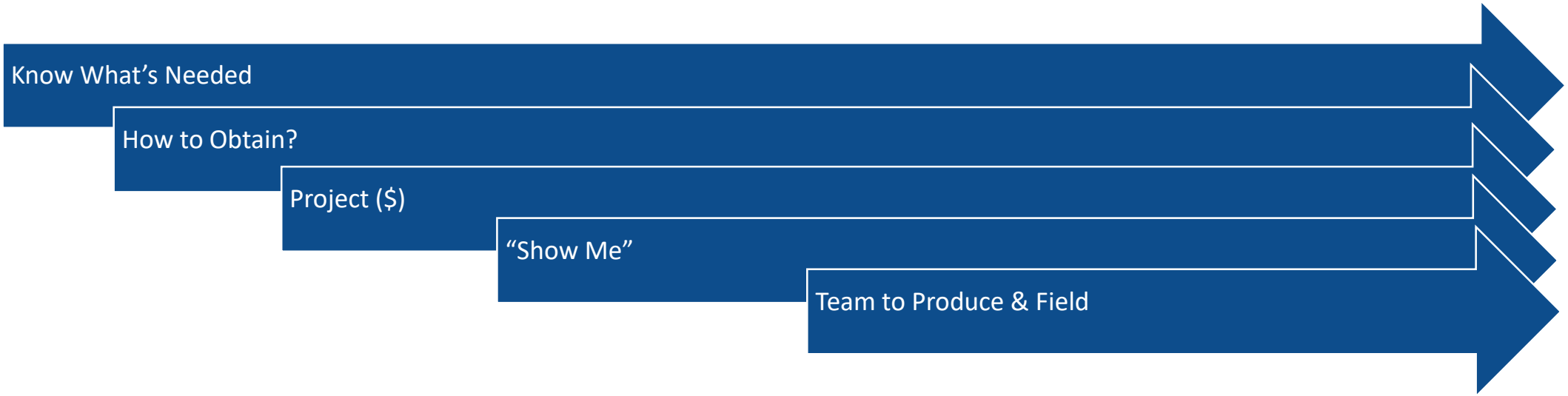
Trusted Systems; Right Capability at Right Layer



DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

Full Cycle

- Knowledge & Understanding
- Requirements
- Forecasts
- Evidence
- Partnerships
- Certification & Validation



DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

Summary

- HACMS → ARES → CASE → ARCOS → HADES
- Teaming and Partnerships are Key
- Build on Success
- Flexible Assured Systems
- Innovate with Evidence

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327

Questions?

douglas.schafer.6@us.af.mil

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number 88ABW-2019-4327