CyBOK

Topic Guide on Cloud Security

Andrew Martin
CyBOK Executive Board/University of Oxford

contact@cybok.org
www.cybok.org

Cloud Security

CyBOK

- Several suggestions that CyBOK needs some collected material on Cloud Security
- Clearly many aspects covered by existing KAs
- Broad topic – but one of considerable interest to many groups

- Identified some practitioner, business, and academic experts
- Scoping Workshop
- Document review

Cloud Security: Findings

CyBOK

- Good scope for a topic guide
- Cloud has security distinctives
  - shared responsibility model
  - distinctive abstractions
  - cloud architecture framework(s)
  - particular threat model
  - ‘everything’ virtualized

- Significant existing KA links
  - Operating Systems & Virtualization
  - Network Security
  - Law and Regulation
  - Hardware Security
  - Distributed Systems Security

as well as AAA, SecOps, Secure Systems Development, Lifecycle

Cloud Security Topic Guide
Indicative Table of Contents

CyBOK

- **Models of cloud computing and their security implications**
  - Public, private, hybrid, etc.
  - IaaS, PaaS, FaaS, SaaS
  - Shared responsibility between user and cloud provider (HW vendor, data centre operations, system integrator, software vendor., etc.) ; assets and accountability of each
  - Multi-tenant security (defining the threat model)
  - Security boundaries
  - Identity and access management in the cloud
- **Virtualization**
  - Virtualization of storage, networking, GPUs, etc.
  - Containers etc.
- **Networking**
  - Virtual networks in cloud environments (e.g., segmentation, internal vs external routing, etc.)
- **Compliance and data sovereignty**
  - Cloud provider compliance
- **Data security**
  - Data encryption at rest and in use
  - Assurance and verification
  - Secure key management and release
  - Physical data centre security
- **Confidential Computing**
  - Confidential Computing in cloud settings
  - Attestation and attestation services
- **Dev-Ops/Dev-Sec-Ops**
  - How does this change in the cloud setting?
  - Software supply chain
  - Automated tooling
  - Hybrid scenarios
- **Security monitoring and forensics**
  - How does this change in the cloud setting?
  - Data collection and preservation challenges
- **Configuration management and integration**
  - Shared responsibility model
  - Patching, vulnerability response etc.
  - Security posture management
  - Continuous controls monitoring

Cloud Security Topic Guide
Next steps

CyBOK

- currently identifying potential authors and reviewers
- will invite an author to produce a 'strawman' outline
  - including detailed cross-references to existing KAs
- to be reviewed by nominated reviewers
- then edit/finalize cycle, again with reviews
- publish

- Reflections
  - much localized expertise; fewer have the big picture
  - a lot of the knowledge is in the practitioner community
  - established architecture models, but few standard textbooks or seminal papers
  - let me know if you can fill gaps!


CyBOK