University of BRISTOL

CyBOK

Cyber Security Body of Knowledge: Distributed Systems Security

Neeraj Suri
Systems Security Group
Lancaster Univ, UK

bristol.ac.uk

University of BRISTOL

CyBOK

© Crown Copyright, The National Cyber Security Centre 2021. This information is licensed under the Open Government Licence v3.0. To view this licence, visit http://www.nationalarchives.gov.uk/doc/open-government-licence/.

When you use this information under the Open Government Licence, you should include the following attribution: CyBOK Distributed Systems Security Knowledge Area Issue 1.0 © Crown Copyright, The National Cyber Security Centre 2021, licensed under the Open Government Licence http://www.nationalarchives.gov.uk/doc/open-government-licence/.

The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at contact@cybok.org to let the project know how they are using CyBOK.

bristol.ac.uk

CyBOK

Security

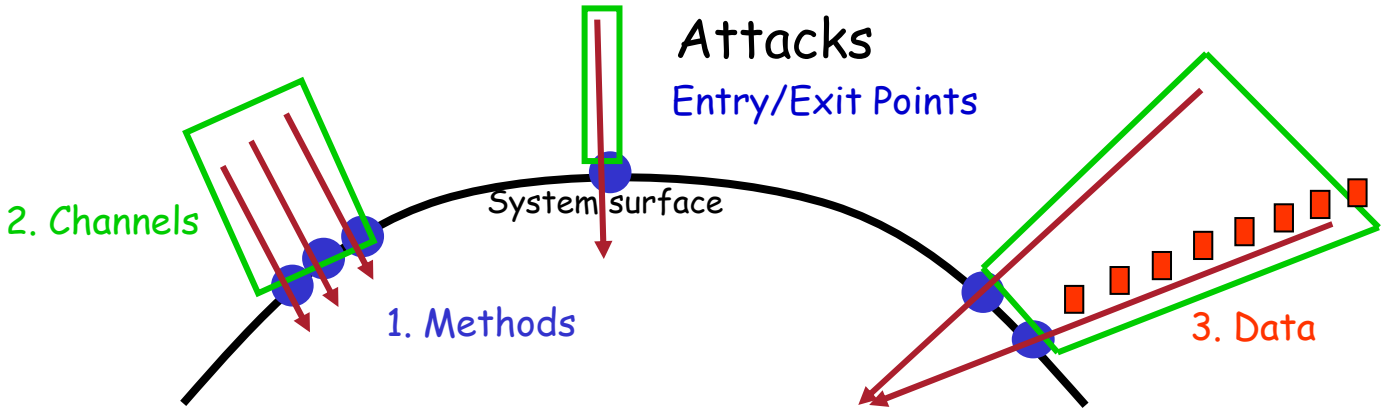
- Provisioning of desired (security) properties despite attacks

- Typical security properties
  - Confidentiality
  - Integrity
  - Availability
  - Reputation
  - Non repudiation
  - …

Security Process

- For a given artifact as a component, a protocol, a system – abstract and/or its realization – ascertain its Attack Surface (AS)
  - "Degree of exposure of being attacked"
  - The attack surface of a system outlines the ways in which an adversary can enter/exit a system to potentially cause damage

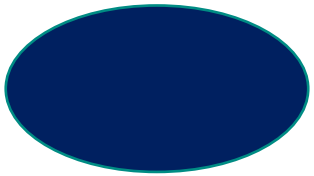
Attack Surface Measurement: Identify relevant resources (methods, channels, and data) + estimate the contribution of each such resource



bristol.ac.uk

An Attack Surface Metric", Manadhata & Wing, IEEE TSE'11

The Security Process: Single Artifact



The Security process → Determine the AS for the artifact

- Determine the vulnerabilities
- Determine the threats
- Protect against them

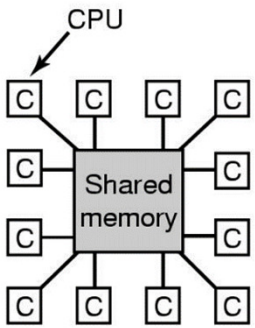
From Single to Distributed

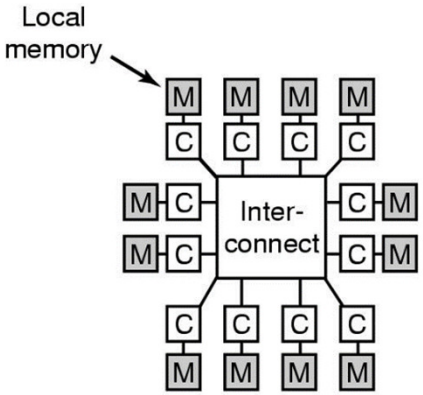
- Volume, throughput, latency, concurrency
- Scale, geo-distributed access across dispersed data producers and consumers
- On-demand, highly-available, highly-reliable access to services

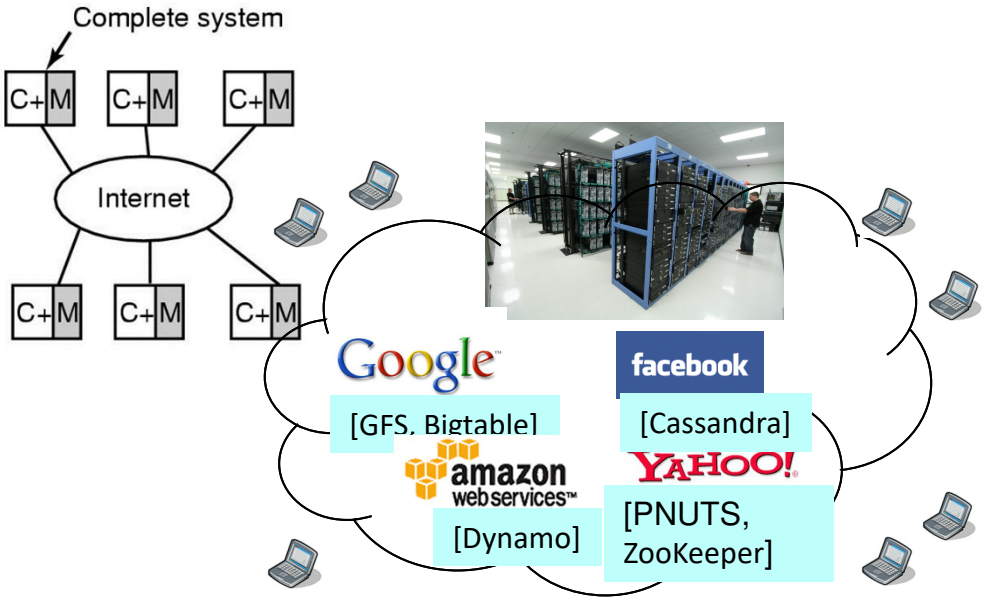
So, what's a Distributed System (DS)?

"A collection of **resources** (OS's, Servers, Storage, Databases, apps..) interlinked by **communication** (data/info) mechanisms to provide the desired services"

→ *Collective of data producers and consumers*







CyBOK

The Security Process… is still the same

- Determine the vulnerabilities
- Detect the threats
- Protect against them

The AS now encompasses the

- DS structures: The distributed resources + their linkages
- DS operations: The distributed services

CyBOK

DS Functionality

Orchestration of the distributed resources such that the user can transparently access the enhanced services arising from the collation of resources without having to deal with the technical mechanisms "handling" the distributed resources and services.

- *Illusion of a logically centralized/coordinated resource or service*

- Resource access
- Data transfers across distributed resources/producers/consumers
- Resource/Service Coordination
- Property based data management

DS Security – What type?

1. Technology solutions where *distribution is a means of providing security* e.g., dispersal of keys vs a centralized store
2. Concepts and mechanisms underlying the *secure delivery of distributed functionality*. Focus on operational structures → Security at the architectural/system levels

- A distributed system is an aggregation of multiple layers – functional and technology!

Types of DS

- Decentralized Control
  - Direct interactions across distributed entities without a centralized controller
- Coordinated Control
  - Across the distributed resources
  - Across the distributed services

DS functions …and disruptions?

- Resource access: Masquerading or identify spoofing for access. Denial of Service (DoS) attacks that detrimentally limit access (e.g., depletion of computing resources and communication channels) → inaccessibility and unavailability of the distributed resources/services
- Data transfers: Network threats routing, message passing, the publish-subscribe modalities of resource interaction, event-based response triggering, and threats across the middleware stack
- Ops for coordination of resources/services (DS - illusion of a single, consistent, reliable centralized): Threats to synchronisation, replication management, view changes, time/event ordering, linearizability, consensus, transactional commit…
- Data Security: Data at rest, data in motion, data-sourcing, data-distribution, data-storage, or data-usage in services

CyBOK

Type I: Decentralized Peer to Peer(P2P)

- Direct message passing across entities
- Inter-changeable server/client roles across peers
- Scalable with low infrastructure costs/dependencies
- Resilience to peer and communication failures
- Data and service survivability through replication
- Heterogeneity of resource provisioning among peers

➢ Decentralized → No central coordinating entity

CyBOK

Basic P2P Operations

- Resource/Data Dissemination
- Resource/Data Discovery

Types of P2P

- **Unstructured**: Geared towards efficient large-scale data dissemination. No structured addressing - search by name/labels e.g., Freenet, Gnutella…
- **Structured**: Geared towards efficiency of data discovery. Topological support/DHT's, e.g., Chord, Pastry, Kad, CAN…
  - Hybrid
  - Hierarchical

P2P Ops and Attack Surface

Basic P2P Operations:

- Naming of peers
- Routing across peers
- Discovery of peers

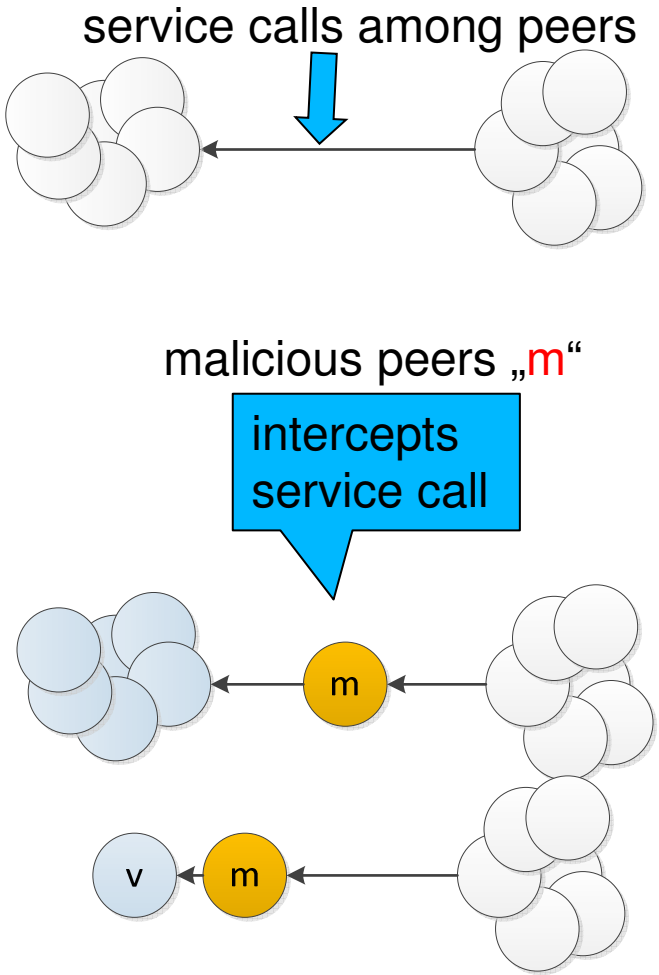
Exposure of:

- P2P Operations (P-OP) Discovery, query, routing, download. Functionality typically relates to the network level
- P2P Data Structures (P-DS) Data, shared with other peers, stored in a peer's routing table or resources. Accessible locally on the peer's host machine or at the network level

P2P Security?

- Attacks against individual peers
- Attacks against communication strata
  - General attacks as denial-of-service, pollution, routing...
  - Specific P2P attacks, e.g., Eclipse or Sybil
    - Partition of the P2P overlay network
    - Peers prevented from service provision
    - Affects availability, integrity, confidentiality

Eclipse Attack



P2P Attacks

Attack	Availability	Integrity	Confidentiality	Functionality
DoS/DDoS	✓	✗	✗	P-OP
Collusion	✓	✓	✓	P-OP
Pollution	✗	✓	✗	P-DS
White washing & censorship	✓	✓	✗	P-DS
Routing	✓	✓	✗	P-DS
Buffer map cheating	✓	✓	✗	P-OP
Sybil	✓	✗	✓	P-OP
Eclipse	✓	✓	✓	P-DS, P-OP

Distributed Systems

- Technology level – Implementations (System Stack)
- Functional level – Operational structures

Discrete DS?

- Multitude of distributed systems where interactions across the distributed resources and services are orchestrated using coordination mechanisms that provide the illusion of a “logically” centralized system or service → Coordination

CyBOK

Type II: Coordinated Resources/Services

- Coordination of Resources Service is replicated on distributed resources to enable geo-dispersed access to users while sustaining the required type of consistency specifications on the service. Cloud, Client-Server systems
  - **Focus is on resources not services**
- Coordination of Services Dispersed service participants interact to yield the collective distributed service for given consistency requirements. e.g., transactional databases and distributed ledgers for strong consistency. Web crawlers, searches, or logistics applications for weak consistency specifications.
  - **Focus is on service not resources**

- Coordination Styles: Synchronous, Asynchronous, Hybrid
- Coordination properties: Consensus, Group Membership, Consistency

Recall Basic DS Characteristics

- Services linking geo-dispersed computing resources as data producers and consumers
- High-availability via fault tolerant replication to cover resource (computing and communication) failures
- Collective aggregated capability (computational or services) from the distributed resources to provide (an illusion of) a logically centralized/ coordinated resource or service

DS Disruption Classes?

Disruption of the resources, communication, interfaces, and/or data that either impairs the resource availability or disrupts the communication layer interconnecting the resources to impact C.I.A of the overall system and its services. (Access Control, Data Distribution, Interfaces, Coordination)

- Timing based: Omission of messages, early, delayed, or out-of-order messaging. Crashes, denial-of-service → disruptions of the proper temporal delivery of messages by obstructing access to the communication channels or resources
- Value based: Spoofing attacks, mimicking, duplication, information leakage (CSA, SCA) → Content manipulation
- Persistence: Transient, episodic, intermittent, or permanent in nature.
- Concurrency: combination of timing, value, persistence, and dispersed locations, potentially due to collusion between multiple attacking entities.

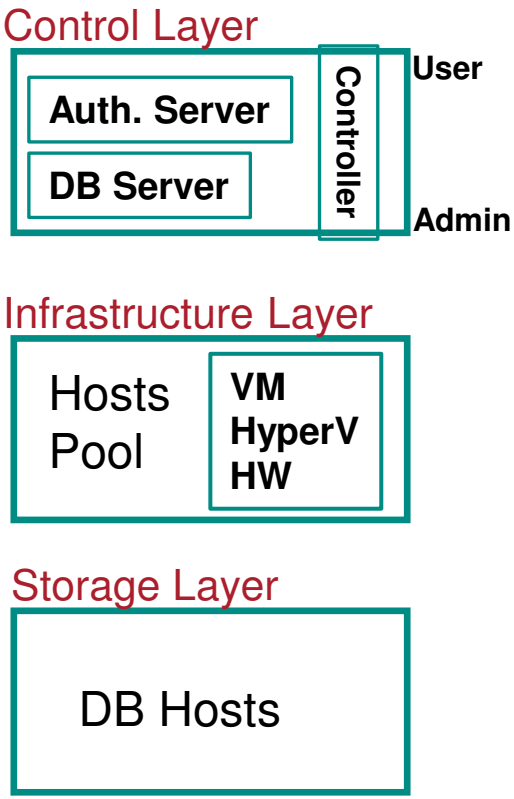
Causes (arise over the AS) → Effects (transpire on CIA) → Mitigation typically handled by replication management & coordination schemas (CAP, Paxos, BFT, Commit…)

DS 1: Resource Coordination

- Cloud Models: Resource platforms (Elastic, Available, Reliable)
  - Aggregation of geo-dispersed resources
  - User transparent to composition, location and resource access mechanisms
- Client-Server Models: Resource groups that provide services
  - Dedicated entities (servers – service providers) provide a specified service (e.g., Web services – file system servers, name servers, databases, data miners, web crawlers, etc.) to a set of data consumers (clients)
  - Communication/middleware infrastructures link servers to the clients
  - Servers and clients are replicated to provide a collective distributed service or for fault tolerance

Cloud Ops

- Customer authentication
- Resource access/brokering
- VM invocation/allocation
- VM resource/storage binding
- Scheduling/monitoring/balancing
- Dynamic adaptations
- Accounting
- …



Compromises of DS Functionality

- Compromise of resources
- Compromise of access/admission control
- Compromise of broker
- Compromise of VM
- Compromise of scheduler
- Compromise of communication
- Compromise of monitoring and accounting

DS 2: Service Coordination

CyBOK

Service type determines the supporting resources & coordination

- Web Services: Data mining, web crawlers, information servers…
  Weak/Eventual consistency
- Key Distribution: Strong consistency
- Storage/KVS: Strong consistency
- Transactional: ACID
- Blockchain: Strong consistency

Security Compromises

- Key distribution: Compromise of PK authentication process. Affects service Integrity and Confidentiality.
- Data at rest: Storage integrity compromises
- Data in motion
  - Short transactions E.g., KVS. Need: Strong consistency/low latency. DoS affects latency → loss of integrity
  - Long transactions E.g., Blockchains: Need: Integrity. DoS, compromise of crypto keys, collusion attacks affecting PoW
  - Mixed transactions E.g., e-commerce: Need: Integrity, Availability
    E.g., data retrieval: Need: Weak Consistency/Latency → Integrity and/or Availability

Summary

- Determine the functional blocks of the DS
- Determine the corresponding AS
- Determine the effects (from a CIA perspective) that arise from perturbation of the DS functionality

➢ The essence is to understand the DS functionality in order to understand the security impact of their getting disrupted!