2018-05-18 SAFE Meeting Notes

Working Group Proposal: Safe Access for Everyone (SAFE)

Attendance (PLEASE ADD YOURSELF):

- Dan Shaw, security expert, Node.js
- Doug Davis, IBM
- Mark Underwood, Synchrony
- Arnab Roy, Fujitsu US
- Christian Kemper, Google Cloud Security
- Rachel Myers, Google Policy (Firebase)

Agenda:

- Attendance/Check-in
- (As needed) Check-in from partner SIGs and WGs
    - Kubernetes SIG-Auth
    - Kubernetes Policy WG
    - NIST Big Data WG
- PR yourself as a member on https://github.com/cn-security/safe
- SAFE WG Scheduling Use Cases

Notes (Please anyone feel free to join in shared note-taking):

- Scribes:
    - Mark
    - Dan
- Links:
    - Meeting video recording: https://www.dropbox.com/s/mdhy0rqjswjwgch/zoom_0.mp4?dl=0

Mark-Transcription

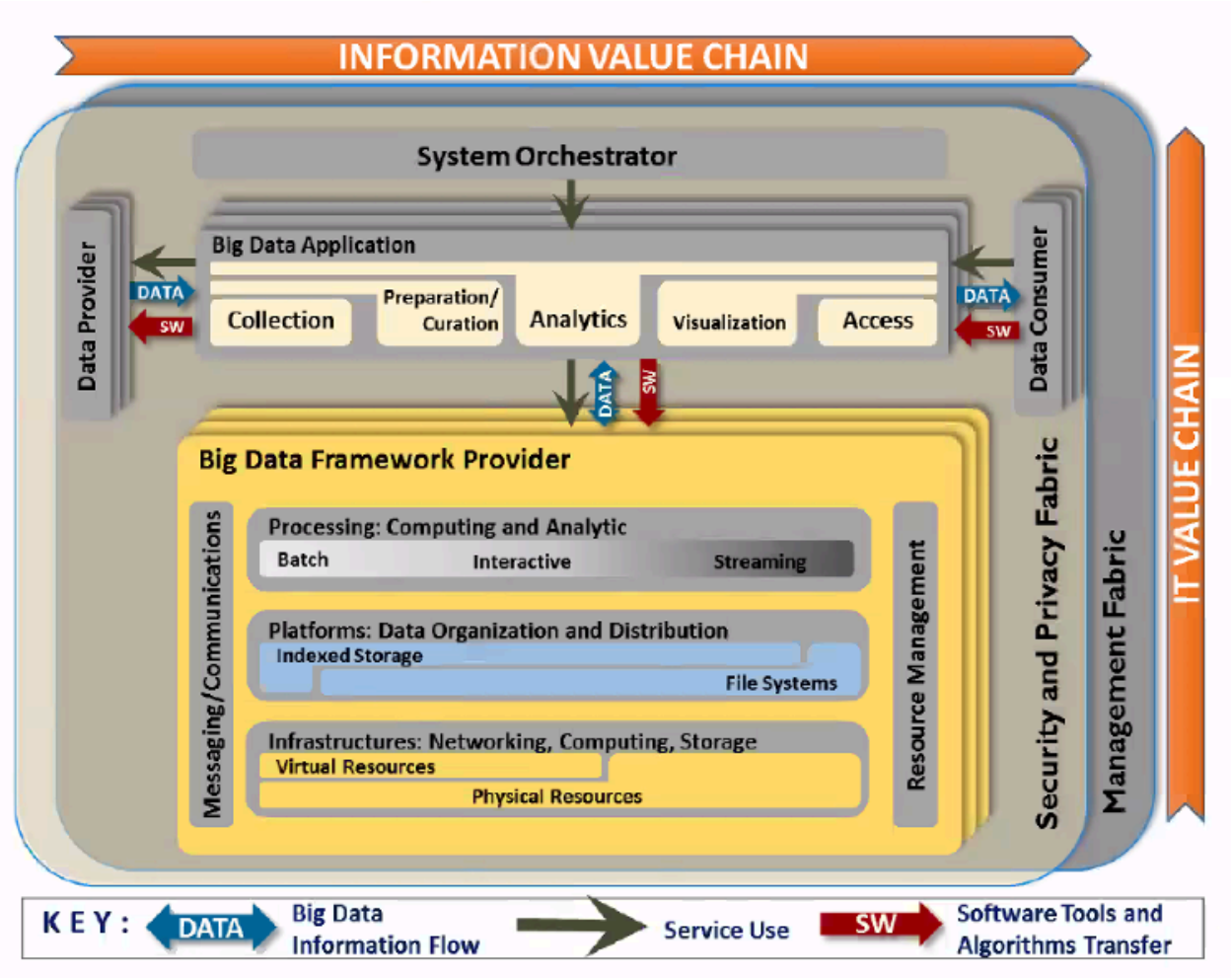
Notes from the SIGs? None.

NIST Big Data Public Working Group (NBDPWG https://bigdatawg.nist.gov/)
Contact for Dr. Roy aroy@fujitsu.us

Arnab notes that perhaps this presentation will be weak on use cases for now (we can do this as a later task).
Dan summarized the SAFE group mission for Arnab.
Arnab suggests there will be a crosswalk for analogies that apply to the two groups (Mark: e.g., orchestration).

- Possible commonalities:
  - Scalability risk
  - Cloud-Cloud “mixing” for code (e.g., infrastructure scripts), data,
    - Mixing produces emergent S&P problems include veracity, variety
  - Distributed IDM, authentication
  - Threat Models that emerge may be similar
  - Volatility associated with multi-tiered storage (Mark: zones, partitions, microsegs)
  - System health for CNative: hybridized dashboards? Manageability? Utility models for cost / performance management / operational intelligence
  - The notion of “fabric” is a central metaphor which has been embraced elsewhere, albeit not always in S&P
  - Encryption/ cert support from cloud providers and implications for SAFE
  - Federation issues and sharing of anonymous / aggregated data
- Mark proposed a family of multi-cloud, multi

There is a sharable deck.
Arnab recapped NIST SP1500 document format and objectives.
“Security and Privacy doesn’t ‘compose’”
Presented the Reference Model

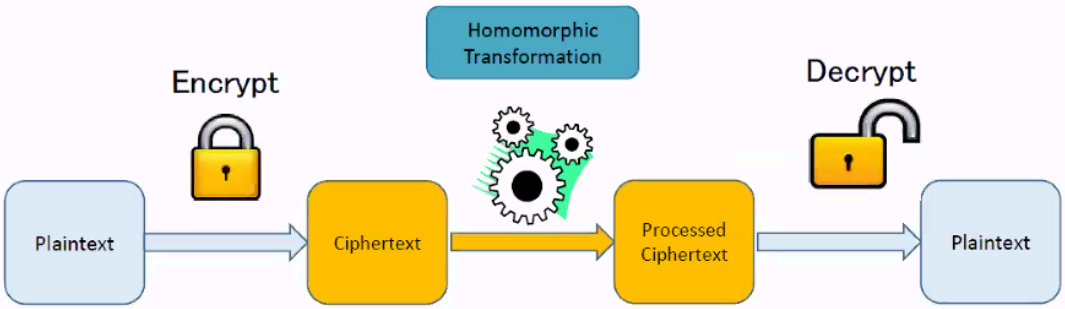


Dan asked how the NBDPWG arrived at the reference model.
Dan explains the perceived challenges of creating something similar to this for SAFE.
Arnab mentions the process for creating this deliberately simplified representation vs. the more detailed granularity of the Cloud Security Alliance (and the NIST Cloud Security effort)
Rationale: diversity of big data systems, and an awareness that “cloud” tended to background distributed systems in some readers’ minds.

Introduced: fully homomorphic encryption for Big data

Fully Homomorphic Encryption (FHE)

Sec 5.8

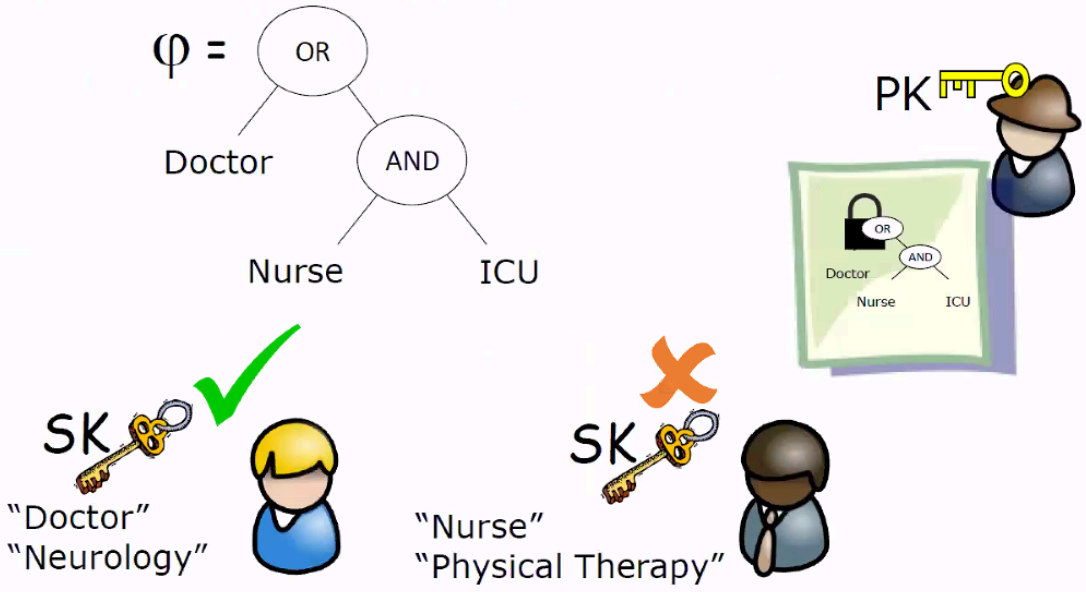


- With FHE, computation on plaintext can be transformed into computation on ciphertext
- As a use case, a cloud can keep and process customer's data without ever knowing the contents
  - Only customer can decrypt the processed data
  - End to end security of customer data

Presented access control via policy-based encryption

Policy-Based Encryption

Sec 5.8



Mitchell et al.

Mitchell et al is a good reference for this approach.

Arnab notes that there is considerable work happening in R&D for cryptography that will help with issues.

Arnab touches on the notion of a “privacy budget” in differential privacy

What is a “group signature” / Is this a future solution to anonymous / access
Dan’s Notes

NIST Big Data working group has been working for several years.
Arnab and Mark co-chair big data group
Arnab is the primary contributor on blockchain and data at rest considerations.

What is big data?

- Needed to start with a shared definition of what big data is.