**NIST Big Data Working Group (NBD-WD)**

**NBD-WD-2013/M0098**

**Source: Security and Privacy Subgroup**

**Status: Draft**

**Title: Security and Privacy Subgroup Meeting Minutes for August 7, 2013**

**Author: Arnab Roy (Fujitsu), Nancy Landreville (U. of MD), Akhil Manchanda (GE)**

**Deliverables by September 27, 2013**

1. Big Data Use Cases for Security and Privacy
2. Big Data Security and Privacy Reference Architecture

**Action Items**

Seeking contributions on use cases from all verticals. Format:

* Vertical
  + List of scenarios
  + For each scenario, current method to ensure security and privacy
  + Gaps, if any
  + Current research on the topic (Can be filled in later)

**New:**

Seeking use cases on data access policies *internal* to organizations. This may also be structured in terms of verticals.

**Discussion of Taxonomy of Security and Privacy topics and their relation to Big Data Reference Architectures.**

Taxonomy of S&P topics along a technical axis were discussed (Figure 1 below).

* Feedbacks:
  + There needs to be delineation of authorization mechanisms, authentication mechanisms and access control mechanisms.
  + Identity and Access Management
  + Roles and Responsibilities for drawing the boundary around data

S&P overlay on Big Data Reference Architecture was discussed (Figure 2 below).

* Feedbacks:
  + Include anonymization of data
  + Split along procedural aspects such as specific types of processing.
  + Include systems retirement and data destruction.

Approach on “Following the data for Security”

* Resolve ownership of data at source
  + Optional integrity
    - Digital signatures
  + Roles
    - The attributes that an entity should have to access data
  + Content
* Derive an access control policy
  + Could be part of a contract
  + Encrypted Data
    - Optional Capabilities: Search, Computation
    - Crypto-enforced policy-based access control
  + Plaintext Data
    - Data available to the collecting entity
    - Understanding of dissemination guarantees
* Feedbacks:
  + Also consider data, which may not be subject to control at outset, but acquire emergent value after analysis. What are the security implications of such a scenario and what sort of S&P mechanisms should be in place?

Figure 1

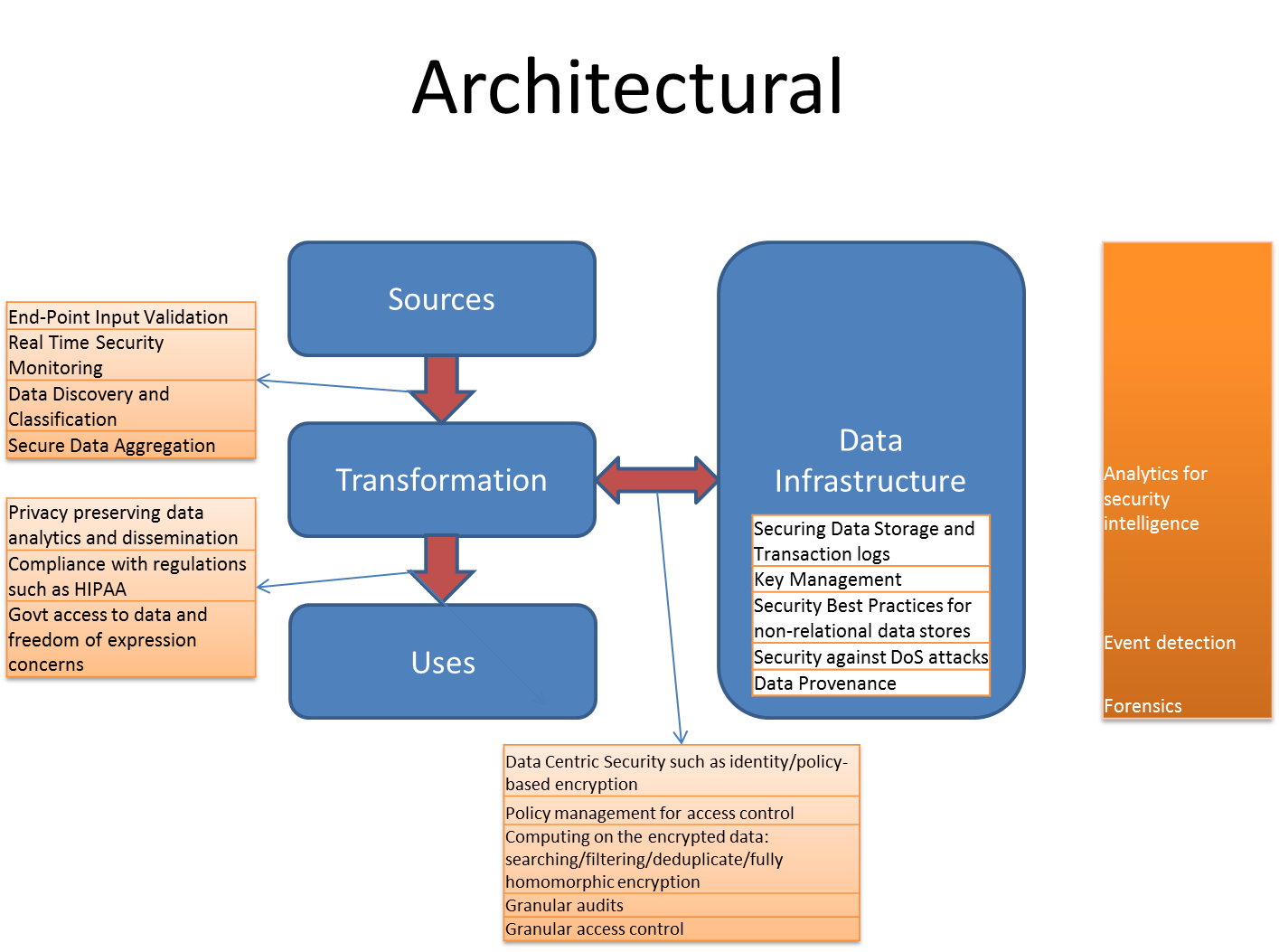


Figure 2

**Web Minutes**

(7:55 AM) Wo Chang (Host, NIST) disconnected.

(7:59 AM) Roy D'Souza(AlephCloud) joined.

(8:00 AM) William Miller (MaCT USA) joined.

(8:00 AM) Arnab Roy (Fujitsu, Host) joined.

(8:01 AM) Bob Marcus (ET-Strategies) joined.

(8:05 AM) Wo Chang (Host, NIST) joined.

(8:05 AM) Eddie Garcia (Gazzang, Inc.) joined.

(8:08 AM) Akhil Manchanda joined.

(8:10 AM) Akhil Manchanda disconnected.

(8:12 AM) Akhil Manchanda joined.

(8:14 AM) PavithraKenjige joined.

(8:15 AM) William Miller (MaCT USA) disconnected.

(8:16 AM) Marcia Mangold joined.

(8:18 AM) Orit Levin (Microsoft) joined.

(8:18 AM) Roy D'Souza(AlephCloud): Could be creator, modifier, access, etc..

(8:19 AM) Orit Levin (Microsoft): Good morning. In listening mode (on Web) only today.

(8:19 AM) Roy D'Souza(AlephCloud): I'd argue "who" woud include who created, who modified, who accessed

(8:21 AM) Marcia Mangold disconnected.

(8:22 AM) Pw Carey(Compliance Partners, LLC) joined.

(8:23 AM) Pw Carey(Compliance Partners, LLC): Any data modifications could become an issue during a forensics investigation.....

(8:24 AM) Marcia Mangold joined.

(8:24 AM) Roy D'Souza(AlephCloud): If it's public, but reference data, then there could still need to be provenance that indicates who may be able to (or may have) modified that reference data perhaps

(8:25 AM) Roy D'Souza(AlephCloud): It may be a public data set but can you trust it?

(8:25 AM) Pw Carey(Compliance Partners, LLC): This touches upon the 'security' within the cloud, in such areas as 'chain of custody'....however, any forensics investigation must rest on the 'merits' of the investigation and not on the esoteric nature of the technology.....Ok

(8:25 AM) Brent Comstock joined.

(8:26 AM) Pw Carey(Compliance Partners, LLC): Ok....understood....thank you, too....

(8:26 AM) Pw Carey(Compliance Partners, LLC): Good point....

(8:27 AM) Pw Carey(Compliance Partners, LLC): We're on Mutae....

(8:28 AM) Roy D'Souza(AlephCloud): sorry I was on mute.

(8:28 AM) Wo Chang (Host, NIST): PW: you can unmute yourself using \*6 on your phone

(8:30 AM) Marcia Mangold disconnected.

(8:31 AM) Pw Carey(Compliance Partners, LLC): 'Policies' 'People' & 'Technology' are the 3 lynch pins for data CIA & GRC.....

(8:32 AM) Pw Carey(Compliance Partners, LLC): In our opinion.....that is...

(8:33 AM) Marcia Mangold joined.

(8:34 AM) PavithraKenjige disconnected.

(8:34 AM) PavithraKenjige joined.

(8:36 AM) Pw Carey(Compliance Partners, LLC): If the CIO/CISO has

(8:36 AM) Pw Carey(Compliance Partners, LLC): Supervisory Responsibilities over the data....yes....

(8:38 AM) PavithraKenjige disconnected.

(8:38 AM) PavithraKenjige joined.

(8:39 AM) PavithraKenjige disconnected.

(8:40 AM) PavithraKenjige(PK Technologies) joined.

(8:43 AM) Eugene Luster (DISA CTO/R2AAD) joined.

(8:50 AM) Wo Chang (Host, NIST)95 joined.

(8:50 AM) Wo Chang (Host, NIST) disconnected.

(8:51 AM) Pw Carey(Compliance Partners, LLC): Yes....Control of the Data....is one aspect of our conversation regarding the differences between current IT Data Warehouses va Big Data....

(8:51 AM) Pw Carey(Compliance Partners, LLC): Sorry....we meant...."vs"....

(8:53 AM) PavithraKenjige(PK Technologies) disconnected.

(8:55 AM) PavithraKenjige (PK Technologies) joined.

(8:56 AM) Pw Carey(Compliance Partners, LLC): Me too....

(8:56 AM) Pw Carey(Compliance Partners, LLC): Your welcome....

(8:58 AM) PavithraKenjige (PK Technologies) disconnected.

(8:59 AM) PavithraKenjige (PK Technologies) joined.

(9:01 AM) Orit Levin (Microsoft): Could we add/list anonymization here?

(9:02 AM) Orit Levin (Microsoft): Thanks!

(9:02 AM) Pw Carey(Compliance Partners, LLC): How should we address the 'term limits' regarding data, such as personal data.....please note, there are criminal investigations that appear to have no statute of limitations......

(9:03 AM) Pw Carey(Compliance Partners, LLC): And possibly 'administrative' and 'civil' investigations when the dollar amount is large enough.....

(9:04 AM) Yale Li (Microsoft/CSA) joined.

(9:08 AM) Pw Carey(Compliance Partners, LLC): For some reason your voices are intermittently breaking up...but we don't any any questions at this time other than we look forward to receiving any info. regarding our Assignment.....thanks...Pw

(9:08 AM) Pw Carey(Compliance Partners, LLC): We don't have any questions at this time....

(9:10 AM) Pw Carey(Compliance Partners, LLC): One last question, how should we deal with 'system retirements' & data 'archival' & 'data destruction'......satisfying all Regulatory & Compliance obligations.....end of Pws questions....thanks...

(9:13 AM) Serge Mankovski (CA Technologies) joined.

(9:14 AM) Arnab Roy (Fujitsu, Host) disconnected.

(9:14 AM) Arnab Roy (Fujitsu, Host) joined.

(9:14 AM) Serge Mankovski (CA Technologies) disconnected.

(9:14 AM) Serge Mankovski (CA Technologies) joined.

(9:15 AM) Orit Levin (Microsoft) disconnected.

(9:17 AM) Serge Mankovski (CA Technologies) disconnected.

(9:18 AM) Serge Mankovski (CA Technologies) joined.

(9:19 AM) Pw Carey(Compliance Partners, LLC): Good point...it could be part of a Contract....along the lines of a Service Level Agreement....

(9:20 AM) Pw Carey(Compliance Partners, LLC): This looks pretty good...

(9:20 AM) Sanjay Mishra(VERIZON) joined.

(9:21 AM) PavithraKenjige (PK Technologies): Data.. has secure information .. so does big data

(9:21 AM) PavithraKenjige (PK Technologies): The security level that applies to information applies to data

(9:21 AM) Pw Carey(Compliance Partners, LLC): Include the various types of data...jpg, wav.....txt...doc...et cetera....

(9:21 AM) Brent Comstock disconnected.

(9:22 AM) Pw Carey(Compliance Partners, LLC): During forensic analysis...all these types of data come into question.....

(9:22 AM) Pw Carey(Compliance Partners, LLC): Or...play...

(9:23 AM) Pw Carey(Compliance Partners, LLC): Also, VOIP.....

(9:23 AM) Pw Carey(Compliance Partners, LLC): Not sure....good question....

(9:26 AM) PavithraKenjige (PK Technologies): Actors, roles & responsibilities about accessibility?

(9:26 AM) Pw Carey(Compliance Partners, LLC): A nasty delivery mechanism could be an image file...while the package would be an executable .exe file.....

(9:28 AM) PavithraKenjige (PK Technologies): Subject of the information and relevant security compliance

(9:32 AM) Serge Mankovski (CA Technologies): I think we are making a mistake here. We are thinking of BIg Data as "all the data". However I would think that data that requires tight security contorl is not necesserely "Big". I think the difference is exactly that -- we might draw a line where BIg Data would not require tight security and compliance control. I would say geoposition of a cell phone might be Big Data, but content of the phone address book should not be. Does it make sense?

(9:34 AM) Pw Carey(Compliance Partners, LLC): Good point....Big Data is appropriate and better that current IT solutions in some environment's requirements....highly regulated vs non-regulated...(if such a thing exists anymore....)

(9:35 AM) Pw Carey(Compliance Partners, LLC): Big Data is better at some things and not so much with other requirements....

(9:37 AM) Pw Carey(Compliance Partners, LLC): Correct....

(9:39 AM) Alicia Zuniga/Alvarado joined.

(9:39 AM) Pw Carey(Compliance Partners, LLC): Some data is appropriate for Big Data and some data is not appropriate for Big Data...

(9:40 AM) Pw Carey(Compliance Partners, LLC): Dear Serge...welcome to the Team....Respectfully yours, Pw

(9:44 AM) Sanjay Mishra(VERIZON): Welcome Serge

(9:44 AM) Arnab Roy (Fujitsu, Host) disconnected.

(9:45 AM) Arnab Roy (Fujitsu, Host) joined.

(9:45 AM) Pw Carey(Compliance Partners, LLC): I think part of our responsibiity is to make the user aware of such issues, that are not part of their job description or performance evaluation....

(9:46 AM) Pw Carey(Compliance Partners, LLC): until things go South.....

(9:47 AM) PavithraKenjige (PK Technologies): Relevant Security policy & indicator for content

(9:51 AM) PavithraKenjige (PK Technologies): Metadata for context and content??

(9:52 AM) Bob Marcus (ET-Strategies) disconnected.

(9:52 AM) Pw Carey(Compliance Partners, LLC): Me too...

(9:53 AM) Pw Carey(Compliance Partners, LLC): No...we didn't....

(9:54 AM) Pw Carey(Compliance Partners, LLC): Can we access this presentation....?

(9:57 AM) PavithraKenjige (PK Technologies): Governance policy should address roles and responsibiities

(9:57 AM) paul savitz joined.

(9:59 AM) Akhil Manchanda disconnected.

(9:59 AM) Wo Chang (Host, NIST)95: I was the one asked for the compiler security, thanks Arnab!

(10:00 AM) Pw Carey(Compliance Partners, LLC): This power point is available on the NIST Subgroup Web Site....?

(10:01 AM) Pw Carey(Compliance Partners, LLC): Ok, thank you.....

(10:01 AM) Alicia Zuniga/Alvarado disconnected.

(10:01 AM) Pw Carey(Compliance Partners, LLC): What is your email address....

(10:02 AM) Serge Mankovski (CA Technologies) disconnected.

(10:02 AM) Wo Chang (Host, NIST)95: thanks Arnab!

(10:02 AM) Yale Li (Microsoft/CSA) disconnected.

(10:02 AM) Arnab Roy (Fujitsu, Guest): aroy@us.fujitsu.com

(10:02 AM) PavithraKenjige (PK Technologies): thanks

(10:02 AM) Eddie Garcia (Gazzang, Inc.) disconnected.

(10:02 AM) Mark Underwood [Krypton Brothers] joined.

(10:02 AM) Pw Carey(Compliance Partners, LLC): Thank you....