## Title:

### Author:

## General Description of the Industry / Use Case:

<Insert general description of the use case here>

## Mapping to the Security Reference Architecture:

|  |  |  |
| --- | --- | --- |
| RA Component | Security & Privacy Topic | Use Case Mapping |
| Sources → Transformation | End-Point Input Validation |  |
| Real Time Security Monitoring |  |
| Data Discovery and Classification |  |
| Secure Data Aggregation |  |
|  |  |  |
| Transformation → Uses | Privacy-preserving Data Analytics |  |
| Compliance with Regulations |  |
| Govt access to data and freedom of expression concerns |  |
|  |  |  |
| Transformation ↔ Data Infrastructure | Data Centric Security such as identity/policy-based encryption |  |
| Policy management for access control |  |
| Computing on the encrypted data: searching/filtering/deduplicate/fully homomorphic encryption |  |
| Audits |  |
|  |  |  |
| Data Infrastructure | Securing Data Storage and Transaction logs |  |
| Key Management |  |
| Security Best Practices for non-relational data stores |  |
| Security against DoS attacks |  |
| Data Provenance |  |
|  |  |  |
| General | Analytics for security intelligence |  |
| Event detection |  |
| Forensics |  |

## Title: Nielsen Homescan

### Author: Mark Underwood

## General Description of the Industry / Use Case:

Family level retail transactions and associated media exposure utilizing a statistically valid national sample. A [general description](http://www.nielsen.com/us/en/nielsen-solutions/nielsen-measurement/nielsen-retail-measurement.html) is provided by the vendor. This project description based on the 2006 architecture.

## Mapping to the Security Reference Architecture:

|  |  |  |
| --- | --- | --- |
| RA Component | Security & Privacy Topic | Use Case Mapping |
| Sources → Transformation | End-Point Input Validation | Device-specific keys from digital sources; receipt sources scanned internally and reconciled to family ID . (Role issues) |
| Real Time Security Monitoring | None |
| Data Discovery and Classification | Classifications based on data sources (e.g.,retail outlets, devices, paper sources) |
| Secure Data Aggregation | Aggregated into demographic crosstabs. Internal analysts had access to PII. |
|  |  |  |
| Transformation → Uses | Privacy-preserving Data Analytics | Aggregated to (sometimes) product-specific statistically valid independent variables |
| Compliance with Regulations | Panel data rights secured in advance & enforced through organizational controls |
| Govt access to data and freedom of expression concerns | N/A |
|  |  |  |
| Transformation ↔ Data Infrastructure | Data Centric Security such as identity/policy-based encryption | Encryption not employed in place; only for data center to data center transfers. XML cube security mapped to Sybase IQ, reporting tools. |
| Policy management for access control | Extensive role-based controls |
| Computing on the encrypted data: searching/filtering/deduplicate/fully homomorphic encryption | N/A |
| Audits | Schematron, process step audits |
|  |  |  |
| Data Infrastructure | Securing Data Storage and Transaction logs | Project-specific audits secured by infrastructure team |
| Key Management | Managed by project CSO. Separate key pairs issued for customers, internal users |
| Security Best Practices for non-relational data stores | Regular data Integrity checking via XML schema validation |
| Security against DoS attacks | Industry standard webhost protection provided for query subsystem. |
| Data Provenance | Unique |
|  |  |  |
| General | Analytics for security intelligence | No project-specific initiatives |
| Event detection | N/A |
| Forensics | Usage, cube-creation, device merge audit records were retained for forensics & billing. |

## Title: Pharma Clinical Trial Data Sharing

### Author: Mark Underwood

## General Description of the Industry / Use Case:

## Under an industry trade group proposal, clinical trial data for new drugs will be shared outside intra-enterprise warehouses. Regulatory submissions commonly exceed “millions of pages.”

## Mapping to the Security Reference Architecture:

|  |  |  |
| --- | --- | --- |
| RA Component | Security & Privacy Topic | Use Case Mapping |
| Sources → Transformation | End-Point Input Validation | Opaque – company-specific |
| Real Time Security Monitoring | None |
| Data Discovery and Classification | Opaque – company-specific |
| Secure Data Aggregation | 3rd party aggregator |
|  |  |  |
| Transformation → Uses | Privacy-preserving Data Analytics | Data to be reported in aggregate but preserving potentially small-cell demographics |
| Compliance with Regulations | Responsible developer & 3rd party custodian |
| Govt access to data and freedom of expression concerns | None considered: research limited community use; possible future public health data concern. Clinical Study Reports only, but possibly selectively at study-, patient-level |
|  |  |  |
| Transformation ↔ Data Infrastructure | Data Centric Security such as identity/policy-based encryption | TBD |
| Policy management for access control | Internal roles; 3rd party custodian roles; researcher roles; participating patients’ physicians |
| Computing on the encrypted data: searching/filtering/deduplicate/fully homomorphic encryption | TBD |
| Audits | Release audit by 3rd party |
|  |  |  |
|  | Securing Data Storage and Transaction logs | TBD |
| Key Management | Internal varies by firm; external TBD |
| Security Best Practices for non-relational data stores | TBD |
| Security against DoS attacks | Unlikely to become public |
| Data Provenance | TBD – critical issue |
|  |  |  |
| General | Analytics for security intelligence | TBD |
| Event detection | TBD |
| Forensics |  |

## Title: Large Network Cybersecurity SIEM

### Author: Mark Underwood

## General Description of the Industry / Use Case:

Security Information and Event Management (SIEM) is a family of tools used to defend and maintain networks.

## Mapping to the Security Reference Architecture:

|  |  |  |
| --- | --- | --- |
| RA Component | Security & Privacy Topic | Use Case Mapping |
| Sources → Transformation | End-Point Input Validation | Software-supplier specific; e.g., <http://support.microsoft.com/kb/323076> |
| Real Time Security Monitoring |  |
| Data Discovery and Classification | Varies by tool, but classifies based on security semantics, sources |
| Secure Data Aggregation | Varies: subnet, workstation, server |
|  |  |  |
| Transformation → Uses | Privacy-preserving Data Analytics | Platform-specific; example: Windows groups |
| Compliance with Regulations | Applicable, but regulated events not readily visible to analysts |
| Govt access to data and freedom of expression concerns | NSA, FBI access on demand |
|  |  |  |
| Transformation ↔ Data Infrastructure | Data Centric Security such as identity/policy-based encryption | Usually feature of O.S. |
| Policy management for access control | E.g.: Windows group policy for event log |
| Computing on the encrypted data: searching/filtering/deduplicate/fully homomorphic encryption | Vendor, platform-specific |
| Audits | Complex – audits possible throughout |
|  |  |  |
| Data Infrastructure | Securing Data Storage and Transaction logs | Vendor, platform-specific |
| Key Management | CSO, SIEM product keys |
| Security Best Practices for non-relational data stores | TBD |
| Security against DoS attacks | N/A |
| Data Provenance | E.g., how know an intrusion record was actually associated w/ specific workstation |
|  |  |  |
| General | Analytics for security intelligence | Feature |
| Event detection | Feature |
| Forensics | Feature |

## Title: Consumer Digital Media Usage

### Author: Mark Underwood

## General Description of the Industry / Use Case:

## Content owners license data for usage by consumers through presentation portals, e.g., Netflix, iTunes, etc. Usage is Big Data, including demographics at user level, patterns of use such as play sequence, recommendations, content navigation.

## Mapping to the Security Reference Architecture:

|  |  |  |
| --- | --- | --- |
| RA Component | Security & Privacy Topic | Use Case Mapping |
| Sources → Transformation | End-Point Input Validation | Varies, vendor-dependent. Spoofing is possible. E.g., Protections afforded by securing [Microsoft Rights Management Services](http://bit.ly/14LdzU1). S/MIME |
| Real Time Security Monitoring | Content creation security |
| Data Discovery and Classification | Discovery / classification possible across media, populations, channels |
| Secure Data Aggregation | Vendor-supplied aggregation services – security practices opaque |
|  |  |  |
| Transformation → Uses | Privacy-preserving Data Analytics | Aggregate reporting to content owners |
| Compliance with Regulations | PII disclosure issues abound |
| Govt access to data and freedom of expression concerns | Various issues, e.g, playing terrorist podcast, illegal playback |
|  |  |  |
| Transformation ↔ Data Infrastructure | Data Centric Security such as identity/policy-based encryption | unknown |
| Policy management for access control | User, playback admin, library maintenance, auditor |
| Computing on the encrypted data: searching/filtering/deduplicate/fully homomorphic encryption | Unknown |
| Audits | Audit DRM usage for royalties |
|  |  |  |
| Data Infrastructure | Securing Data Storage and Transaction logs | unknown |
| Key Management | unknown |
| Security Best Practices for non-relational data stores | unknown |
| Security against DoS attacks | N/A? |
| Data Provenance | Traceability to right entities to be preserved. (Add’l use case: Wikipedia privacy issues when distributing data to researchers) |
|  |  |  |
| General | Analytics for security intelligence | Machine intelligence for unsanctioned use/access |
| Event detection | “Playback” granularity defined |
| Forensics | Subpoena of playback records in legal disputes |

## Title: Unmanned Military Vehicle Sensor Systems

### Author: Mark Underwood

## General Description of the Industry / Use Case:

## Unmanned vehicles (“drones”) and their onboard sensors (e.g., streamed video) can produce petabytes of data that must be stored in nonstandard formats. Refer to [DISA large data object contract](http://gcn.com/articles/2013/04/12/disa-plans-exabytes-large-data-objects.aspx) for exabytes in DoD private cloud.

## Mapping to the Security Reference Architecture:

|  |  |  |
| --- | --- | --- |
| RA Component | Security & Privacy Topic | Use Case Mapping |
| Sources → Transformation | End-Point Input Validation | Need to secure sensor (e.g., camera) to prevent spoofing/stolen sensor streams. New transceivers, protocols in DoD pipeline. Sensor streams to include smartphone, tablet sources |
| Real Time Security Monitoring | On-board & control station secondary sensor security monitoring |
| Data Discovery and Classification | Varies from media-specific encoding to sophisticated situation-awareness enhancing fusion schemes. |
| Secure Data Aggregation | Fusion challenges range from simple to complex. Video streams [may be used](http://defensesystems.com/articles/2012/10/31/agg-drone-video-encryption-lags.aspx) unsecured, unaggregated. |
|  |  |  |
| Transformation → Uses | Privacy-preserving Data Analytics | Geospatial constraints: cannot surveil beyond a UTM. Military secrecy: target, point of origin privacy. |
| Compliance with Regulations | Numerous. Also standards issues. |
| Govt access to data and freedom of expression concerns | See Google lawsuit over Street View. |
|  |  |  |
| Transformation ↔ Data Infrastructure | Data Centric Security such as identity/policy-based encryption | Policy-based encryption, often dictated by legacy channel capacity/type |
| Policy management for access control | Transformations tend to be made within DoD-contractor devised system schemes. |
| Computing on the encrypted data: searching/filtering/deduplicate/fully homomorphic encryption | Sometimes performed within vendor-supplied architectures, or by image-processing parallel architectures. |
| Audits | CSO, IG audit |
|  |  |  |
| Data Infrastructure | Securing Data Storage and Transaction logs | The usual, plus data center security levels are tightly managed (e.g., field vs. battalion vs. HQ) |
| Key Management | CSO – chain of command |
| Security Best Practices for non-relational data stores | Not handled differently at present; this is changing in DoD. |
| Security against DoS attacks | DoD anti-jamming e-measures. |
| Data Provenance | Must track to sensor point in time configuration, metadata. |
|  |  |  |
| General | Analytics for security intelligence | DoD develops specific field of battle security software intelligence – event driven, monitoring – often remote. |
| Event detection | E.g.: target identification in a video stream, infer height of target from shadow. Fuse data from satellite IR with separate sensor stream. |
| Forensics | Used for AAR (after action review) – desirable to have full playback of sensor streams. |

## Title: Common Core K-12 Student Reporting

### Author: Mark Underwood

## General Description of the Industry / Use Case:

Cradle-to-grave student performance metrics for every student are now possible – at least within the K-12 community and probably beyond. This could include every test result ever administered.

## Mapping to the Security Reference Architecture:

|  |  |  |
| --- | --- | --- |
| RA Component | Security & Privacy Topic | Use Case Mapping |
| Sources → Transformation | End-Point Input Validation | Application-dependent. Spoofing is possible. |
| Real Time Security Monitoring | Vendor-specific monitoring of tests, test-takers, administrators & data. |
| Data Discovery and Classification | unknown |
| Secure Data Aggregation | Typical: Classroom level |
|  |  |  |
| Transformation → Uses | Privacy-preserving Data Analytics | Various: e.g., teacher level analytics across all same-grade classrooms. |
| Compliance with Regulations | Parent-, student-, taxpayer disclosure & privacy rules apply |
| Govt access to data and freedom of expression concerns | Yes. May be required for grants, funding, performance metrics for teachers, administrators, districts. |
|  |  |  |
| Transformation ↔ Data Infrastructure | Data Centric Security such as identity/policy-based encryption | Support both individual access (student) & partitioned aggregate |
| Policy management for access control | Vendor (e.g., Pearson) controls, state level policies, federal level policies; probably 20-50 roles? |
| Computing on the encrypted data: searching/filtering/deduplicate/fully homomorphic encryption | unknown |
| Audits | Support 3rd party audits by unions, state agencies, resp to subpoenas |
|  |  |  |
| Data Infrastructure | Securing Data Storage and Transaction logs | Large enterprise security, trx controls – classroom to Feds |
| Key Management | CSO’s from classroom level to national |
| Security Best Practices for non-relational data stores | unknown |
| Security against DoS attacks | standard |
| Data Provenance | Traceability to measurement event requires capturing tests @ point in time |
|  |  |  |
| General | Analytics for security intelligence |  |
| Event detection |  |
| Forensics |  |

## Title: Web Traffic Analytics

### Author: Mark Underwood

## General Description of the Industry / Use Case:

## Visit-level webserver logs are high-granularity and voluminous. Web logs are correlated with other sources, including page content (buttons, text, navigation events), and marketing events such as campaigns, media classification.

## Mapping to the Security Reference Architecture:

|  |  |  |
| --- | --- | --- |
| RA Component | Security & Privacy Topic | Use Case Mapping |
| Sources → Transformation | End-Point Input Validation | Device-dependent. Spoofing often easy. |
| Real Time Security Monitoring | Webserver monitoring |
| Data Discovery and Classification | Some geospatial attribution |
| Secure Data Aggregation | Aggregation to device, visitor,button,web event, others |
|  |  |  |
| Transformation → Uses | Privacy-preserving Data Analytics | IP anonymizing, timestamp degrading. Content-specific opt-out. |
| Compliance with Regulations | Anonymization may be required for EU compliance. Opt-out honoring. |
| Govt access to data and freedom of expression concerns | Yes. |
|  |  |  |
| Transformation ↔ Data Infrastructure | Data Centric Security such as identity/policy-based encryption | Varies depending on archivist. E.g., Adobe Omniture |
| Policy management for access control | System-, application-level access controls |
| Computing on the encrypted data: searching/filtering/deduplicate/fully homomorphic encryption | unknown |
| Audits | Customer audits for accuracy, integrity supported |
|  |  |  |
| Data Infrastructure | Securing Data Storage and Transaction logs | Storage archiving – big issue |
| Key Management | CSO + applications |
| Security Best Practices for non-relational data stores | unknown |
| Security against DoS attacks | Standard |
| Data Provenance | Server, application, IP-like identity, page point-in-time DOM, point-in-time marketing events |
|  |  |  |
| General | Analytics for security intelligence | Access to web logs often requires priv elevation. |
| Event detection | Can infer e.g., numerous sales, marketing & overall web health events |
| Forensics | See SIEM use case. |