Digital Preservation

Authenticity and Provenance

Stefan Pröll

Outline

- Trust in digital archives
  - Why do archives need to be trustworthy
- Authenticity
  - What does authenticity mean
- Provenance
  - How to map the genealogy of digital data
- Metadata for authenticity and provenance
- Security
  - How to secure archives and their content

The Concept of Trust

- Archives store digital objects. They need to be:
  - Safe
  - Reliable
  - Trustworthy
- Trust is a fundamental property of digital archives
  - Trust is hard to establish
  - Easy to destroy
- How to establish trust?

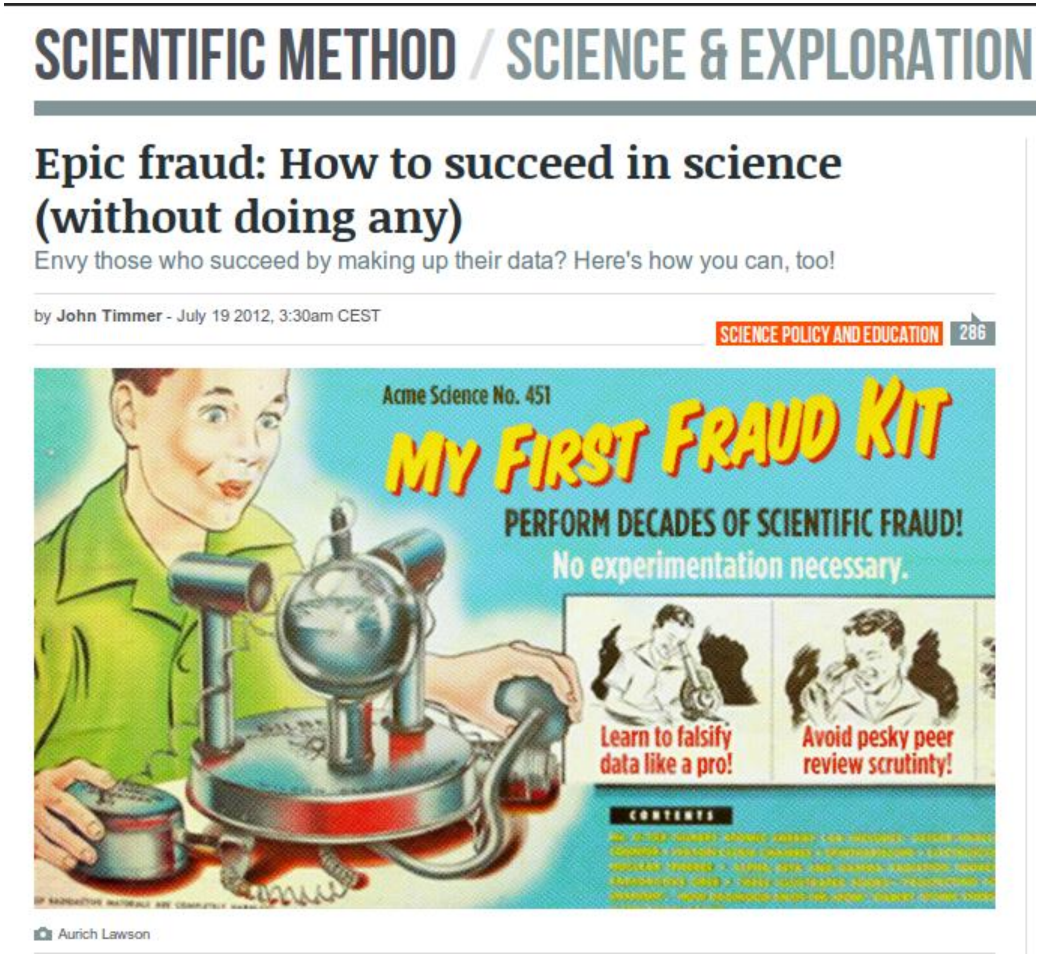
Authenticity

- What is Authenticity?

http://weird.cz/ali-g

- Authenticity: The degree a digital object actually is what it claims to be.
- Authenticity is judged on the basis of evidence

Epic Fraud



SCIENTIFIC METHOD / SCIENCE & EXPLORATION

Epic fraud: How to succeed in science (without doing any)

Envy those who succeed by making up their data? Here's how you can, too!

by **John Timmer** - July 19 2012, 3:30am CEST

SCIENCE POLICY AND EDUCATION 286

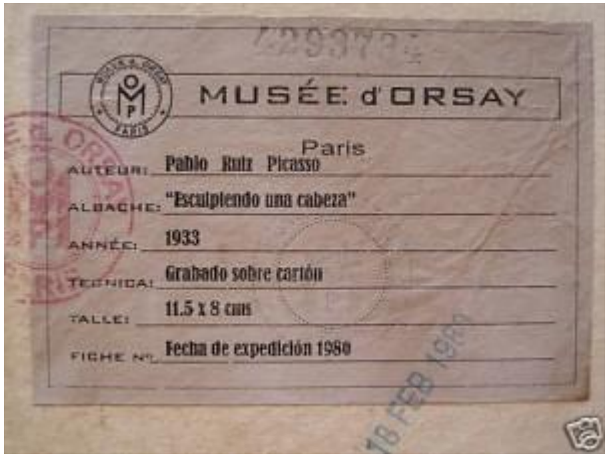
Acme Science No. 451
MY FIRST FRAUD KIT
PERFORM DECADES OF SCIENTIFIC FRAUD!
No experimentation necessary.
Learn to falsify data like a pro!
Avoid pesky peer review scrutinty!
CONTENTS

Aurich Lawson

Source: http://arstechnica.com/science/2012/07/epic-fraud-how-to-succeed-in-science-without-doing-any/

Judging Authenticity

- Well established for physical objects.
- Example: Paintings
  - Age
  - Certificates
  - Ownership and Provenance
  - Condition
  - Known style, hand writing
  - Repairs or alterations
  - Reference and context



MUSÉE d'ORSAY

Paris

AUTEUR: Pablo Ruiz Picasso

ALBACHE: "Esculpiendo una cabeza"

ANNÉE: 1933

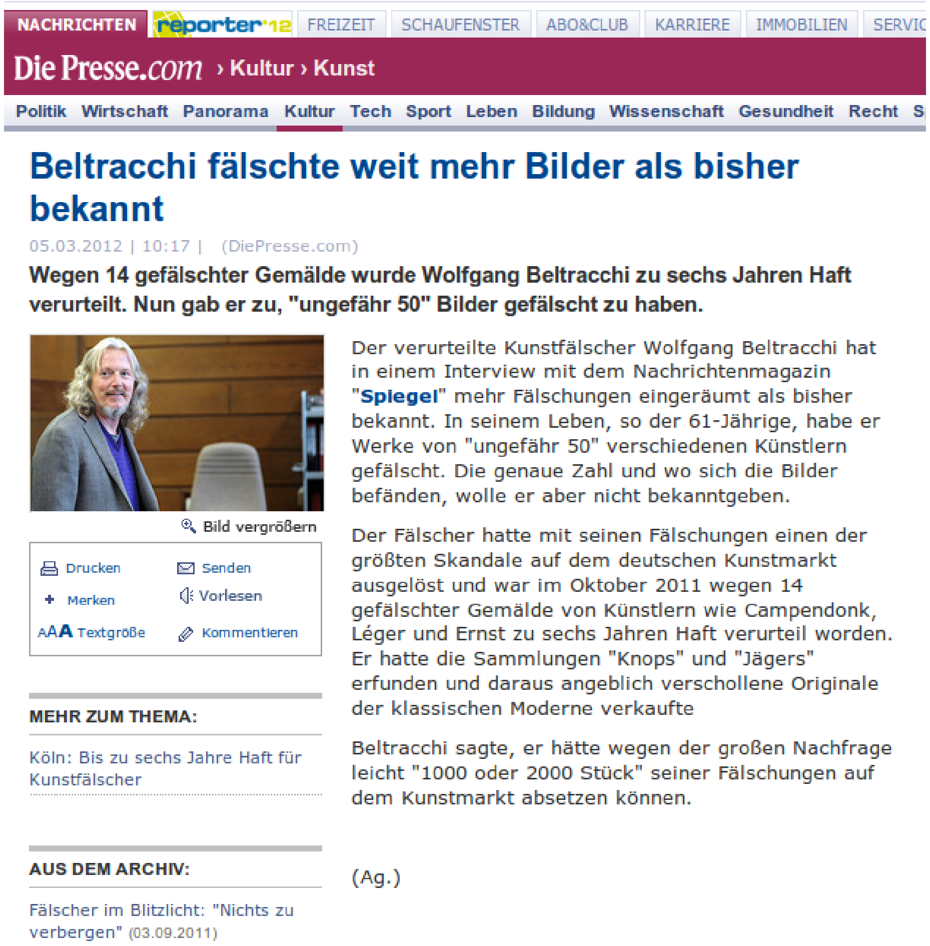
TECNICA: Grabado sobre cartón

TALLE: 11.5 x 8 cms

FICHE Nº: Fecha de expedición 1980

© www.artmarketblog.com

But still…



Beltracchi fälschte weit mehr Bilder als bisher bekannt

05.03.2012 | 10:17 | (DiePresse.com)

Wegen 14 gefälschter Gemälde wurde Wolfgang Beltracchi zu sechs Jahren Haft verurteilt. Nun gab er zu, "ungefähr 50" Bilder gefälscht zu haben.

Der verurteilte Kunstfälscher Wolfgang Beltracchi hat in einem Interview mit dem Nachrichtenmagazin "**Spiegel**" mehr Fälschungen eingeräumt als bisher bekannt. In seinem Leben, so der 61-Jährige, habe er Werke von "ungefähr 50" verschiedenen Künstlern gefälscht. Die genaue Zahl und wo sich die Bilder befänden, wolle er aber nicht bekanntgeben.

Der Fälscher hatte mit seinen Fälschungen einen der größten Skandale auf dem deutschen Kunstmarkt ausgelöst und war im Oktober 2011 wegen 14 gefälschter Gemälde von Künstlern wie Campendonk, Léger und Ernst zu sechs Jahren Haft verurteil worden. Er hatte die Sammlungen "Knops" und "Jägers" erfunden und daraus angeblich verschollene Originale der klassischen Moderne verkaufte

Beltracchi sagte, er hätte wegen der großen Nachfrage leicht "1000 oder 2000 Stück" seiner Fälschungen auf dem Kunstmarkt absetzen können.

(Ag.)

MEHR ZUM THEMA:

Köln: Bis zu sechs Jahre Haft für Kunstfälscher

AUS DEM ARCHIV:

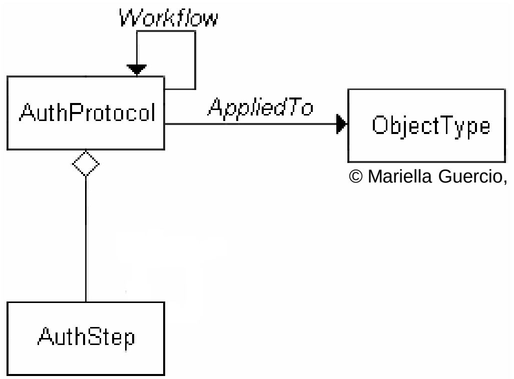
Fälscher im Blitzlicht: "Nichts zu verbergen" (03.09.2011)

Judging Authenticity of Digital Data

- How to assess authenticity?
  - Analyze metadata accompanying the digital object
  - Examine checksums (fixity)
  - Compare to redundant copies
  - Investigate the context of the object
  - Track provenance (see later...)
  - Use signatures and encryption (see later...)

Authenticity Models

- Authenticity Protocol
  - CASPAR Project www.casparpreserves.eu
  - Authenticity Protocol (AP) is a workflow that is applied to a set of digital objects having the same features (e.g. images or documents)

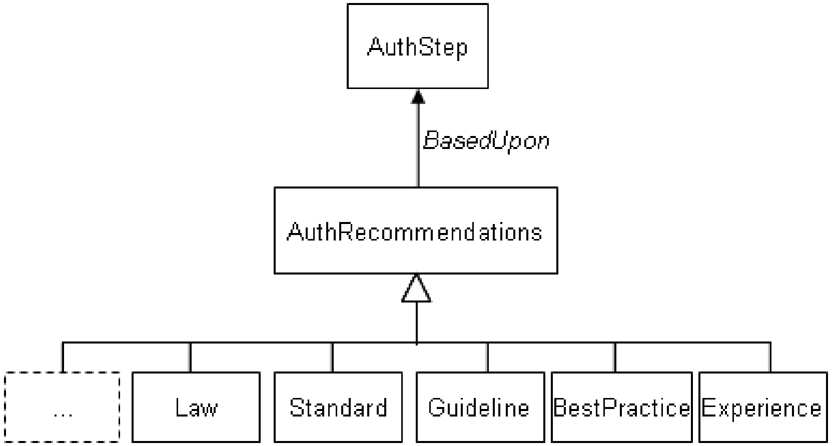


© Mariella Guercio, CASPAR

  - The process itself consists of different Authenticity Steps (AS) that deal with a certain aspect of a digital object

Authenticity Steps

- Interrelated steps to assess authenticity
- Based on:
  - Reference
  - Provenance
  - Fixity
  - Context
  - Recommendations

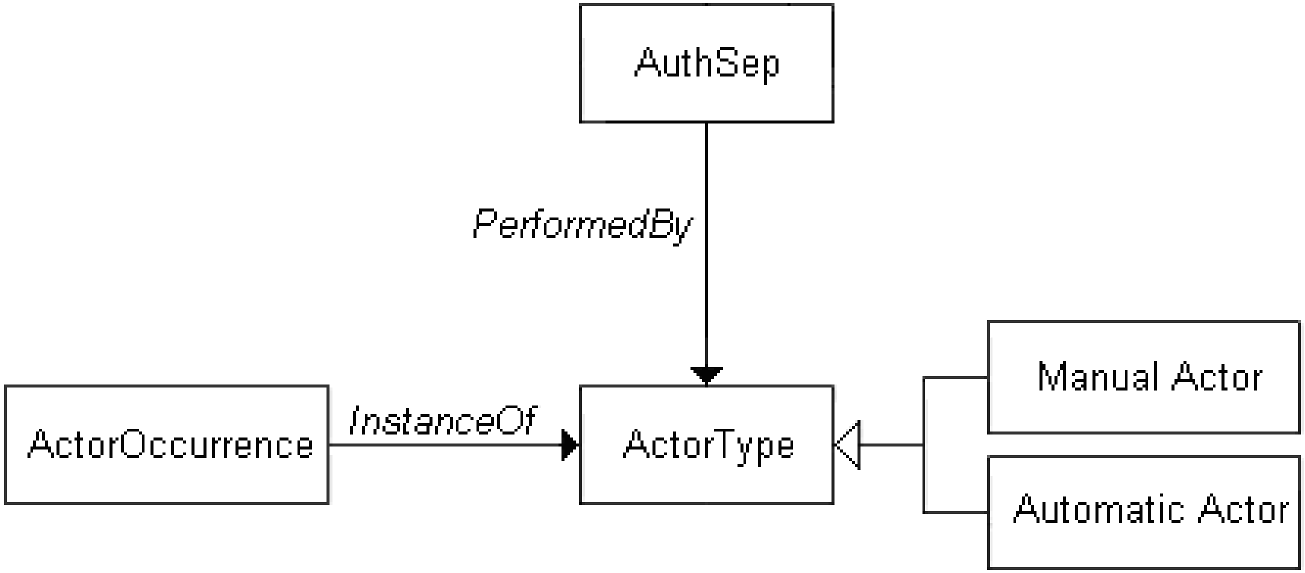


© Mariella Guercio, CASPAR

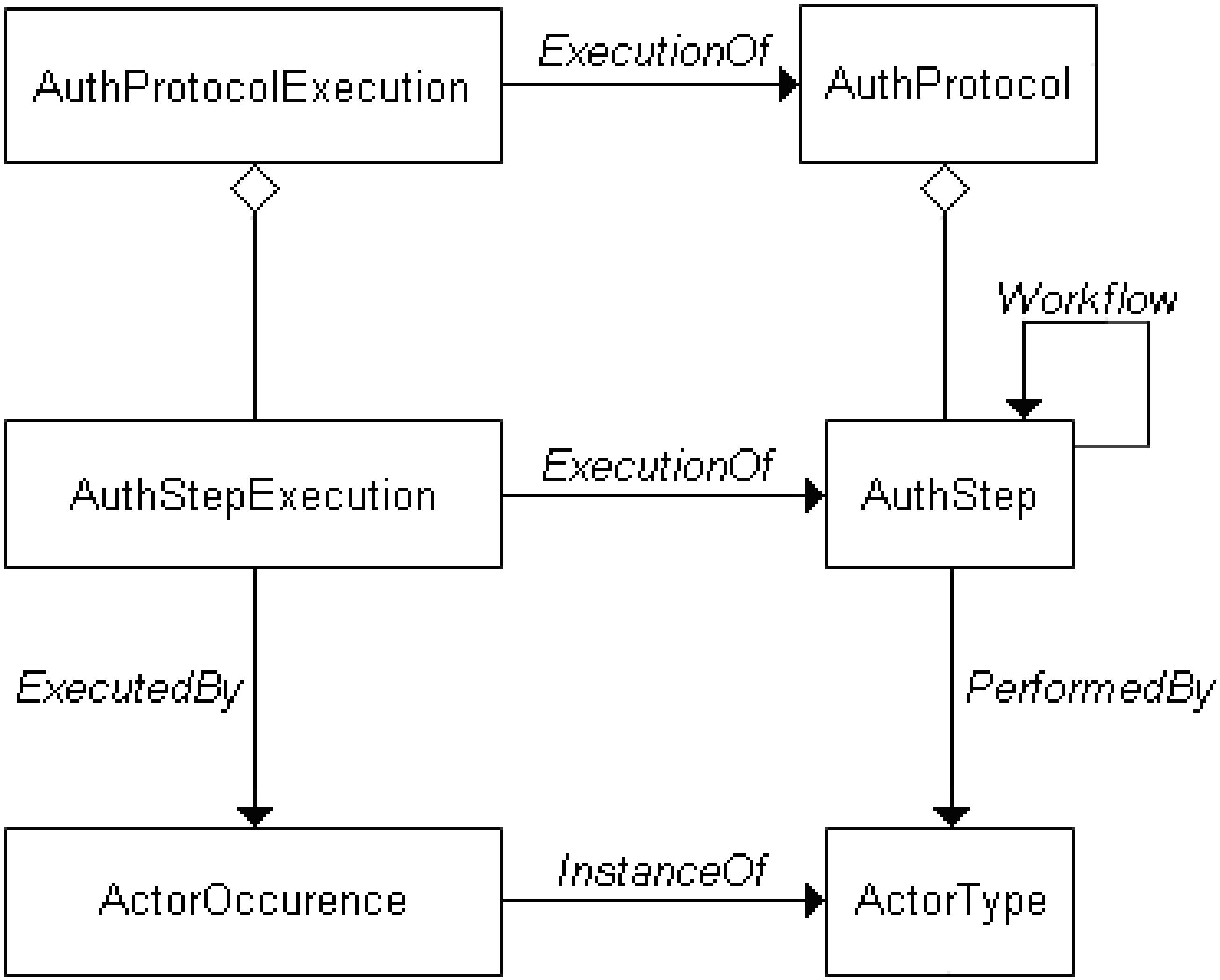
© Mariella Guercio, CASPAR

Authenticity Protocol Actors

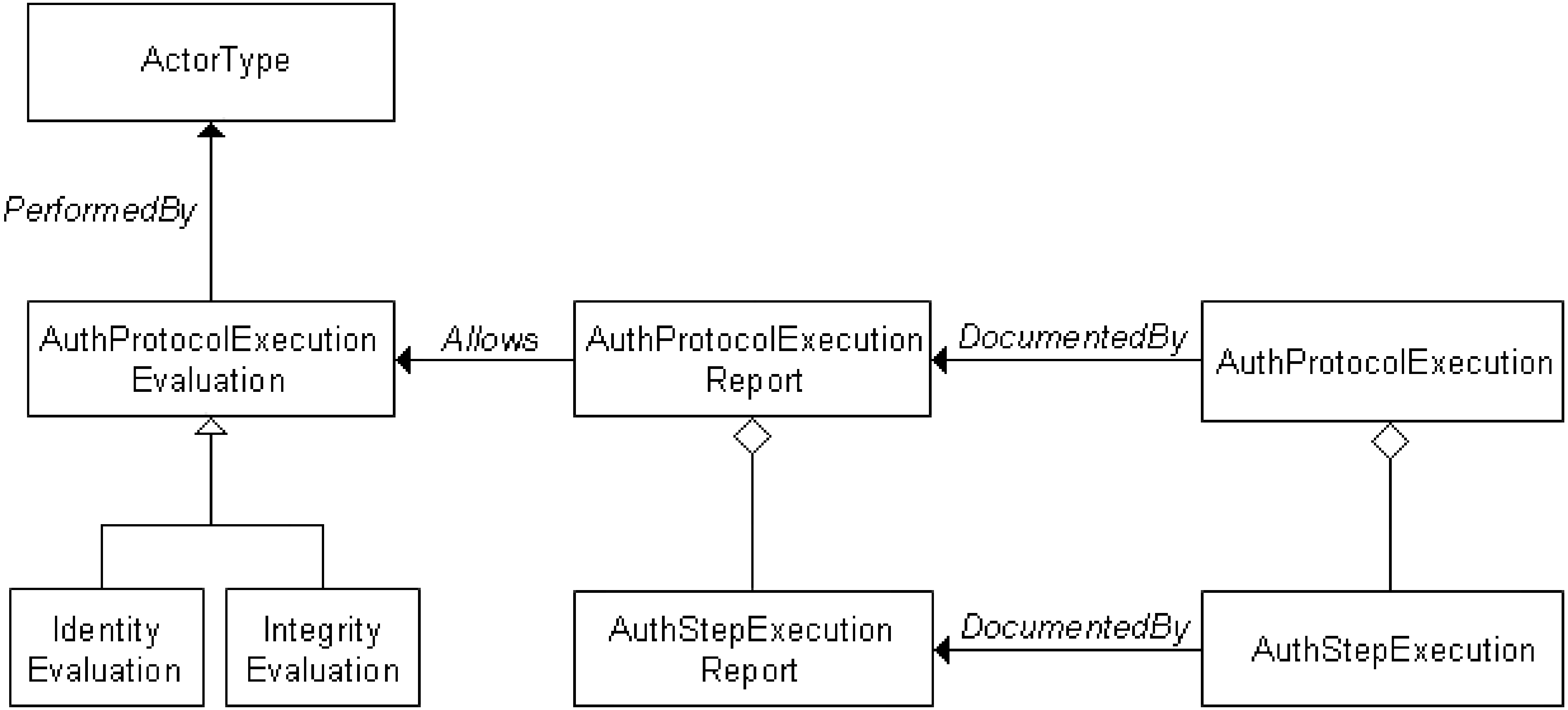
- Actors
  - – Manual actors: human beings
  - – Automatic actor: software



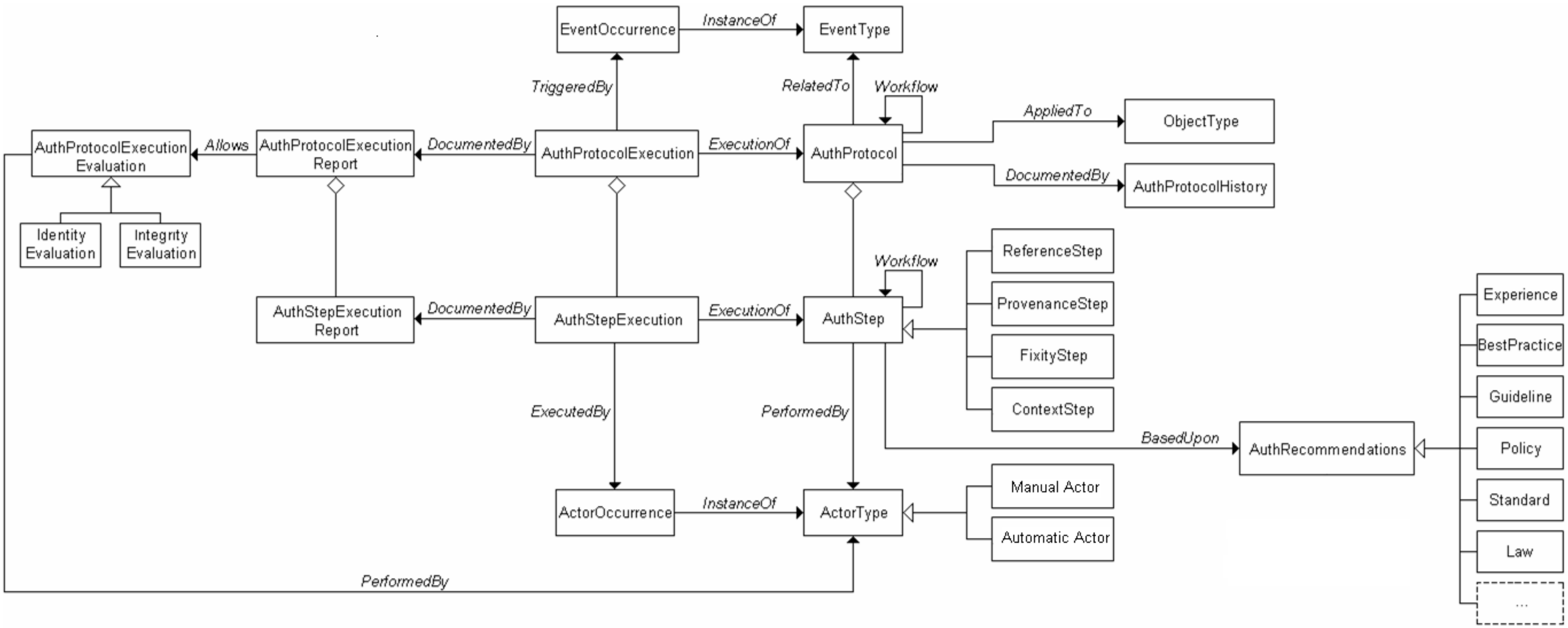
Authenticity Protocol Execution



Authenticity Report and Evaluation



The CASPAR Authenticity Protocol



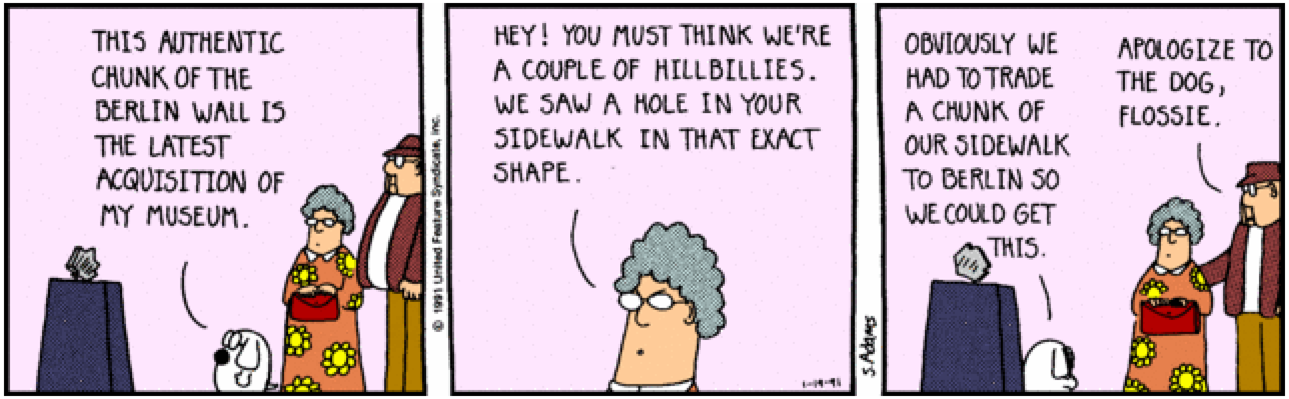
Evidence

- Each AS should be supported by evidence
  - Can be technical like checksums
  - Non-technical like the reputation of administrators
- Evidence itself needs to be long term compatible
  - You can‘t assess authenticity if you can‘t read the evidence
- Comprehensive descriptions how evidence was collected are needed

Summary: Authenticity

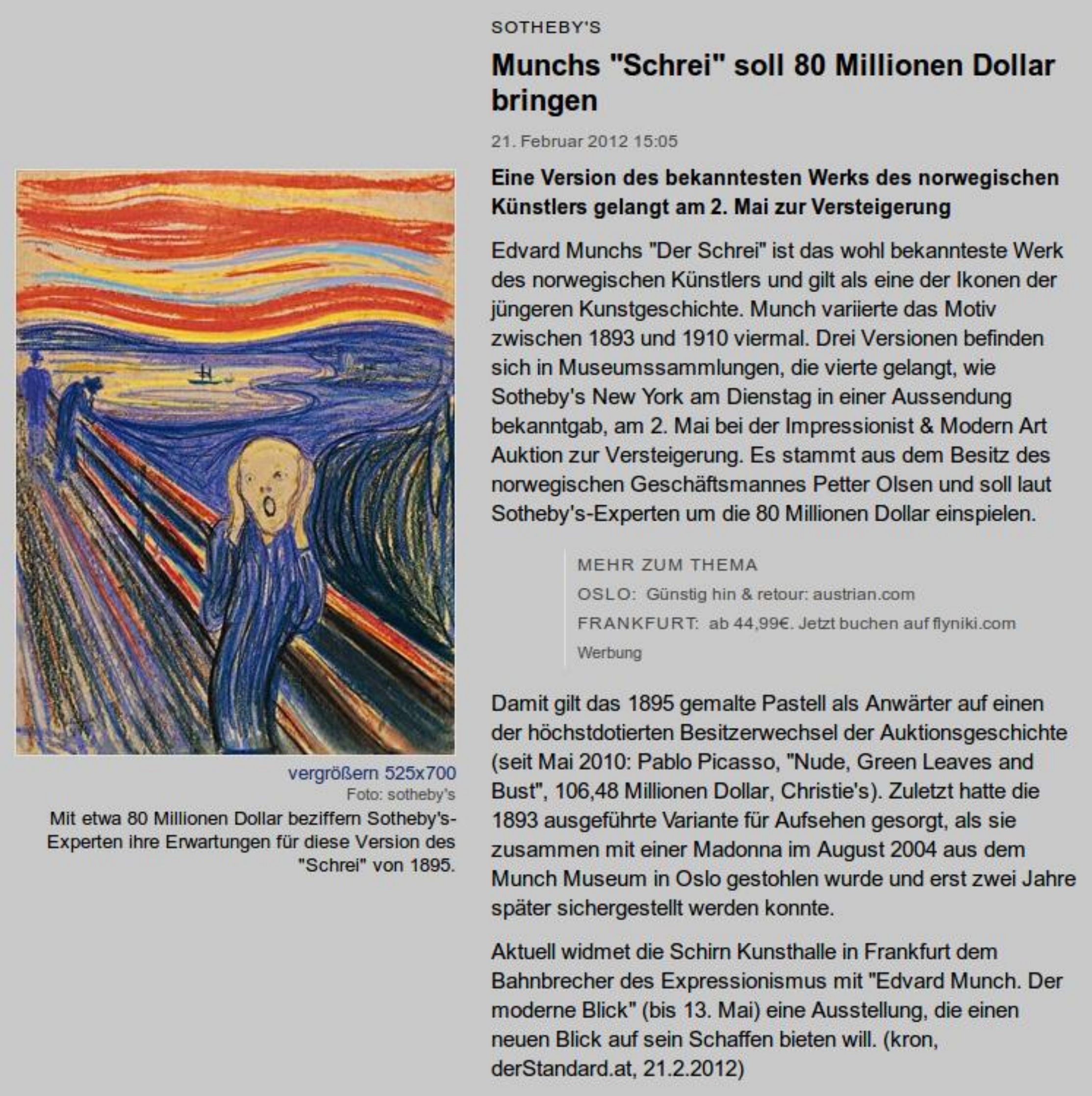
- Degree to which an object is what it purports to be
  - Needs to be assessed -> Authenticity Protocol
  - Needs to be maintained
- Metadata about evidence:
  - Technical properties
    - Checksums
    - Context
    - …
  - Social properties
    - Trust
    - Reputation

Questions?


THIS AUTHENTIC CHUNK OF THE BERLIN WALL IS THE LATEST ACQUISITION OF MY MUSEUM.
© 1991 United Feature Syndicate, Inc.
HEY! YOU MUST THINK WE'RE A COUPLE OF HILLBILLIES. WE SAW A HOLE IN YOUR SIDEWALK IN THAT EXACT SHAPE.
S.Adams
OBVIOUSLY WE HAD TO TRADE A CHUNK OF OUR SIDEWALK TO BERLIN SO WE COULD GET THIS.
APOLOGIZE TO THE DOG, FLOSSIE.

© Dilbert.com

What is Provenance?



SOTHEBY'S

Munchs "Schrei" soll 80 Millionen Dollar bringen

21. Februar 2012 15:05

Eine Version des bekanntesten Werks des norwegischen Künstlers gelangt am 2. Mai zur Versteigerung

vergrößern 525x700

Foto: sotheby's

Mit etwa 80 Millionen Dollar beziffern Sotheby's-Experten ihre Erwartungen für diese Version des "Schrei" von 1895.

Edvard Munchs "Der Schrei" ist das wohl bekannteste Werk des norwegischen Künstlers und gilt als eine der Ikonen der jüngeren Kunstgeschichte. Munch variierte das Motiv zwischen 1893 und 1910 viermal. Drei Versionen befinden sich in Museumssammlungen, die vierte gelangt, wie Sotheby's New York am Dienstag in einer Aussendung bekanntgab, am 2. Mai bei der Impressionist & Modern Art Auktion zur Versteigerung. Es stammt aus dem Besitz des norwegischen Geschäftsmannes Petter Olsen und soll laut Sotheby's-Experten um die 80 Millionen Dollar einspielen.

Damit gilt das 1895 gemalte Pastell als Anwärter auf einen der höchstdotierten Besitzerwechsel der Auktionsgeschichte (seit Mai 2010: Pablo Picasso, "Nude, Green Leaves and Bust", 106,48 Millionen Dollar, Christie's). Zuletzt hatte die 1893 ausgeführte Variante für Aufsehen gesorgt, als sie zusammen mit einer Madonna im August 2004 aus dem Munch Museum in Oslo gestohlen wurde und erst zwei Jahre später sichergestellt werden konnte.

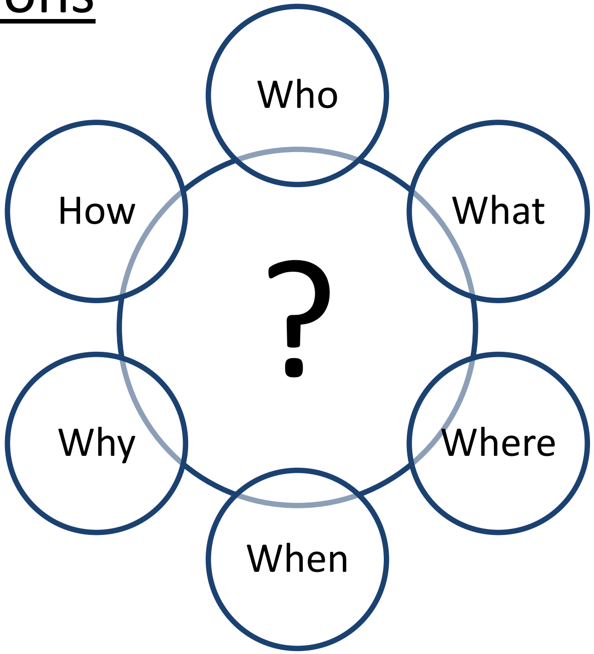
Aktuell widmet die Schirn Kunsthalle in Frankfurt dem Bahnbrecher des Expressionismus mit "Edvard Munch. Der moderne Blick" (bis 13. Mai) eine Ausstellung, die einen neuen Blick auf sein Schaffen bieten will. (kron, derStandard.at, 21.2.2012)

What is Provenance?

- Provenance of objects describes:
  - Origin
  - Lineage and chain of ownership
  - Chronology of important events
- Relation to Digital Preservation:
  - Provenance documents the history of digital objects
  - Digital archives need to collect and maintain provenance information

Provenance

- Metadata describes the complete history of digital information
  - Includes creators, authors, timestamps,….
  - Transactions, modifications, contributions…
- Answers six questions



Provenance Challenges

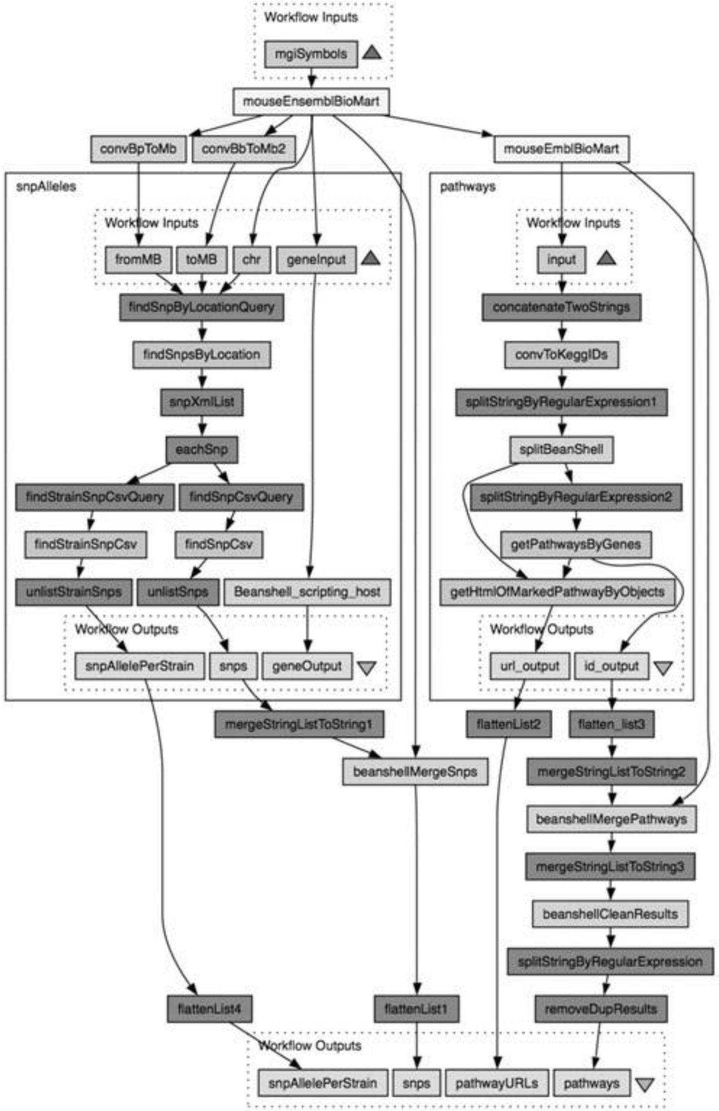
- There is no “original” of a digital object like in the physical world
- Any copy has the exact same attributes
  - A copy does not destroy the provenance of a digital object
- Digital objects have to be transformed
  - Transformations have to be tracked in the provenance information
  - Provenance is part of the workflow

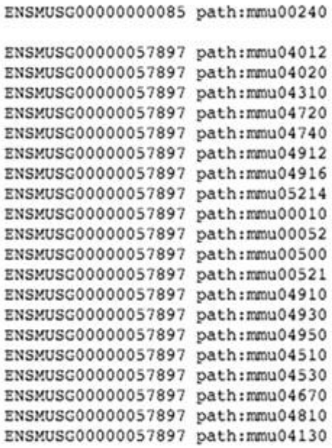
Data Provenance

- Essential for science, governance and commerce
  - Whenever evidence for documents and information is needed
- Many applications
  - Verification of scientific experiments
  - Financial transactions
  - Information flows
  - Drug trials
  - …
- Provenance is a fundamental principle of archiving

- Secure Provenance: Protecting the Genealogy of Bits, R. Hasan et. al.

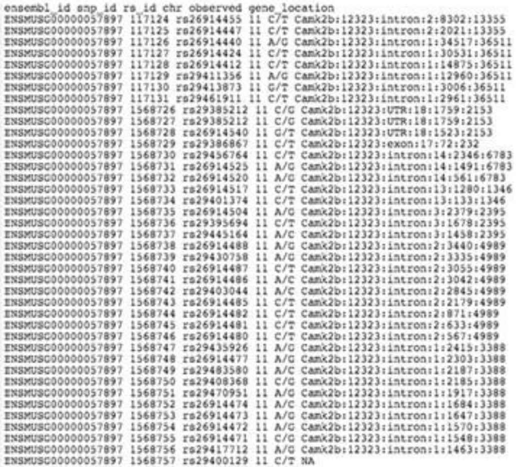
Example



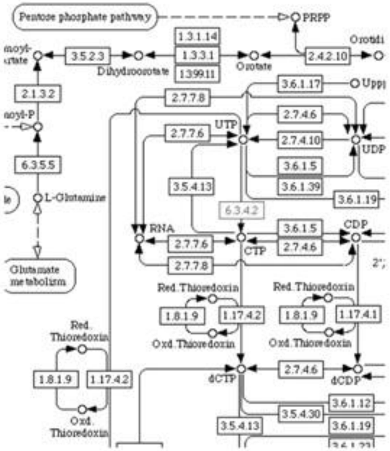


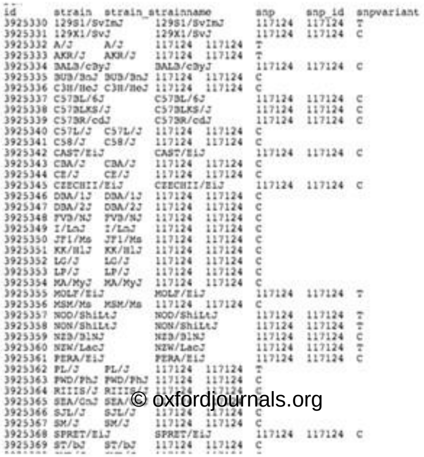
```
ENSMUSG00000000085 path:mmu00240

ENSMUSG00000057897 path:mmu04012
ENSMUSG00000057897 path:mmu04020
ENSMUSG00000057897 path:mmu04310
ENSMUSG00000057897 path:mmu04720
ENSMUSG00000057897 path:mmu04740
ENSMUSG00000057897 path:mmu04912
ENSMUSG00000057897 path:mmu04916
ENSMUSG00000057897 path:mmu05214
ENSMUSG00000057897 path:mmu00010
ENSMUSG00000057897 path:mmu00052
ENSMUSG00000057897 path:mmu00500
ENSMUSG00000057897 path:mmu00521
ENSMUSG00000057897 path:mmu04910
ENSMUSG00000057897 path:mmu04930
ENSMUSG00000057897 path:mmu04950
ENSMUSG00000057897 path:mmu04510
ENSMUSG00000057897 path:mmu04530
ENSMUSG00000057897 path:mmu04670
ENSMUSG00000057897 path:mmu04810
ENSMUSG00000057897 path:mmu04130
```



```
ensembl_id snp_id rs_id chr observed gene_location
ENSMUSG00000057897 117124 rs26914455 11 C/T Camk2b:12323:intron:2:8302:13355
ENSMUSG00000057897 117125 rs26914447 11 C/T Camk2b:12323:intron:2:2021:13355
ENSMUSG00000057897 117126 rs26914440 11 A/G Camk2b:12323:intron:1:34517:36511
ENSMUSG00000057897 117127 rs26914424 11 C/T Camk2b:12323:intron:1:30531:36511
ENSMUSG00000057897 117128 rs26914412 11 C/T Camk2b:12323:intron:1:14875:36511
ENSMUSG00000057897 117129 rs29411356 11 A/G Camk2b:12323:intron:1:12960:36511
ENSMUSG00000057897 117130 rs29413873 11 G/T Camk2b:12323:intron:1:3006:36511
ENSMUSG00000057897 117131 rs29461911 11 C/T Camk2b:12323:intron:1:2961:36511
ENSMUSG00000057897 1568726 rs29385212 11 C/G Camk2b:12323:UTR:18:1759:2153
ENSMUSG00000057897 1568727 rs29385212 11 C/G Camk2b:12323:UTR:18:1759:2153
ENSMUSG00000057897 1568728 rs26914540 11 G/T Camk2b:12323:UTR:18:1523:2153
ENSMUSG00000057897 1568729 rs29386867 11 C/T Camk2b:12323:exon:17:72:232
ENSMUSG00000057897 1568730 rs29456764 11 C/T Camk2b:12323:intron:14:2346:6783
ENSMUSG00000057897 1568731 rs26914525 11 A/G Camk2b:12323:intron:14:1491:6783
ENSMUSG00000057897 1568732 rs26914520 11 A/G Camk2b:12323:intron:14:561:6783
ENSMUSG00000057897 1568733 rs26914517 11 C/T Camk2b:12323:intron:13:1280:1346
ENSMUSG00000057897 1568734 rs29401374 11 C/T Camk2b:12323:intron:13:133:1346
ENSMUSG00000057897 1568735 rs26914504 11 A/G Camk2b:12323:intron:3:2379:2395
ENSMUSG00000057897 1568736 rs29395694 11 C/T Camk2b:12323:intron:3:1678:2395
ENSMUSG00000057897 1568737 rs29445164 11 A/C Camk2b:12323:intron:3:1458:2395
ENSMUSG00000057897 1568738 rs26914488 11 A/G Camk2b:12323:intron:2:3440:4989
ENSMUSG00000057897 1568739 rs29430758 11 A/G Camk2b:12323:intron:2:3335:4989
ENSMUSG00000057897 1568740 rs26914487 11 C/T Camk2b:12323:intron:2:3055:4989
ENSMUSG00000057897 1568741 rs26914486 11 A/C Camk2b:12323:intron:2:3042:4989
ENSMUSG00000057897 1568742 rs29403044 11 A/C Camk2b:12323:intron:2:2845:4989
ENSMUSG00000057897 1568743 rs26914485 11 C/T Camk2b:12323:intron:2:2179:4989
ENSMUSG00000057897 1568744 rs26914482 11 C/T Camk2b:12323:intron:2:871:4989
ENSMUSG00000057897 1568745 rs26914481 11 C/T Camk2b:12323:intron:2:633:4989
ENSMUSG00000057897 1568746 rs26914480 11 C/T Camk2b:12323:intron:2:567:4989
ENSMUSG00000057897 1568747 rs29435926 11 A/G Camk2b:12323:intron:1:2415:3388
ENSMUSG00000057897 1568748 rs26914477 11 A/G Camk2b:12323:intron:1:2303:3388
ENSMUSG00000057897 1568749 rs29483580 11 A/C Camk2b:12323:intron:1:2187:3388
ENSMUSG00000057897 1568750 rs29408368 11 C/G Camk2b:12323:intron:1:2185:3388
ENSMUSG00000057897 1568751 rs29470951 11 A/G Camk2b:12323:intron:1:1917:3388
ENSMUSG00000057897 1568752 rs26914474 11 A/C Camk2b:12323:intron:1:1684:3388
ENSMUSG00000057897 1568753 rs26914473 11 A/G Camk2b:12323:intron:1:1647:3388
ENSMUSG00000057897 1568754 rs26914472 11 A/G Camk2b:12323:intron:1:1570:3388
ENSMUSG00000057897 1568755 rs26914471 11 C/G Camk2b:12323:intron:1:1548:3388
ENSMUSG00000057897 1568756 rs29417712 11 A/G Camk2b:12323:intron:1:1463:3388
ENSMUSG00000057897 1568757 rs29400129 11 C/T NA
```





```
id       strain   strain_strainname      snp      snp_id   snpvariant
3925330 129S1/SvImJ       129S1/SvImJ    117124   117124   T
3925331 129X1/SvJ         129X1/SvJ      117124   117124   C
3925332 A/J     A/J     117124   117124  T
3925333 AKR/J   AKR/J   117124   117124  T
3925334 BALB/cByJ         BALB/cByJ      117124   117124   C
3925335 BUB/BnJ BUB/BnJ 117124   117124  C
3925336 C3H/HeJ C3H/HeJ 117124   117124  C
3925337 C57BL/6J          C57BL/6J       117124   117124   C
3925338 C57BLKS/J         C57BLKS/J      117124   117124   C
3925339 C57BR/cdJ         C57BR/cdJ      117124   117124   C
3925340 C57L/J  C57L/J  117124   117124  C
3925341 C58/J   C58/J   117124   117124  C
3925342 CAST/EiJ          CAST/EiJ       117124   117124   C
3925343 CBA/J   CBA/J   117124   117124  C
3925344 CE/J    CE/J    117124   117124  C
3925345 CZECHII/EiJ       CZECHII/EiJ    117124   117124   C
3925346 DBA/1J  DBA/1J  117124   117124  C
3925347 DBA/2J  DBA/2J  117124   117124  C
3925348 FVB/NJ  FVB/NJ  117124   117124  C
3925349 I/LnJ   I/LnJ   117124   117124  C
3925350 JF1/Ms  JF1/Ms  117124   117124  C
3925351 KK/HlJ  KK/HlJ  117124   117124  C
3925352 LG/J    LG/J    117124   117124  C
3925353 LP/J    LP/J    117124   117124  C
3925354 MA/MyJ  MA/MyJ  117124   117124  C
3925355 MOLF/EiJ          MOLF/EiJ       117124   117124   T
3925356 MSM/Ms  MSM/Ms  117124   117124  C
3925357 NOD/ShiLtJ        NOD/ShiLtJ     117124   117124   T
3925358 NON/ShiLtJ        NON/ShiLtJ     117124   117124   T
3925359 NZB/BlNJ          NZB/BlNJ       117124   117124   C
3925360 NZW/LacJ          NZW/LacJ       117124   117124   T
3925361 PERA/EiJ          PERA/EiJ       117124   117124   C
3925362 PL/J    PL/J    117124   117124  T
3925363 PWD/PhJ PWD/PhJ 117124   117124  C
3925364 RIIIS/J RIIIS/J 117124   117124  C
3925365 SEA/GnJ SEA/[illegible]
3925366 SJL/J   SJL/J   117124   117124  C
3925367 SM/J    SM/J    117124   117124  C
3925368 SPRET/EiJ         SPRET/EiJ      117124   117124   C
3925369 ST/bJ   ST/bJ   117124   117124  C
```

© oxfordjournals.org

Capturing Provenance

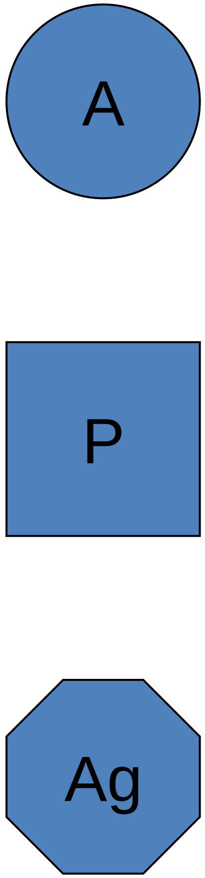
- Complex experiments and business workflows
  - Data sources and data flows have to be traced in order to be used later
  - Monitor data leakage, redundancy and efficiency of information flows
- Benefits of capturing provenance data:
  - Security
    - Detect anomalies
    - Prevent fraud
  - Data quality
    - Assess quality of stored data assets
    - Poor quality will have serious consequences
    - Horror example: U.S. bombing of the Chinese embassy in Belgrade 1999 caused by outdated map (http://www.defense.gov/transcripts/transcript.aspx?transcriptid=536)

The Open Provenance Model

- The Open Provenance Model
  - Can be used for digital and physical objects
  - Is a reference model
  - Defines a core set of inference rules
  - Enables interoperability between different systems
- Goals:
  - Controlled vocabulary
  - Serialization formats
  - APIs

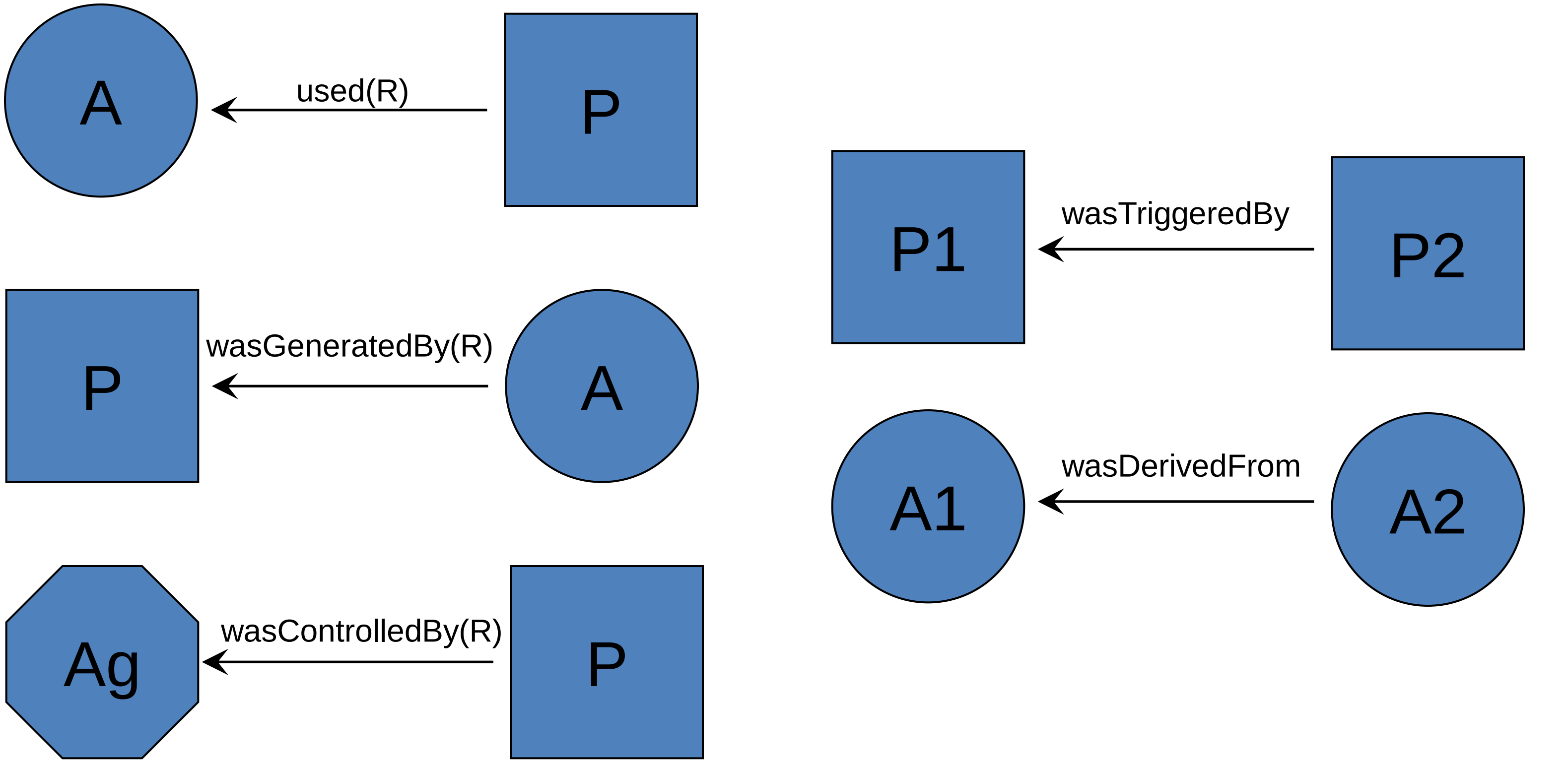
OPM Nodes

- Artifact
  - Object (digital or physical)
- Process
  - Action or series of actions
  - performed on or caused by artifacts
  - Results in new artifacts
- Agent
  - Responsible for process execution

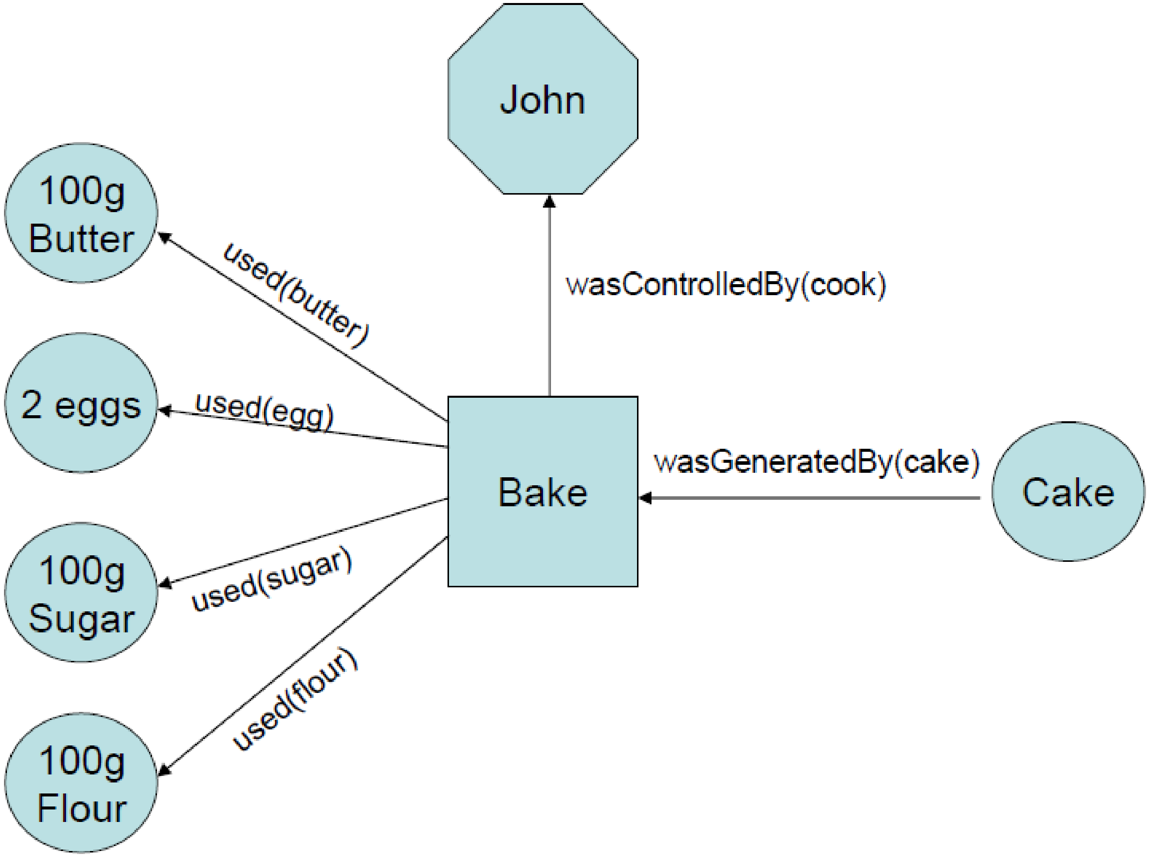


© www.openprovenance.org/tutorial/

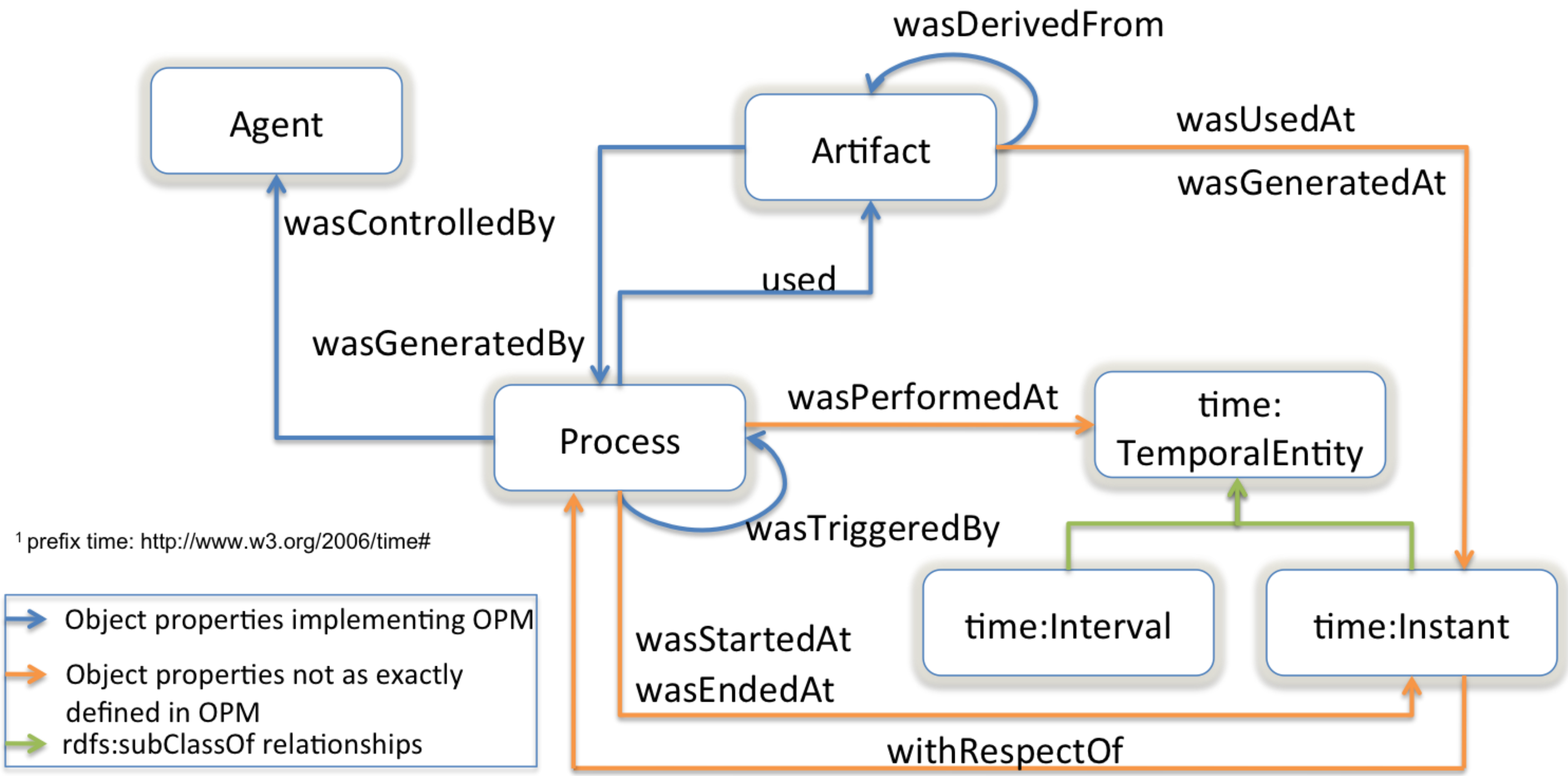
OPM Edges


A
used(R)
P
P1
wasTriggeredBy
P2
P
wasGeneratedBy(R)
A
A1
wasDerivedFrom
A2
Ag
wasControlledBy(R)
P

OPM: A Simple Example



The Open Provenance Model Extensibility



[1] prefix time: http://www.w3.org/2006/time#

© http://open-biomed.sourceforge.net/opmv/ns.html

Generating Provenance Data

- Provenance data should be generated
  - Automatically (i.e. log files)
  - Machine readable
  - In suitable granularity
  - Securely

Provenance- Questions?

- Why is provenance data important?
- What are metadata?
- How can provenance be modelled?

Relation of Authenticity and Provenance

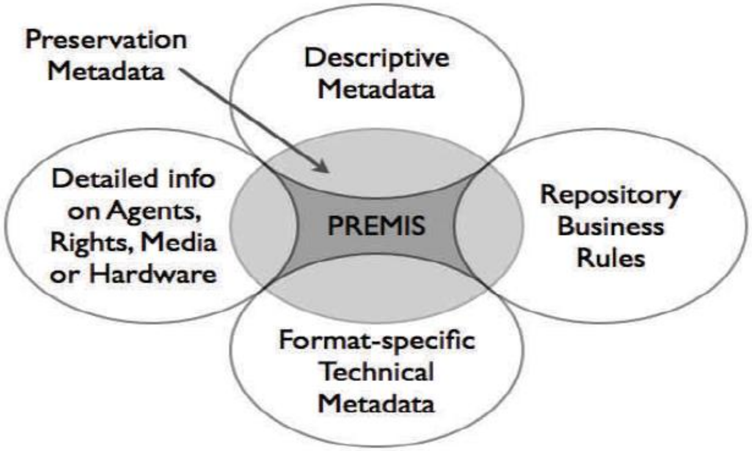
- Provenance can serve as evidence for authenticity
  - If the full provenance traces are available, the degree of authenticity is higher
- Authenticity has to be maintained along the object lifecycle
  - Each event that interacts with the object needs to trigger an authenticity protocol execution
  - Provenance metadata keeps track of this events and the actors involved

Preservation Metadata

- Metadata describes data and events in a precise way
  - Needed for authenticity and provenance information
  - Collect all metadata an archive needs for supporting digital preservation processes
- Different Metadata standards exist for various purposes
  - Level of granularity

PREMIS

- Preservation Metadata: Implementation Strategies (PREMIS)
  - Data dictionary
  - XML Schema

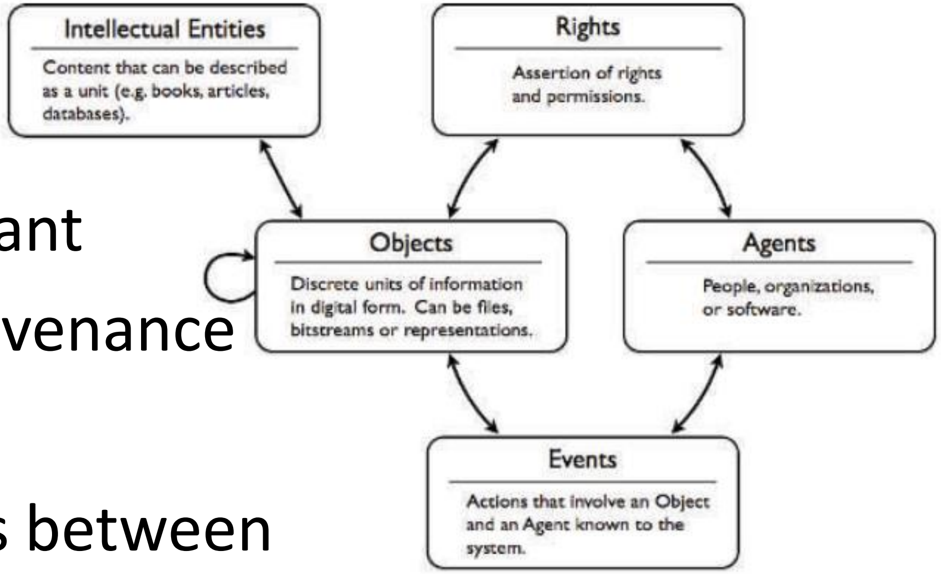


Preservation Metadata
Descriptive Metadata
Detailed info on Agents, Rights, Media or Hardware
PREMIS
Repository Business Rules
Format-specific Technical Metadata

© http://www.loc.gov/standards/premis/

PREMIS

- PREMIS data model
  - Events capture relevant actions and map provenance information.
  - Models relationships between the objects



Intellectual Entities
Content that can be described as a unit (e.g. books, articles, databases).

Rights
Assertion of rights and permissions.

Objects
Discrete units of information in digital form. Can be files, bitstreams or representations.

Agents
People, organizations, or software.

Events
Actions that involve an Object and an Agent known to the system.

© http://www.loc.gov/standards/premis/

- Provides OWL ontology
  - Defines clear semantics of the metadata elements
  - Reasoning

Security Considerations

- Authenticity and provenance data needs to be protected from manipulation
  - No tampering
  - No insertions, updates or deletes
- Provenance data can be sensitive
  - Privacy considerations
  - Espionage of critical business processes

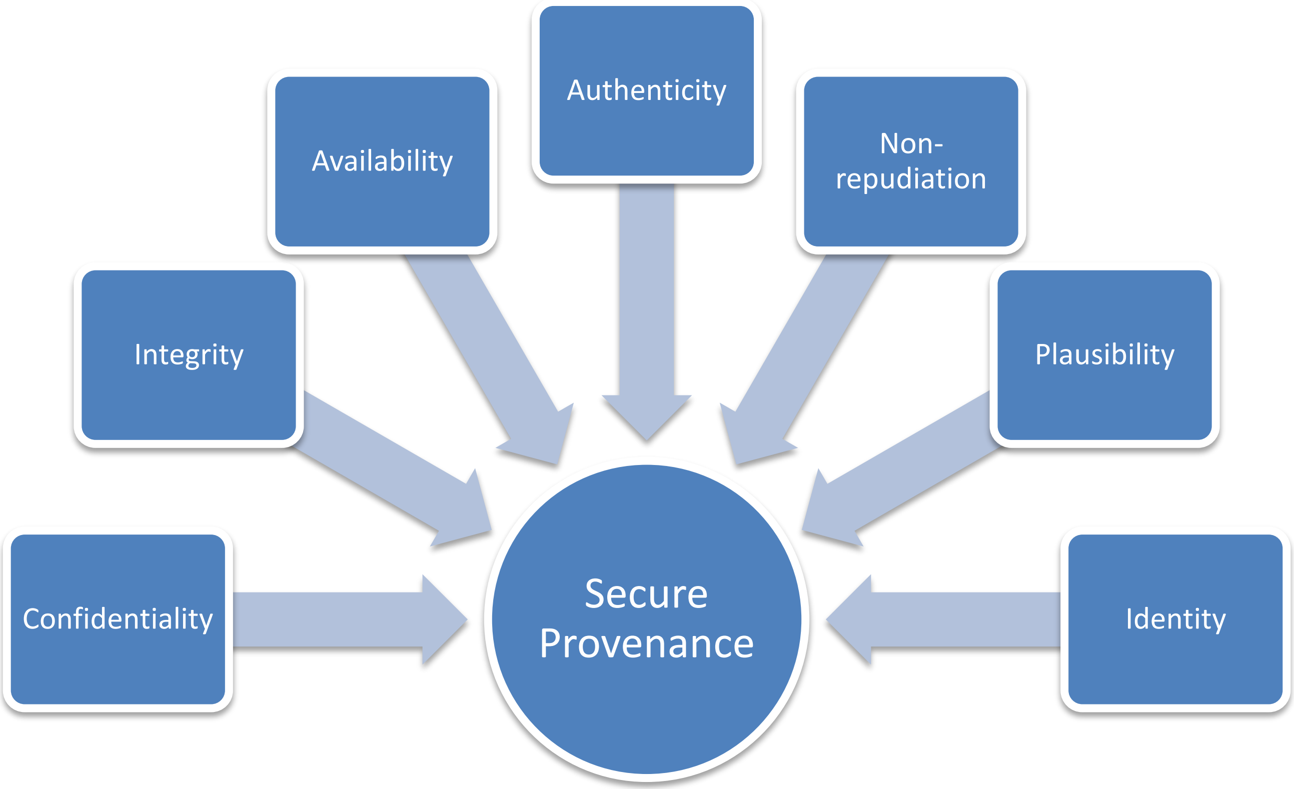
Security Requirements

- Confidentiality
  - Sensitive data must be protected
  - Cryptography
  - Policies
- Integrity
  - Completeness and wholeness in all the significant properties of a digital object
  - Not only on bit-level, but on intellectual form
- Availability
  - Data must be available when they are needed
  - Information must be protected

Security Requirements

- Authenticity
  - Degree to which digital objects are what they seem to be
- Non-Repudiation
  - The participation of an activity can not be denied
  - Events are verifiable
- Plausibility
  - Occurring events to not contradict logical assumptions
- Identity
  - Uniqueness
  - Distinguishable from other digital objects

Information Security Aspects of Authenticity and Provenance



Threat Model for Provenance

- Attackers could try to
  - Delete provenance records
    - Remove incriminating evidence
  - Add fake entries
    - Claim authorship of data
    - „Enhancements“ -> Scientific fraud
  - Manipulate records and alter history
    - Cover tracks
  - Hide contributions
    - Deny responsibility

Secure Provenance

- Logging mechanisms
  - Provenance data can be collected by logs
  - Logs capture relevant events automatically
  - Granularity of logs from high level to system calls
- Log architectures
  - Sender transmits event notification to relay or collector
  - Scalability is important
- Logs have to be auditable
  - Event chain has to be reproducible

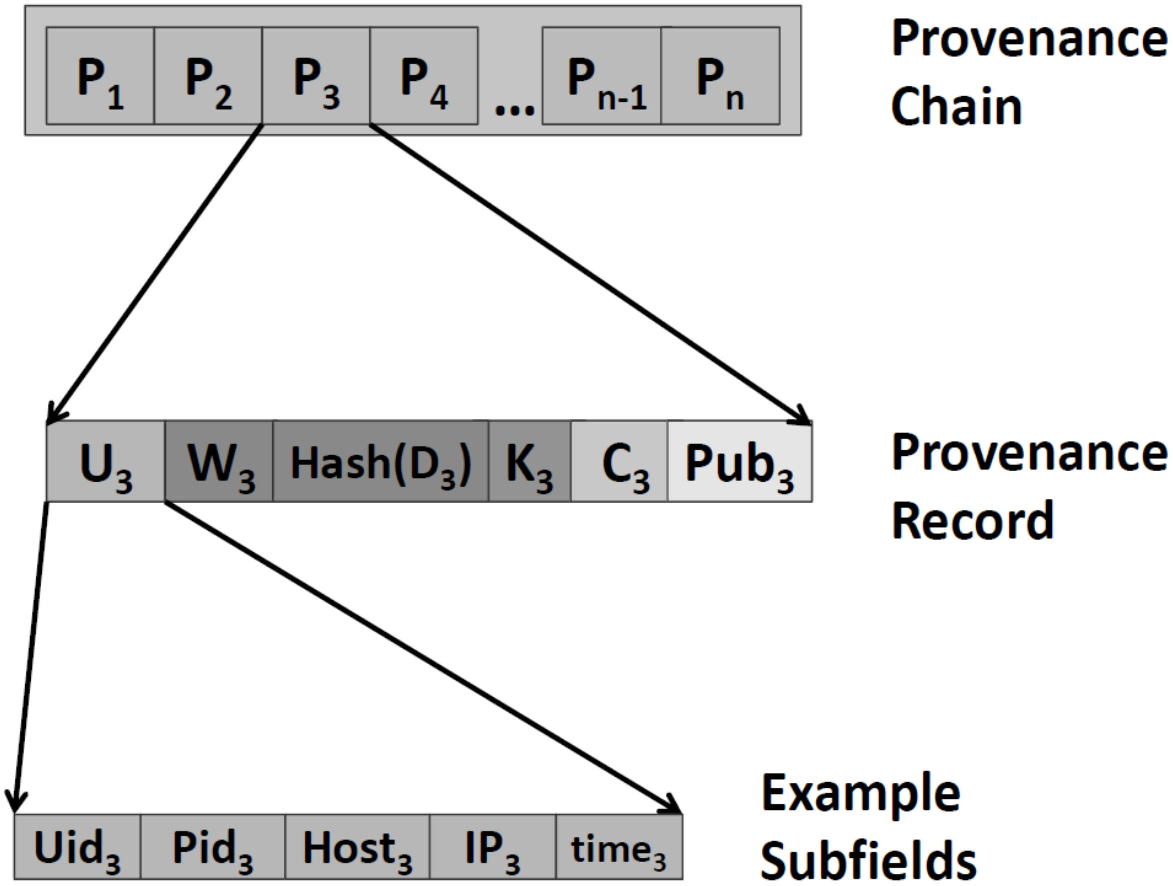
Secure Logging

- Log file content is highly sensitive
  - Have to be safeguarded against unauthorized access and manipulation
  - Sender and receiver have to agree on a shared cryptographic protocol
  - Signatures ensure integrity
  - Encryption hides content from intruders

Append-Only Signatures

- Signature chains
  - Ensure fixity by signing all occurred events
  - Signatures have to be protected from manipulation
    - Only allow new records to the provenance chain to appended to the end
    - Append-only signatures aggregate signatures from previous records -> no intermediate records can be inserted
    - Forward-secure signatures

Signature Chains



P_1 | P_2 | P_3 | P_4 | ... | P_{n-1} | P_n

Provenance Chain

U_3 | W_3 | $Hash(D_3)$ | K_3 | C_3 | Pub_3

Provenance Record

Uid_3 | Pid_3 | $Host_3$ | IP_3 | $time_3$

Example Subfields

Hasan et. al. [2]

Secure Logging - Challenges

- Preservation and encryption
  - Cryptographic methods have to be observed for obsoletion
  - What if the keys are lost?
  - XML Advanced Electronic Signatures (XAdES)
- Audits
  - Frequent audits are necessary
  - Auditors are only allowed to read relevant pathways in the graph

Secure Storage

- Specialized Provenance Stores
  - Provenance Aware Storage System (PASS)
  - Provenance Data Store (PDS)
- Write Once Read Many
  - Prevents records from being altered or deleted
  - Various systems available

Security Questions

- Why is provenance data a profitable goal for attacks?
- What are the requirements for secure logs?
- What solutions are available?

Literature and Links

- CASPAR Project
  - www.casparpreserves.eu
  - www.casparpreserves.eu/Members/metaware/Events/training/newsletter-december-2008/training-presentations/michetti-guercio.pdf
- Secure Provenance: Protecting the Genealogy of Bits, R. Hasan et. al.
- The OPM Provenance Model
  - www.openprovenance.org
  - http://twiki.ipaw.info/bin/view/OPM/
- Data provenance – the foundation of data quality. P. Buneman, S. Davidson, University of Edinburgh. Edinburgh, UK

Thank you for your attention.

sproell@sba-research.org