Purpose

This document specifies the PROV-TC language, which is a dialect of the W3CPROV language (specifically the PROV-N compliant representation of that language). PROV-TC is meant to be used by the Transparent Computing ADAPT project team (and hopefully other teams) for communication between technical areas one and two.

Contact

Please contact Dave Archer, dwa@galois.com, regarding this specification.

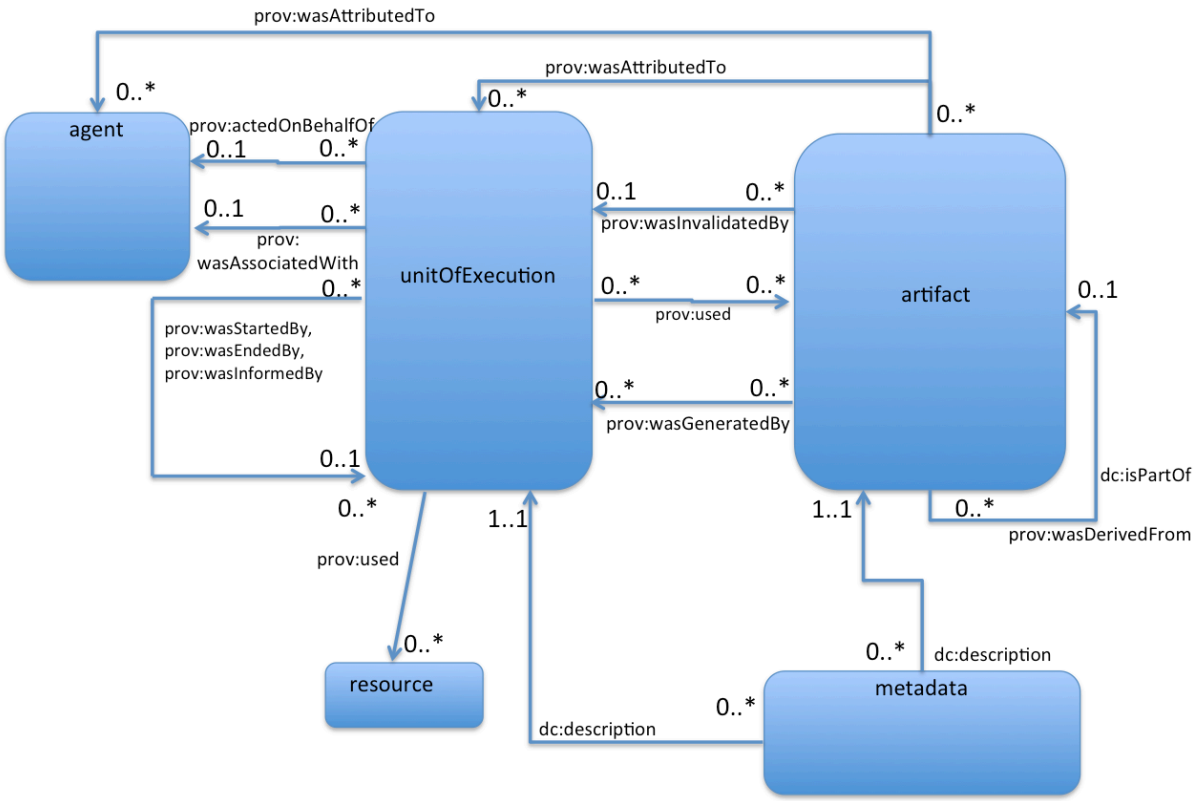
Working Prototypes

The ADAPT team has demonstrated the following so far:

- a translator from the 5-Directions sample data syntax to PROV-TC
- successful translation of all 46 5-Directions data samples into PROV-TC (these are available, just ask)
- an XML file specifying PROV-TC specific attributes to PROV-N constructs that is used to generate SRI SPADE data compliant to PROV-TC
- successful generation of several SPADE samples in PROV-TC
- an ingestor that parses, syntax checks, and type checks PROV-TC, and creates a prototype graph database from the ingested data
- successful ingest of all 5-Directions and SPADE samples generated so far in PROV-TC
- the examples used in this literate specification of PROV-TC

Conceptual Model

PROV-TC is a domain-specific language designed to implement a conceptual model for transfer of knowledge between Transparent Computing TA1 and TA2 teams. The conceptual model has been discussed and refined for several months, and is shown below.



PROV-TC Prelude and Postlude

Every valid PROV-TC document has a prelude consisting of at least the following

```
document
// declare the ontologies used in the code

// namespace for instance names of entities and relations
prefix ex <http://example.org/>

// namespace for our specific attributes
prefix prov-tc <http://spade.csl.sri.com/rdf/audit-tc.rdfs#>
```

Every valid PROV-TC document concludes with

```
end document
```

Quick checking for basic syntax correctness

Because we specify a dialect of PROV-N, an easy on-line tool can be used as a basic check of syntactic correctness prior to using our ingester tools to check more deeply. You can find this tool here.

A more complete check, including checking of attributes specific to PROV-TC, can be had by contacting the ADAPT team.

PROV-TC Entities

We allow for instances of the following entity classes. In each case, we specify all currently recognized attributes. Those attributes that are required for syntactic correctness are marked as required in the code examples. All others are optional. No alternates to the attributes shown are allowed. That is, the shown attributes are the only option available to represent the semantics they represent. Other semantics may be included, but will be ignored for now.

Artifact

An artifact is an entity that may be created, referenced, used, or destroyed, but does not take action on its own. Artifacts recognized at present in the TC domain include files, network packets, memory locations, and registry file entries. More may be added later. An artifact instance is reified as an entity in the PROV model, and includes several attributes, many of which are optional. Shown below is an example artifact: a file with name */users/dwa/mystuff/bin/create.exe*, and referred to with the tag *ex:createExe*. Required attributes are marked with comments and include the type of entity (*prov:type*), the type of artifact (*adapt:entityType*), an identifier (the type of which depends on the artifact type), a location within that item (which also depends on the artifact type), a creation time, a version, a destruction time, an owning account, a size, and a 32b taint. Alternative values for the different artifact types are shown in comments.

```
entity(ex:createExe, [
            prov-tc:source="/dev/audit",
            //alternately, "/proc"
            prov-tc:entityType="file", //required: one of the 4 options here
            // alternately, "network"
            // alternately, "memory"
            // alternately, "registryEntry"
            // currently looking at alternatives to add here for MIT
            prov-tc:path="/users/dwa/mystuff/bin/create.exe",
            // alternately, destinationAddress="128.10.125.71"
            // alternately, destinationPort="88"
            // alternately, sourceAddress="127.0.0.1"
            // alternately, sourcePort="1234"
            // alternately, pageID="0x123"
            // alternately, registryKey="stuff"
            prov-tc:fileOffset="0x00000000",
            // alternately, packetID="0x1234"
            // alternately, address="0x00000000"
            // alternately, registryValue="some value"
            prov-tc:time="015-10-16T02:13:07Z",
            prov-tc:hasVersion="23",
            prov-tc:uid="dwa",
            prov-tc:size="4096",
            prov-tc:taint="0x00000001"])
```

Resource

A resource is a thing that may be used, but not created or destroyed. Typical resources include GPS units, cameras, keyboards, and accelerometers. More may be added later. The *adapt:devType* attribute that specifies the resource type is required. Optional is an attribute *adapt:devID* that names a specific resource.

```
// a GPS sensor resource called ex:GPSunit
entity(ex:GPSunit, [
            prov-tc:source="/dev/audit",
            //alternately, "/proc"
            prov-tc:devType="GPS",
            // alternately, "microphone",
            // alternately, "accelerometer",
            // alternately, "camera"
            prov-tc:devID="Default GPS sensor"])
```

Unit of Execution (UoE)

A UoE is a thread of execution running on a processor. It may be created or destroyed, and may take

action on its own to create or destroy other UoEs or to affect artifacts. A UoE is reified in PROV as an *activity*. Below we show an example UoE called "parent". Recognized but optional attributes are an ID string unique to the machine where the UoE runs, the times at which the UoE started and ended, the privileges with which the UoE ran, the account name and group name under which it ran, its process ID and parent process ID, the directory where it started, the command line used, and the command used.

```
//
activity(ex:parentb, -, -, [
            prov-tc:source="/dev/audit",
            //alternately, "/proc"
            prov-tc:machineID="0000000100000001",
            prov:startedAtTime="015-10-16T02:13:07Z",
            prov:endedAtTime="015-10-16T02:13:07Z",
            prov-tc:privs="mode=u",
            foaf:accountName="dwa",
            prov-tc:group="Group1",
            prov-tc:pid="12",
            prov-tc:ppid="1",
            prov-tc:cwd="/users/dwa",
            prov-tc:commandLine="xterm",
            prov-tc:programName="xterm"])
//     the connection between them
```

Agent

An agent represents an actor that is not a UoE on a monitored machine. An agent may be human, may be a machine in the target network that has no monitoring, or may be a machine outside the monitored network. Agents have no required attributes. Available attributes include an identifier for a machine, a name, and an account name.

```
// a remote agent named ex:exernalAgent
agent(ex:externalAgent, [
        prov-tc:source="/dev/audit",
        //alternately, "/proc"
        prov-tc:machineID="0000000100000002"])
```

Metadatum

A metadatum is a thing that describes a UoE or an artifact. A metadatum is an entity that has an identifier and contains a triple of form (name, type, value).

```
// a metadatum named ex:mdata1
entity(ex:mdata1, [
    prov-tc:source="/dev/audit",
    //alternately, "/proc"
    prov-tc:metadata="name, type, value"]) //required
```

Relationships Among PROV-TC Entities

An artifact such as *ex:createExe* can be created by a UoE such as *ex:parentb* executing an operation *adapt:genOp* that is one of 'write', 'send', 'connect', 'truncate', 'chmod', or 'touch'. Other attributes include the time at which the generation event occurred, and the permissions with which the entity was created (if applicable).

```
// newprog.exe was created by the parent process (activity ex:parentb)
wasGeneratedBy(ex:createExe, ex:parentb, 015-10-16T02:13:07Z, [
                prov-tc:source="/dev/audit",
                //alternately, "/proc"
                prov-tc:operation="write",
                prov-tc:permissions="0o775",
                prov-tc:time="015-10-16T02:13:07Z"])
```

An artifact such as *ex:createExe* can be deleted by a UoE such as *ex:parentb*. The sole attribute, required, is the deletion time.

```
wasInvalidatedBy(ex:createExe, ex:parentb, 015-10-16T02:13:07Z, [
            prov-tc:source="/dev/audit",
            //alternately, "/proc"])
```

An artifact such as *ex:createExe* can be used by a UoE such as *ex:parentb* executing an operation *adapt:useOp* that is one of 'read', 'recv', 'accept', or 'execute'. Required attributes include the time of the use action, and the use operation. Optional attributes include an entry address (for example, if useOp is 'execute'), an argument list passed to an executed function, and a return value returned by an executed function.

```
used(ex:parentb, ex:createExe, 015-10-16T02:13:07Z,[
            prov-tc:source="/dev/audit",
            //alternately, "/proc"
            prov-tc:entryAddress="0x8048170",
            prov-tc:args="",
            prov-tc:returnValue="0",
            prov-tc:operation="execute",
            // alternately: "write", "send", "truncate", "chmod", "recv", "accept"
            prov-tc:time="015-10-16T02:13:07Z"]
                        )
```

Similarly, a resource such as *ex:GPSunit* may be used by a UoE such as *ex:childB*. Required are the start and end time of the use. Optionsl are a command string sent to the device and a value returned from the device.

```
used(ex:childB, ex:GPSunit, 015-10-16T02:13:07Z, [
            prov-tc:source="/dev/audit",
            //alternately, "/proc"
            prov-tc:operation="read",
            // alternately, "stop"
            // alternately, "write"
            // alternately, "start"
            prov-tc:returnValue="45.52119128833272,-122.67789063043892"
            ])
```

An artifact such as *ex:createExe* can be attributed to a UoE or an agent such as *ex:parenta*.

```
wasAttributedTo(ex:createExe, ex:parenta, [
            prov-tc:source="/dev/audit",
            //alternately, "/proc"])
```

A UoE such as *ex:parenta* can act on behalf of an agent such as *ex:externalAgent*. Note that the activity portion of the UoE is shown in the third argument position:

```
// the parent process acted on behalf of this remote agent
actedOnBehalfOf(ex:parenta, ex:externalAgent, ex:parentb, [
            prov-tc:source="/dev/audit",
            //alternately, "/proc"])
```

A UoE can be associated with an agent. This relationship is somewhat looser and less well defined than the above case.

```
// the parent process was also associated with this remote agent
wasAssociatedWith(ex:parentb, ex:externalAgent, -, [
            prov-tc:source="/dev/audit",
            //alternately, "/proc"])
```

A UoE can start, end, or inform another UoE. The former requires a start time, while the middle requires an end time. The latter requires both a timestamp and the operation that must be one of fork, clone, execve, kill, or setuid.

```
wasStartedBy(ex:childB, -, ex:parentb, 015-10-16T02:13:07Z, [
            prov-tc:source="/dev/audit",
            //alternately, "/proc"])

wasEndedBy(ex:childB, -, ex:parentb, 015-10-16T02:13:07Z, [
            prov-tc:source="/dev/audit",
            //alternately, "/proc"])

wasInformedBy(ex:childB, -, ex:parentb, 015-10-16T02:13:07Z, [
            prov-tc:source="/dev/audit",
            // alternately, "/proc"
            adapt:operation="kill"
            // alternately, "fork", "clone", "execve", "setuid"
            ])
```

An artifact such as *ex:newprogExe* can be derived from another artifact such as *ex:newprogSrc* using an *adapt:deriveOp* operation that is one of rename, link, or compile.

```
// showing the derivation of newprog.exe from newprog.c
wasDerivedFrom(ex:newprogExe, ex:newprogSrc, [
            prov-tc:source="/dev/audit",
            //alternately, "/proc"
            prov-tc:operation="compile",
            // alternately, "rename", "link"
            prov-tc:time="015-10-16T02:13:07Z"])
```

An artifact can be part of another artifact. We use dc:isPartOf for this construction.

```
dc:isPartOf(ex:childThing, ex:parentThing)
```