SACM Tasks

Henk Birkholz, Dan Haynes,
Nancy Cam-Winget, Jarret Lu

Management of Target Endpoints over time

- Improving the definition of SACM tasks
- Providing more structure to the targeted Collection and the complementary un-targeted Discovery Task
- Keeping track of target endpoints over time via Characterization Records

SACM Tasks

- SACM components are composed of software that conducts SACM tasks
  - e.g. TE discovery, TE characterization, collection, etc
- SACM tasks are about Target Endpoint Assessment or SACM component control and management
- SACM components can act as an provider or a consumer
  - correspondingly SACM tasks provide or consume data (Input/Output of tasks)
- SACM tasks are based on use SACM use cases that are generalized and defined in the architecture and the information model

Goals of SACM Tasks

- Assessment of Target Endpoints ("endpoints of interest")
- Providing the prerequisites for Target Endpoints Assessment
  - associate provided information that is "about a target endpoint“, e.g. software running on a TE
- Over time SACM Tasks:
  - refine and update that collection of data,
  - "re-detect" the presence of a target endpoint, and
  - assert that "this is the information that could be acquired before"

SACM Tasks and Target Endpoints

- SACM tasks do handle/process:
  - different kinds of target endpoints
  - in different ways (e.g. different interfaces or methods)
  - via different kinds of SACM components
- TE (the endpoints of interest) compose a spectrum ranging from:
  - owned, classified, e.g. including an internal collector
  - unknown, hardened, e.g. observable only via network behavior

"Front line" SACM Task: Collection

- "**targeted task**" that can be triggered by (i.e. consumes output of) the discovery task
- requires some **initial knowledge** regarding "what to collect" and "how to collect“ (guidance based on, e.g. discovery)
- i.e. the collection tasks requires a notion about "collect from/about this target endpoint"

"Front line" SACM Task: TE Discovery

- "**un-targeted tasks**" that acquire potential attributes about known or previously unknown target endpoints.
- **ongoing** acquisition of potential endpoint attributes from infrastructure components, such as switches, routers, aaa servers, dynamic address distribution, IDS, network profiler, etc.
- these task can run on the **infrastructure components** themselves or can acquire potential endpoint attributes from infrastructure components remotely

Keeping track of target endpoints over time

- Target Endpoints **cannot always** be associated with an identifier that is unique in a SACM domain due to potentially "lying" or obfuscating target endpoints, unmet requirements, etc.
- The **Characterization Task** addresses this problem by:
  - creating characterization records for each set of endpoint attributes that might represent a distinguishable target endpoint
  - splitting and merging or simply associating these records over time
- A record **can be** associated with a unique label in a SACM domain.
  - if information is sparse, more then one record can represent the same target endpoint
  - if not enough information (associated target endpoint attributes) is available this cannot be avoided

Examples

- **Known TE** with Internal collector:
  - the collector is **pre-deployed** on a target endpoint and the TE is well known to the enterprise
  - the **discovery task** is "a formality", the internal collector initiates communication with the SACM domain and identifies itself
- **Unknown TE** with no interfaces to collect from:
  - the **only** initially available endpoint attributes are network-related , e.g. layer2 addresses and layer3 packet flows
  - the **discovery task** is initially the primary provider of information, a targeted collection is limited to continuous observation of network behavior until the discovery task can provide more endpoint attributes that would indicate other viable ways of collection

Characterization Record

- Each Characterization Record is intended to represent a **single target endpoint**
  - it includes every endpoint attribute that can be associated in a way that implies it is about a specific target endpoint
  - therefore, a Characterization Record includes all identifying target endpoint attributes that could be acquired over time

Managing Characterization Record over time

- if a discovered or collected endpoint attribute cannot be associated with an existing Characterization Record, a new one is **created** (because it is probably about a previously unknown target endpoint)
- if freshly acquired endpoint attributes indicate that two records are about the same target endpoint, they are **merged**
- if freshly acquired endpoint attributes indicate that a record is actually about two target endpoints it has to be **split up**

No more content.
This is the last slide.