790-132: Principled Security **Spring 2017**

Hyperproperties

Lecturer: Lee Barnett *Date: January 19*

1 Introduction

Some security policies are not easily expressed as properties of individual execution traces.

Example. Service-level agreements, non-interference, secure information flow

More generally, any policy that stipulates relations among traces is not a property. We want to extend the theory for trace properties (like we saw in Calvin's talk) to formalize security policies in the same way.

Formalize security policies as properties of *systems*, which we represent by sets of execution traces. Then

Definition. *A* hyperproperty *is a set of trace properties.*

Qualities of system behavior can be specified as hyperproperties. Thus hyperproperties can describe both trace properties and security policies.

Like trace properties, every hyperproperty is expressible as the intersection of a safety hyperproperty and a liveness hyperproperty.

2 Hyperproperties

Σ – finite set of states

t – trace, where $t \in \Sigma^* \cup \Sigma^\omega =: \Psi$

$t[i], t[..i], t[i..]$ – same as last time

$t \leq t'$ – t is a prefix of t'

π – system, where $\pi \subseteq \Sigma^\omega$ and $\pi \neq \emptyset$

Prop $:= \mathcal{P}(\Sigma^\omega)$ – set of trace properties

For $P \in$ Prop and set of traces T, say T *satisfies* P (written $T \models P$) when $T \subseteq P$

We need hyperproperties to specify certain security policies, but notice that some policies are expressible as trace properties this way.

Example. Guaranteed Service. Policy requiring that every request is eventually satisfied. Let $\text{isReq}(s)$ and $\text{isRespToReq}(s', s)$ be state predicates. Can specify the policy as

$$\{t \in \Sigma^\omega \mid \forall i \in \mathbb{N}\ (\text{isReq}(t[i]) \Longrightarrow \exists j > i\ (\text{isRespToReq}(t[j], t[i])))\}$$

The set of all hyperproperties $\boldsymbol{HP}$ is defined as $\mathcal{P}(\text{Prop})$

Definition. *A set T of traces* satisfies *a hyperproperty $\boldsymbol{H}$, written $T \models \boldsymbol{H}$, when $T \in \boldsymbol{H}$.*

Definition. *The* lift *of a trace property P is the hyperproperty $[\boldsymbol{P}] := \mathcal{P}(P)$*

We can describe security policies not expressible as trace properties using hyperproperties.

Example. Mean response time. Policy requiring that the mean response time over all executions in a system is less than 1 second. Let $\text{respTimes}(t)$ be the set of response times (in seconds) from request/response events in a trace t. Can specify the policy as

$$\boldsymbol{RT} = \left\{ T \in \text{Prop} \;\middle|\; \text{avg}\left(\bigcup_{t \in T} \text{respTimes}(t) \right) \leq 1 \right\}$$

Example. Non-interference. Policy requiring that commands issued by high-level users should be removable without affecting low-level user observations. For trace t define

- $ev(t)$ – sequence of input / output events occurring when system transitions between the states of t
- $ev_{\text{L}}(t)$ – low-level events in $ev(t)$
- $ev_{\text{H-in}}(t)$ – high-level input events in $ev(t)$.

Can specify the policy as

$$\boldsymbol{NI} = \{T \in \text{Prop} \mid T \in \boldsymbol{SM} \wedge \forall t \in T \ (\exists t' \in T \ (ev_{\text{H-in}}(t') = \epsilon \wedge ev_{\text{L}}(t') = ev_{\text{L}}(t)))\}$$

2.1 Hypersafety

Covered safety properties last time. Slightly different formulation:

Definition. *A trace property S is a* safety property *if*

$$\forall t \in \Sigma^\omega \ (t \notin S \Longrightarrow \exists m \in \Sigma^* \ (m \leq t \wedge \forall t' \in \Sigma^\omega \ (m \leq t' \Longrightarrow t' \notin S)))$$

Want to generalize this to define safety hyperproperties. Need the following:

$\text{Obs} := \mathcal{P}^{\text{fin}}(\Sigma^*)$ – set of *observations* (collection of finite traces)

$T \leq T'$ for sets of traces T, T' if for each trace $t \in T$ there is a $t' \in T'$ such that $t \leq t'$.

Definition. *A hyperproperty $\boldsymbol{S}$ is a* safety hyperproperty*, or is* hypersafety*, if*

$$\forall T \in \text{Prop} \ (T \notin \boldsymbol{S} \Longrightarrow \exists M \in \text{Obs} \ (M \leq T \wedge (\forall T' \in \text{Prop} \ (M \leq T' \Longrightarrow T' \notin \boldsymbol{S}))))$$

Example. Non-interference $\boldsymbol{NI}$ above is hypersafety.

S is a safety property iff $[\boldsymbol{S}]$ is a safety hyperproperty.

2.2 Hyperliveness

Covered liveness properties last time. Again, slightly different formulation:

Definition. *A trace property L is a* liveness property *if*

$$\forall t \in \Sigma^* \ (\exists t' \in \Sigma^\omega \ (t \leq t' \wedge t' \in L))$$

Want to generalize to get hyperliveness (in the same way we did from safety to hypersafety)

Definition. *A hyperproperty $\boldsymbol{L}$ is a* liveness hyperproperty*, or is* hyperliveness*, if*

$$\forall T \in \text{Obs} \ (\exists T' \in \text{Prop} \ (T \leq T' \wedge T' \in \boldsymbol{L}))$$

Example. Mean-response time $\boldsymbol{RT}$ above is hyperliveness.

L is a liveness property iff $[\boldsymbol{L}]$ is a liveness hyperproperty.

2.3 Other hyperproperties

Not all hyperproperties are hypersafety or hyperliveness.

Example. Medical information system. Must (1) maintain confidentiality of patient records and (2) eventually notify patients when their records are accessed.

Recall that all trace properties are the intersection of a safety property and a liveness property. Analogous result holds for hyperproperties:

Theorem. $\forall \boldsymbol{P} \in \boldsymbol{HP} \ (\exists \boldsymbol{S} \in \boldsymbol{SHP}, \boldsymbol{L} \in \boldsymbol{LHP} \ (\boldsymbol{P} = \boldsymbol{S} \cap \boldsymbol{L}))$

3 Topology

Broad area of math dealing with properties of space preserved under continuous deformations

> "A cardinal principle of modern mathematical research may be stated as a maxim: One must always topologize." – Marshall Stone

Topological space– (S, τ) with $\tau \subseteq \mathcal{P}(S)$ s.t. $\emptyset \in \tau$, $S \in \tau$, and τ is closed under finite intersections and (arbitrary) unions.

Elements of a topology are called *open* sets. The complement of an open set is a *closed* set.

A set that intersects every nonempty open set is called *dense*.

A *basis* for a topology is a collection of sets $\mathcal{B}$ such that every open set is a union of elements in $\mathcal{B}$.

A *subbasis* is a collection of sets $\mathcal{A}$ such that the finite intersections of elements of $\mathcal{A}$ form a basis.

3.1 Topology of properties

Definition. *A property O is* observable *if*

$$\forall t \in \Sigma^\omega \ (t \in O \Longrightarrow (\exists m \in \Sigma^* \ (m \leq t \land (\forall t' \in \Sigma^\omega \ (m \leq t' \Longrightarrow t' \in O)))))$$

Let $\mathcal{O}$– set of observable properties. Then $(\Sigma^\omega, \mathcal{O})$ is a topological space, and $\mathcal{O}$ is called the *Plotkin* topology.

Correspondence in the Plotkin topology:

- Closed sets are safety properties
- Dense sets are liveness properties

Can prove the intersection theorem about trace properties using this topology.

3.2 Topology of hyperproperties

Want to construct a topology that extends this correspondence to hyperproperties.

$\uparrow M := \{T \in \text{Prop} \mid M \leq T\}$ – *completion* of an observation $M \in \text{Obs}$.

Then $\boldsymbol{\mathcal{O}^{SB}} := \{\uparrow M \mid M \in \text{Obs}\}$ is a subbasis for such a topology.

This is in fact a well-known topology called the *Vietoris* topology.

Let $\boldsymbol{\mathcal{C}}$– closed sets, $\boldsymbol{\mathcal{D}}$– dense sets. Then:

- $\text{SHP} = \boldsymbol{\mathcal{C}}$
- $\text{LHP} = \boldsymbol{\mathcal{D}}$

4 Remarks

SP – set of all safety properties is not hypersafety (in fact it is hyperliveness)

LP – set of all liveness properties is hyperliveness

Only hyperproperty that is both hyperliveness and hypersafety is $\boldsymbol{true} := \text{Prop}$.

Note also that $\boldsymbol{false} := \{\emptyset\}$ is hypersafety but not hyperliveness.

References

[1] M. Clarkson and F. Schneider, "Hyperproperties," *Journal of Computer Security, 18*, 2010, pp. 1157–1210.