Specialisation of Attack Trees with Sequential Refinement

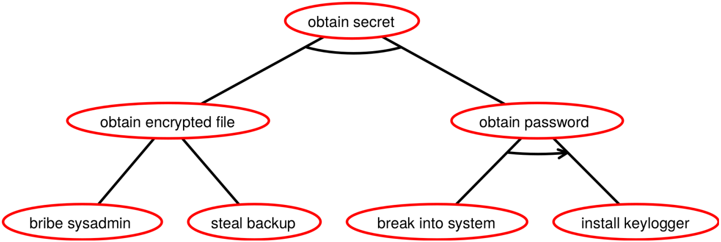
Seminar for Security and Trust of Software Systems group at University of Luxembourg

Ross Horne

School of Computer Science and Engineering, Nanyang Technological University, Singapore

7 November 2017

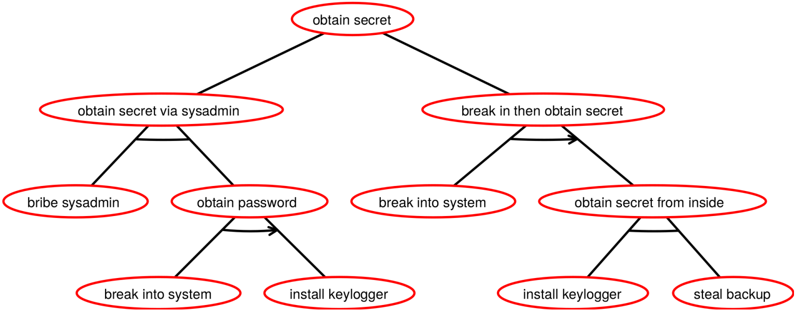
Causal Attack Trees



Three types of refinement:

- Node with undirected arc represents *conjunctive refinement*.
- Node with no arc represents *disjunctive refinement*.
- Node with directed arc represents *sequential refinement*.

Attack Trees Evolve as Domain Knowledge is Specialised



In this specialised tree, “steal backup” can only be performed after breaking into the system.

Criterion for Specialisation of Attack Trees

Criterion:

A **specialisation** between attack tree is **sound** with respect to an **attribute domain** whenever:

valuations are **correlated**, for any assignment of values to basic actions.

Notes:

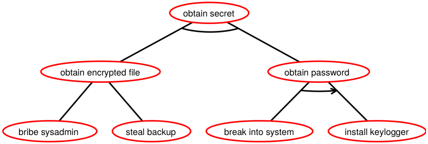
- "specialisation" and "correlation" have many interpretations.
- more general than equality.

Example: Minimum Attack Time Attribute Domain

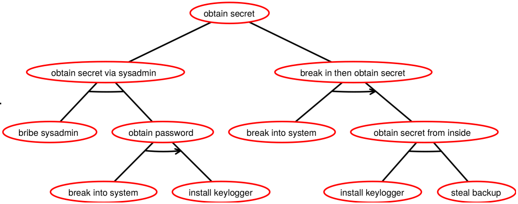
Basic minimum attack times:

bribe sysadmin $\mapsto 25$ steal backup $\mapsto 5$ break into system $\mapsto 9$ install keylogger $\mapsto 2$

$\max\{\min\{25, 5\}, 9+2\} = 11$



$\min\{\max\{25, 9+2\}, 9+\max\{2, 5\}\} = 14$



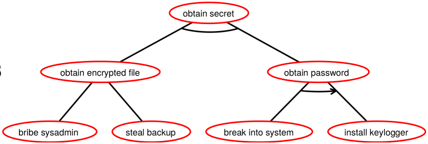
How do we know: first $\leq$ second for all assignments?

Example: Minimum Number of Experts

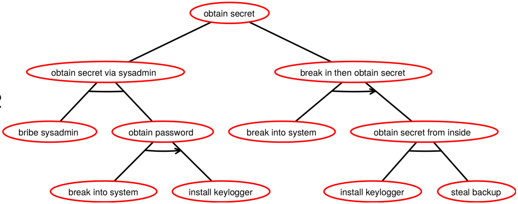
Basic number of experts:

bribe sysadmin $\mapsto 3$ steal backup $\mapsto 1$ break into system $\mapsto 2$ install keylogger $\mapsto 1$

$\min\{3, 1\} + \max\{2, 1\} = 3$

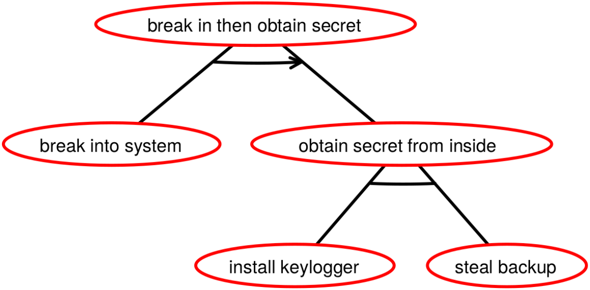


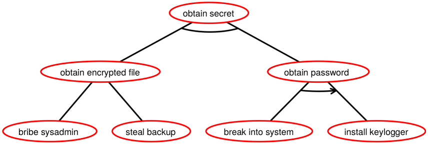
$\min\{3 + \max\{2, 1\}, \max\{2, 1 + 1\}\} = 2$



Valuations correlated, but in opposite direction to previous example.

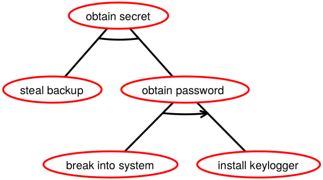
Trees Correlated Only for Some Domains

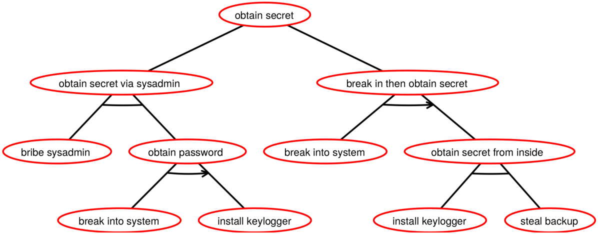




- Correlated for “minimum attack time”.
- Uncorrelated for “minimum number of experts”. (Some some valuations $\leq$ other $\geq$)

Trees Correlated Only for Some Domains





Uncorrelated for “minimum attack time”. Check assignments:

bribe sysadmin $\mapsto$ 25 steal backup $\mapsto$ 5 break into system $\mapsto$ 9 install keylogger $\mapsto$ 2

bribe sysadmin $\mapsto$ 25 steal backup $\mapsto$ 35 break into system $\mapsto$ 9 install keylogger $\mapsto$ 2

Correlated for “minimum number of experts”.

- Even for small examples, *time consuming* and *error-prone* to judge specialisations.
- Unclear what “specialisation” means.
- Better to have tool to check automatically to assist with attack tree manipulation.

Solution define a **semantics** with a **decidable** specialisation relation.
(sound for classes for attribute domain)

Linear Logic in the Sequent Calculus

MALL (Girard 1993):

$$\frac{}{\vdash \overline{a}, a}\ axiom \qquad \frac{\vdash P, Q, \Delta}{\vdash P \parallel Q, \Delta}\ \parallel \qquad \frac{\vdash P, \Gamma \quad \vdash Q, \Delta}{\vdash P \otimes Q, \Gamma, \Delta}\ \otimes \qquad \frac{\vdash \Gamma \quad \vdash \Delta}{\vdash \Gamma, \Delta}\ mix$$

$$\frac{\vdash P_i, \Delta}{\vdash P_1 \oplus P_2, \Delta}\ \oplus,\ i \in \{1, 2\} \qquad \frac{\vdash P, \Delta \quad \vdash Q, \Delta}{\vdash P \,\&\, Q, \Delta}\ \&$$

Linear negation defines de Morgan dualities:

$$\overline{P \parallel Q} = \overline{P} \otimes \overline{Q} \qquad \overline{P \otimes Q} = \overline{P} \parallel \overline{Q}$$

$$\overline{P \,\&\, Q} = \overline{P} \oplus \overline{Q} \qquad \overline{P \oplus Q} = \overline{P} \,\&\, \overline{Q}$$

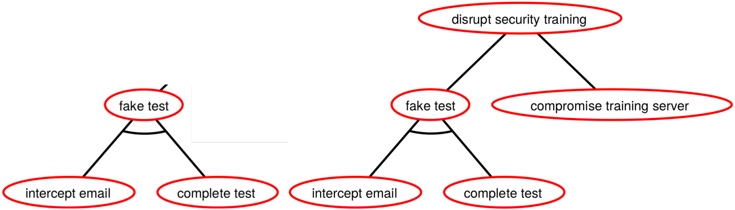
$$\overline{\overline{a}} = a$$

Linear implication (not P or Q):

$$P \multimap Q = \overline{P} \parallel Q$$

A Semantics Refining the Multi-set Semantics for Attack Trees

Attack trees related by specialisation:



Proof in sequent calculus:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\overline{\text{intercept email}}, \text{intercept email}}\,\textit{axiom} \qquad \dfrac{}{\overline{\text{complete test}}, \text{complete test}}\,\textit{axiom}}{\overline{\text{intercept email}} \otimes \overline{\text{complete test}}, \text{intercept email}, \text{complete test}}\,\otimes}{\vdash \overline{\text{intercept email}} \otimes \overline{\text{complete test}}, \text{intercept email} \mathbin{||} \text{complete test}}\,||}{\vdash \overline{\text{intercept email}} \otimes \overline{\text{complete test}}, (\text{intercept email} \mathbin{||} \text{complete test}) \oplus \text{compromise server}}\,\oplus}{\vdash (\text{intercept email} \mathbin{||} \text{complete test}) \multimap ((\text{intercept email} \mathbin{||} \text{complete test}) \oplus \text{compromise server})}\,||$$

Extending for Sequentiality in the Calculus of Structures

MAV (Horne 2015) in Calculus of Structures (Guglielmi 2007):

$$\frac{\vdash \mathcal{C}\{\, \mathrm{I} \,\}}{\vdash \mathcal{C}\{\, \overline{\alpha} \parallel \alpha \,\}} \text{ atomic interaction} \qquad \frac{\vdash \mathcal{C}\{\, (P \parallel R) \mathbin{;} (Q \parallel S) \,\}}{\vdash \mathcal{C}\{\, (P \mathbin{;} Q) \parallel (R \mathbin{;} S) \,\}} \textit{ seq} \qquad \frac{\vdash \mathcal{C}\{\, P \otimes (Q \parallel R) \,\}}{\vdash \mathcal{C}\{\, (P \otimes Q) \parallel R \,\}} \textit{ switch}$$

$$\frac{\vdash \mathcal{C}\{\, P_i \,\}}{\vdash \mathcal{C}\{\, P_1 \oplus P_2 \,\}} \textit{ choice} \qquad \frac{\vdash \mathcal{C}\{\, (P \parallel R) \,\&\, (Q \parallel R) \,\}}{\vdash \mathcal{C}\{\, (P \,\&\, Q) \parallel R \,\}} \textit{ external}$$

$$\frac{\vdash \mathcal{C}\{\, (P \,\&\, R) \mathbin{;} (Q \,\&\, S) \,\}}{\vdash \mathcal{C}\{\, (P \mathbin{;} Q) \,\&\, (R \mathbin{;} S) \,\}} \textit{ medial} \qquad \frac{\vdash \mathcal{C}\{\, \mathrm{I} \,\}}{\vdash \mathcal{C}\{\, \mathrm{I} \,\&\, \mathrm{I} \,\}} \textit{ tidy} \qquad \frac{}{\vdash \mathrm{I}} \textit{ axiom}$$

commutative monoids: $(P, \parallel, \mathrm{I})$ $(P, \otimes, \mathrm{I})$ monoid: $(P, \mathbin{;}, \mathrm{I})$

de Morgan dualities

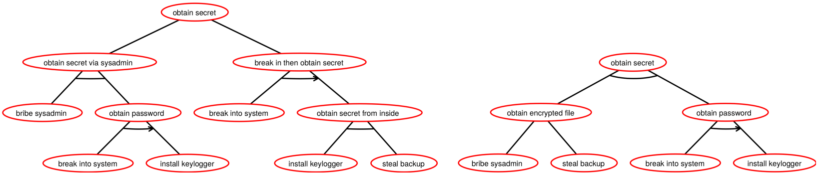
$$\overline{P \otimes Q} = \overline{P} \parallel \overline{Q} \qquad \overline{P \parallel Q} = \overline{P} \otimes \overline{Q}$$

$$\overline{P \oplus Q} = \overline{P} \,\&\, \overline{Q} \qquad \overline{P \,\&\, Q} = \overline{P} \oplus \overline{Q}$$

$$\overline{P \mathbin{;} Q} = \overline{P} \mathbin{;} \overline{Q} \qquad \overline{\overline{\alpha}} = \alpha \qquad \overline{\mathrm{I}} = \mathrm{I}$$

Example Verified using the Calculus of Structures

The first tree specialises (implies) the second.



Proof:

$$\frac{\overline{\;\;}}{\mathrm{I}}\ \textit{axiom}$$

$$\frac{\mathrm{I}}{\mathrm{I}\ \&\ \mathrm{I}}\ \textit{tidy}$$

interaction

$$\vdash \left(\left(\overline{bribe} \parallel bribe\right) \otimes \left(\left(\overline{breakin} \parallel breakin\right) ; \left(\overline{install} \parallel install\right)\right)\right) \mathbin{\&} \left(\left(\overline{breakin} \parallel breakin\right) ; \left(\left(\overline{steal} \parallel steal\right) \otimes \left(\overline{install} \parallel install\right)\right)\right)$$

switch

$$\vdash \left(\left(\overline{bribe} \parallel bribe\right) \otimes \left(\left(\overline{breakin} \parallel breakin\right) ; \left(\overline{install} \parallel install\right)\right)\right) \mathbin{\&} \left(\left(\overline{breakin} \parallel breakin\right) ; \left(\left(\overline{steal} \otimes \overline{install}\right) \parallel steal \parallel install\right)\right)$$

sequence

$$\vdash \left(\left(\overline{bribe} \parallel bribe\right) \otimes \left(\left(\overline{breakin} ; \overline{install}\right) \parallel \left(breakin ; install\right)\right)\right) \mathbin{\&} \left(\left(\overline{breakin} ; \left(\overline{steal} \otimes \overline{install}\right)\right) \parallel steal \parallel \left(breakin ; install\right)\right)$$

switch

$$\vdash \left(\left(\overline{bribe} \otimes \left(\overline{breakin} ; \overline{install}\right)\right) \parallel bribe \parallel \left(breakin ; install\right)\right) \mathbin{\&} \left(\left(\overline{breakin} ; \left(\overline{steal} \otimes \overline{install}\right)\right) \parallel steal \parallel \left(breakin ; install\right)\right)$$

choice

$$\vdash \left(\left(\overline{bribe} \otimes \left(\overline{breakin} ; \overline{install}\right)\right) \parallel \left(bribe \oplus steal\right) \parallel \left(breakin ; install\right)\right) \mathbin{\&} \left(\left(\overline{breakin} ; \left(\overline{steal} \otimes \overline{install}\right)\right) \parallel \left(bribe \oplus steal\right) \parallel \left(breakin ; install\right)\right)$$

external

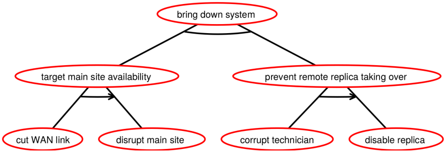
$$\vdash \left(\left(\overline{bribe} \otimes \left(\overline{breakin} ; \overline{install}\right)\right) \mathbin{\&} \left(\overline{breakin} ; \left(\overline{steal} \otimes \overline{install}\right)\right)\right) \parallel \left(bribe \oplus steal\right) \parallel \left(breakin ; install\right)$$

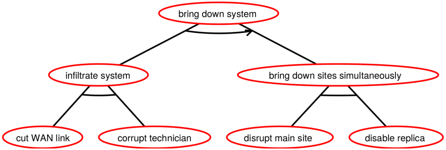
definition

$$\vdash \left(bribe \parallel \left(breakin ; install\right)\right) \oplus \left(breakin ; \left(steal \parallel install\right)\right) \multimap \left(bribe \oplus steal\right) \parallel \left(breakin ; install\right)$$

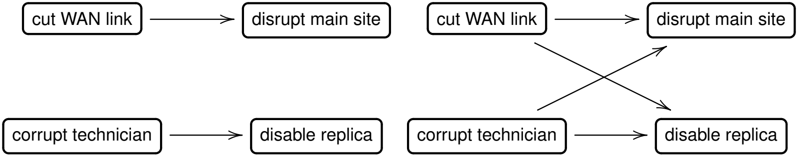
Relates Trees Unrelated by Related Semantics for Causal Attack Trees

Trees Related by Specialisation (but not by set inclusion in Jhawar et al. 2015):



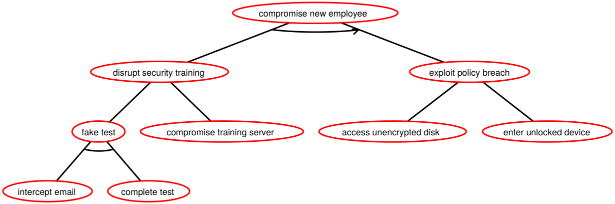


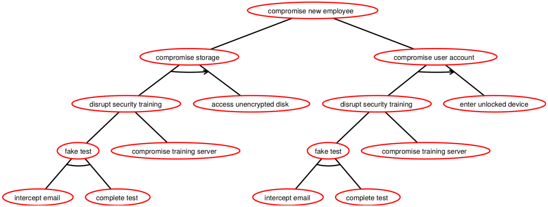
Extra causal dependencies clear in graphical model (adapted from Gischer 1988):



Subtleties: Partial Distributivity

Trees equivalent for Jhawar et al. 2015.





..but specialisation holds in one direction only according to MAV.

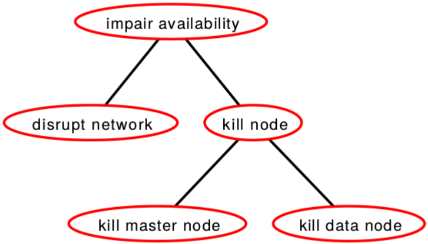
“Operational” explanation: The “local” disjunctive refinment allows choices to be delayed ...permits less coordination between sub-goals.

Perspectives on attack trees

- **Non-deterministic v.s. probabilistic choice:** *minimum* time selects best case choices; *maximum* time selects worst case; *expected* time involves a contribution from all branches; hence projection forbidden.

- **Attack-defence trees:** Semantics lifts to specialisation for attack-defence trees respecting multi-sets semantics (that assumes attacker resolves all choices).

- **Breaking asymmetry:** Does the attacker always have control of choices made during an attack? E.g. can the attacker actively chose whether it is killing a master node or data node in the following (the defender may pro-actively conceal the master node).



- **Provenance and fault diagrams:** provenance diagrams (origin of MAV), fault diagrams ("safety" countermeasures suggest exploitable vulnerabilities)... there are common foundations and applications.

Conclusion

- **Specialisation** useful for comparing attack trees that are **not necessarily equal**.
- Semantics for specialisation depends on **class of attribute domain**:
  - One class illustrated by “minimum attack time”;
  - Another class illustrated by “minimum number of experts”.
- **Semantics** for each class provided by embedding in logical system MAV.
- Specialisation is **decidable**. ...leading to support in ADTool?
- *...but does the attacker always have control of choices?*