The Attacker Does not Always Hold the Initiative:

Attack Trees with External Refinement

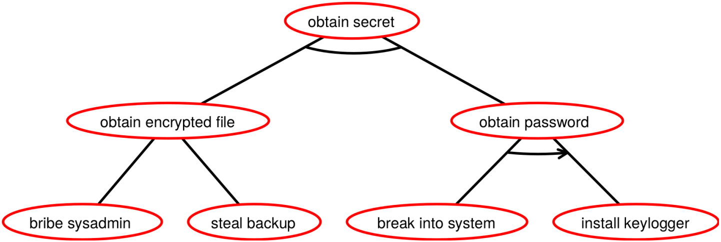
GraMSec 2018, The Fifth International Workshop on Graphical Models for Security

Ross Horne[1], Sjouke Mauw[2] and Alwen Tiu[3]

1. School of Computer Science and Engineering, Nanyang Technological University, Singapore
2. Security and Trust of Software Systems, University of Luxembourg, Luxembourg
3. Research School of Computer Science, Australian National University, Canberra, Australia

8 July 2018

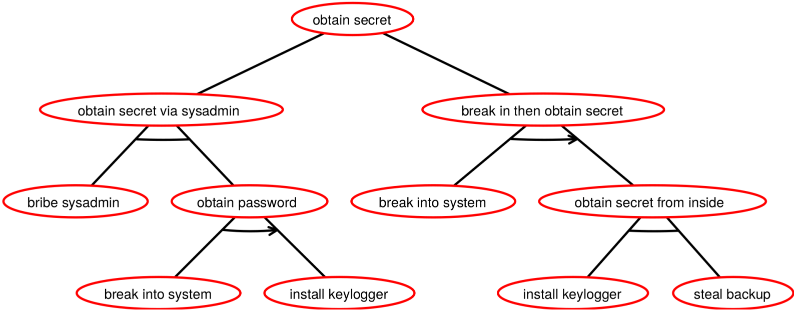
Background: Causal Attack Trees



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:

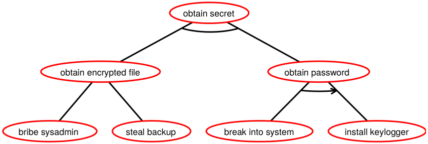
- “specialisation” and “correlation” have many interpretations.
- more general than equality.

Example: Minimum Attack Time Attribute Domain

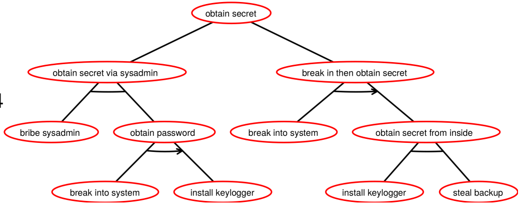
Basic minimum attack times:

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

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



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



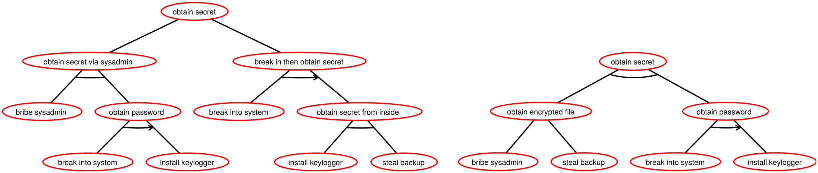
How do we know: first $\leq$ second for all assignments?

- 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 sound **semantics** with a **decidable** specialisation relation.

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

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

switch

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

sequence

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

switch

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

choice

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

external

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

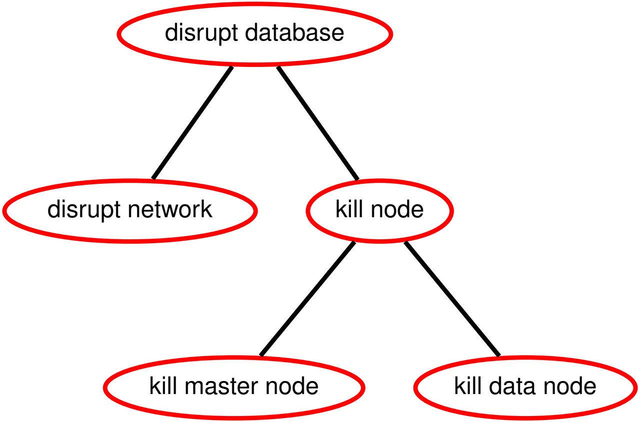
definition

$$\left(\textit{bribe} \parallel \left(\textit{breakin} ; \textit{install}\right)\right) \oplus \left(\textit{breakin} ; \left(\textit{steal} \parallel \textit{install}\right)\right) \multimap \left(\textit{bribe} \oplus \textit{steal}\right) \parallel \left(\textit{breakin} ; \textit{install}\right)$$

Breaking Asymmetry between the Attacker and its Environment

Does the attacker always have control of choices made during an attack?

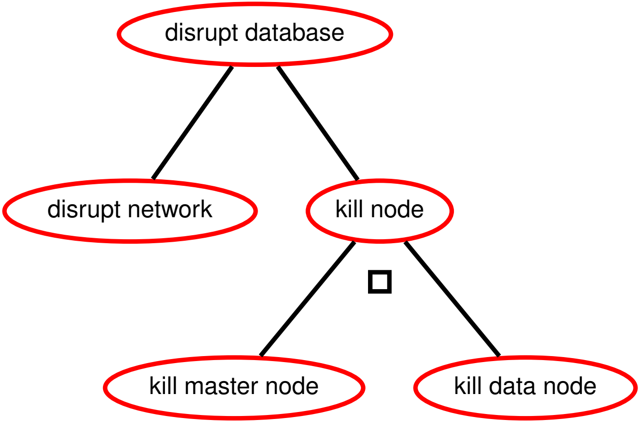
E.g. Can the attacker actively chose whether it is killing a master node or data node?



Breaking Asymmetry between the Attacker and its Environment

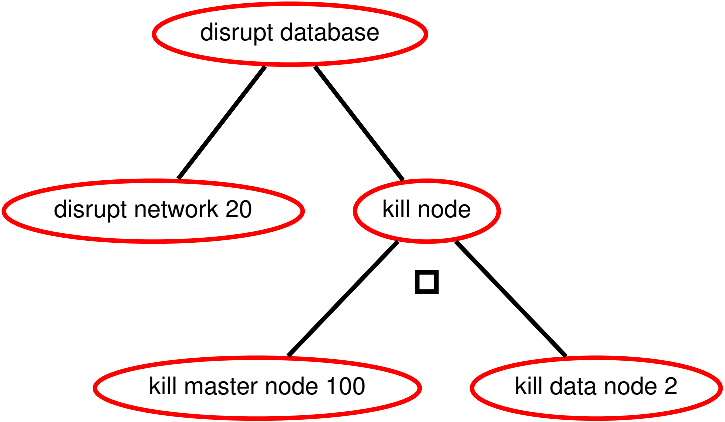
Does the attacker always have control of choices made during an attack?

E.g. Can the attacker actively chose whether it is killing a master node or data node?

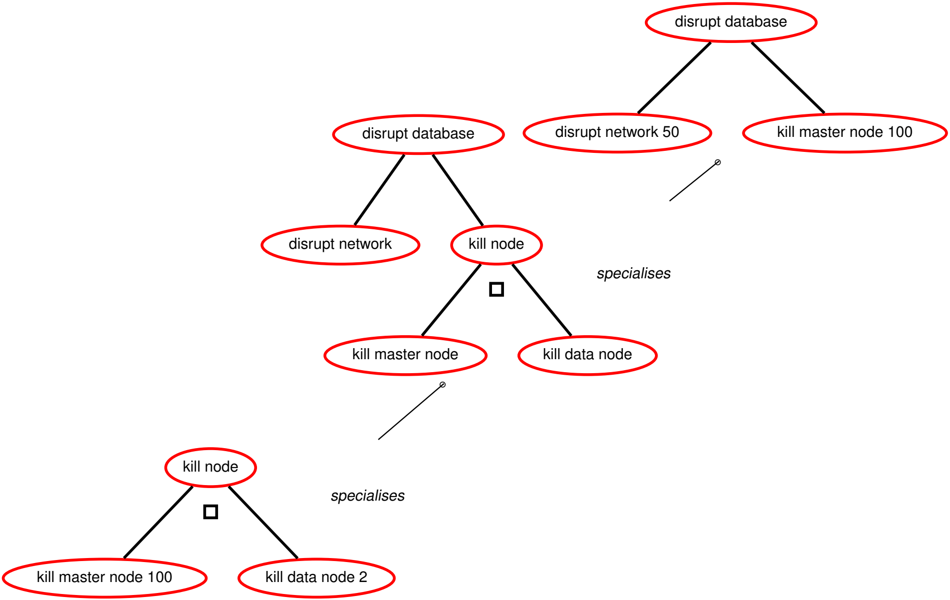


Impact of External Refinement on Quantative Analysis: Max Damage

What is the optimal attack strategy?



Trees Related by Specialisation



Additive Linear Logic in the Sequent Calculus

MALL (Girard 1993):

$$\frac{}{\vdash \overline{a}, a}\ \textit{axiom} \qquad \frac{\vdash P_i, R}{\vdash P_1 \oplus P_2, R}\ \oplus,\ i \in \{1,2\} \qquad \frac{\vdash P, R \quad \vdash Q, R}{\vdash P \,\&\, Q, R}\ \& \qquad \frac{\vdash Q, P}{\vdash P, Q}\ \textit{exchange}$$

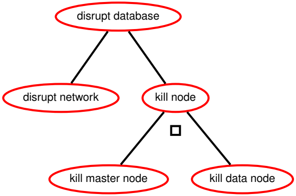
De Morgan dualities:

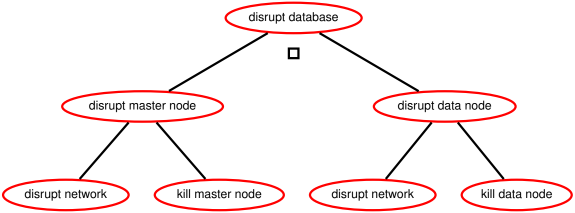
$$\overline{P \,\&\, Q} = \overline{P} \oplus \overline{Q} \qquad \overline{P \oplus Q} = \overline{P} \,\&\, \overline{Q} \qquad \overline{\overline{a}} = a$$

Linear implication ($P \multimap Q$):

$$\vdash \overline{P}, Q$$

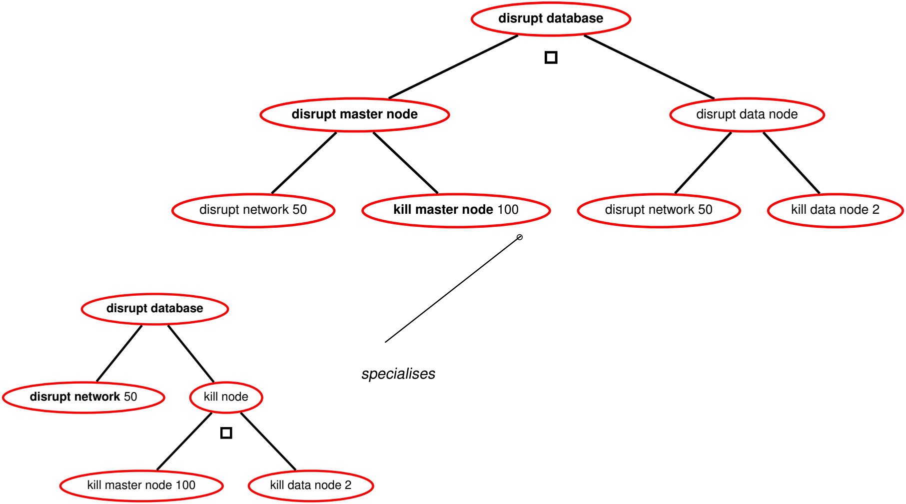
Proof of Specialisation between Attack Trees



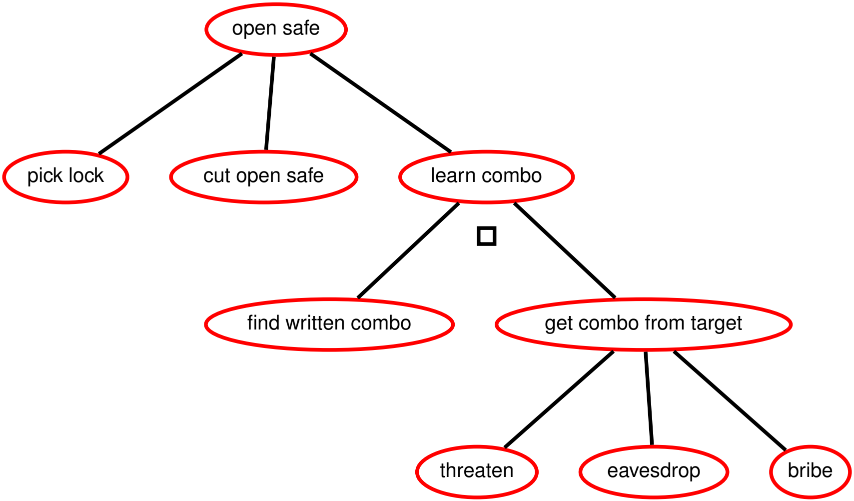


$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \overline{a}, a}\,axiom}{\vdash \overline{a}, a \oplus b}\,\oplus \qquad \dfrac{\dfrac{}{\vdash \overline{a}, a}\,axiom}{\vdash \overline{a}, a \oplus c}\,\oplus}{\vdash \overline{a}, (a \oplus b)\ \&\ (a \oplus c)}\,\& \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \overline{b}, b}\,axiom}{\vdash \overline{b}, a \oplus b}\,\oplus}{\vdash \overline{b} \oplus \overline{c}, a \oplus b}\,\oplus \qquad \dfrac{\dfrac{\dfrac{}{\vdash \overline{c}, c}\,axiom}{\vdash \overline{c}, a \oplus c}\,\oplus}{\vdash \overline{b} \oplus \overline{c}, a \oplus c}\,\oplus}{\vdash \overline{b} \oplus \overline{c}, (a \oplus b)\ \&\ (a \oplus c)}\,\&}{\vdash \overline{a}\ \&\ (\overline{b} \oplus \overline{c}), (a \oplus b)\ \&\ (a \oplus c)}\,\&$$

Uncertaintly in Environment and Attributes: All Strategies Preserved



Are Choices External in Schneier's Example?



Note: do not prune tree since *find writen combo* not impossible.

Conclusion

- **Specialisation** useful for comparing attack trees that are **not necessarily equal**.
- **Semantics** for each class provided by embedding in (extensions of) Linear Logic.
- Asymmetry between **Attacker** and **Environment** broken by marking *external* choices.
- Even without probabilities, specialisation is sensitive to *uncertain information*.
- . . . relevant to Moving Target Defence?