Knowledge and Effect: A Logic for Reasoning about Confidentiality and Integrity Guarantees

(Extended Abstract)

Scott Moore
Harvard SEAS
sdmoore@seas.harvard.edu

Aslan Askarov
Aarhus University
aslan@cs.au.dk

Stephen Chong
Harvard SEAS
chong@seas.harvard.edu

Epistemic logic has previously been used to specify confidentiality security properties [1, 2]. In this work, we introduce modal operators for reasoning about integrity security properties and security properties that combine integrity and confidentiality. Epistemic modal operators can be used to reason what agents *know*; our new modal operators can be used to reason about what agents *effect* (i.e., what agents bring about, or accomplish).

In our logic, modal operator K_A is a standard epistemic operator: formula $K_A\phi$ means that agent A knows formula ϕ. We introduce a new *effect modal operator*, E_A. Formula $E_A\phi$ means agent A is able to "effect" or "bring about" formula ϕ, that is, A's actions ensure that ϕ is true.

We define the semantics of the logic using a Kripke-style possible-worlds semantics. We assume that for every agent A there are two equivalence relations over worlds: the *observational equivalence relation* $\sim_A^{\text{obs}}$, and the *strategy equivalence relation* $\sim_A^{\text{strat}}$. Intuitively, for worlds w and w', if $w \sim_A^{\text{obs}} w'$, then agent A's observations are identical for both w and w'. That is, A cannot distinguish worlds w and w' based on A's observations. Similarly, if $w \sim_A^{\text{strat}} w'$, then agent A's strategy is identical for both w and w'. Then, given a particular world (set of strategies and traces) formula $K_A\phi$ holds if ϕ holds in all w' such that $w \sim_A^{\text{obs}} w'$ and formula $E_A\phi$ holds if ϕ holds in all w' such that $w \sim_A^{\text{strat}} w'$.

Interestingly, both knowledge and effect are S5 modal operators, and thus have similar properties. While our logic does not require any particular relationship between these equivalence relations, in practice an agent knows their own strategy. As such, observational relation $\sim_A^{\text{obs}}$ will refine strategy relation $\sim_A^{\text{strat}}$. In such systems, formula $E_A\phi \Rightarrow K_A\phi$ is a tautology for all formulas ϕ.

The logic provides a concise yet expressive way to specify information security guarantees. Using both our new modal operators and traditional epistemic operators, we provide logical characterizations of existing information security guarantees, including noninterference for confidentiality, noninterference for integrity, and robustness (which combines integrity and confidentiality) [3]. A similar notion of robustness can be formulated for integrity, though it is equivalent to integrity in our language model. Moreover, the duality between knowledge and effect suggests that robust confidentiality and integrity should have analogues for knowledge: guarantees for audited information flow, where B can learn secrets or influence facts only if A knows that B does so. Figure 1 lists the logical formulas that correspond to each of the above guarantees.

Guarantee	Formula
Logical confidentiality	$P \vDash E_A\phi \Rightarrow \neg K_B\phi$
Logical integrity	$P \vDash K_A\phi \Rightarrow \neg E_B\phi$
Robust confidentiality	$P \vDash E_A\phi \Rightarrow \neg K_B\phi \vee E_A K_B\phi$
Robust integrity	$P \vDash K_A\phi \Rightarrow \neg E_B\phi \vee E_A E_B\phi$
Audited confidentiality	$P \vDash E_A\phi \Rightarrow \neg K_B\phi \vee K_A K_B\phi$
Audited integrity	$P \vDash K_A\phi \Rightarrow \neg E_B\phi \vee K_A E_B\phi$

Figure 1. A program P satisfies a logical guarantee if the corresponding formula is satisfied for all non-trivial ϕ. In each definition, we consider the security of a trusted/secret agent A and an untrusted/public agent B.

By focusing on the input/output duality of confidentiality and integrity rather than the readers/writers duality, the logic makes the connections between different security guarantees readily apparent. For example, confidentiality and integrity noninterference, which are known to be equivalent, are contrapositives in our logic. Furthermore, robust confidentiality and robust integrity can easily be identified as "integrity of confidentiality" and "integrity of integrity."

We have demonstrated that the first two guarantees, logical confidentiality and logical integrity, are equivalent to language-based noninterference in a simple interactive setting with two agents. We anticipate that the correspondence extends to a multi-agent setting and that similar equivalencies can be demonstrated for the other guarantees in Figure 1.

Balliu et al. [2] use a temporal epistemic logic and a language-based computational model to reason about confidentiality guarantees. Their success in applying symbolic execution and model checking to epistemic logic [4] suggests a promising avenue for enforcing logical guarantees that combine confidentiality and integrity.

References

[1] J. Y. Halpern and K. R. O'Neill, "Secrecy in multiagent systems," *ACM Transactions on Information and System Security (TISSEC)*, vol. 12, no. 1, pp. 5:1–5:47, Oct. 2008.

[2] M. Balliu, M. Dam, and G. Le Guernic, "Epistemic temporal logic for information flow security," in *Proceedings of the ACM SIGPLAN 6th Workshop on Programming Languages and Analysis for Security*, 2011.

[3] S. Zdancewic and A. C. Myers, "Robust declassification," in *Proceedings of the 14th IEEE Workshop on Computer Security Foundations (CSF)*, 2001.

[4] M. Balliu, M. Dam, and G. Le Guernic, "ENCoVer: Symbolic exploration for information flow security," in *Proceedings of the IEEE 25th Computer Security Foundations Symposium (CSF)*, June 2012.