How Useful are Formal Models of Accountability?

Joan Feigenbaum
http://www.cs.yale.edu/homes/jf/

1. Introduction

Computer scientists have traditionally approached information security through *prevention*: Before accessing confidential data, connecting to a private network, or taking any other security-sensitive action, an entity is expected prove that it is authorized to do so. In online life, which is characterized by enormous scale and complexity, the purely preventive approach to security has proven to be insufficient. Several researchers, including Lampson [7] and Weitzner *et al.* [11], have suggested that the preventive approach be augmented by an *accountability* approach: When a security-sensitive action occurs, it should be possible to determine (perhaps after the fact) whether a rule has been violated and, if so, to punish the violators in some fashion.

Feigenbaum *et al.* [3,4] provided support for the accountability approach and developed a formal framework. Their formalism features (1) unified treatment of scenarios in which accountability is enforced automatically and those in which it is enforced by a mediating authority and (2) the ability to handle scenarios in which the parties who are held accountable can remain anonymous as well as those in which they must be identifiable by those to whom they are accountable. Essential technical elements include *event traces* and *utility functions*.

In this talk, we review the framework of [3,4] and ask how applicable it is to real-world scenarios that demand information accountability. Specifically, we ask whether accountability formalism can help us escape the NSA surveillance morass.

2. Related work

There has been a great deal of work on accountability in the social sciences. Broad-ranging social and legal theories of accountability often lack rigor, as noted by Mashaw [8], who states that "[a]ccountability is a protean concept, a placeholder for multiple contemporary anxieties" and Mulgan [9], who notes that "accountability has not yet had time to accumulate a substantial tradition of academic analysis… [T]here has been little agreement, or even common ground of disagreement, over the general nature of accountability or its various mechanisms." An exception is the work of Grant and Keohane [6], who study accountability in the interaction of nation states; they define it as the "right of some actors to hold other actors to a set of standards, to judge whether they have fulfilled their responsibilities in light of these standards, and to impose sanctions if they determine that these responsibilities have not been met." In an early, prescient study of "computerized society," Nissenbaum [10] draws on philosophical analyses of moral blame and responsibility to identify barriers to accountability in software development and deployment.

Within computer science, Lampson adopts a definition that is similar to that of Grant and Keohane: "Accountability is the ability to hold an entity, such as a person

or organization, responsible for its actions." Many computer scientists have developed logics with which to study accountability, *e.g.*, Barth *et al.* [2], who defined a logic for utility and privacy that they applied to models of business practices, and Backes *et al.* [1], who used a protocol logic to prove properties of contract-signing protocols, including accountability properties. See [5] for an extensive overview of the computer-science literature on accountability.

3. Next steps

To demonstrate the value of formal accountability frameworks, we need more examples of their use in the analysis of real-world systems that claim to provide accountability and/or in the design of systems that can be proven to provide accountability. We will focus in this talk on the question of whether this type of analysis and design can be brought to bear on NSA surveillance programs, in which there has been an all-around catastrophic failure of accountability. Relevant questions include: Can intelligence agencies actually be accountable to elected officials, and can the latter actually be accountable to the citizens on the subject of surveillance – *in a formal, rigorously analyzable sense*? Could punishment for violation of our Fourth-Amendment rights be automatic, or must it be mediated by the judicial system? What is the appropriate relationship between accountability and principals' identifiability in the intelligence context?

4. References

[1] M. Backes *et al.*, ``Compositional analysis of contract-signing protocols,'' *Theoretical Computer Science* **367:1-2** (2006), pp. 33–56.

[2] A. Barth *et al.*, "Privacy and utility in business processes," in *Proceedings of the 20th Computer Security Founds. Symp.*, IEEE Computer Society, 2007, pp. 279–294.

[3] J. Feigenbaum *et al.*, "Accountability and Deterrence in Online Life (Extended Abstract)," in *Proceedings of the 3rd Int'l. Conference on Web Science*, ACM, 2011.

[4] J. Feigenbaum, A. D. Jaggard, and R. N. Wright, "Towards a Formal Model of Accountability," in *Proceedings of the 14th New Security Paradigms Workshop*, ACM, 2011, pp. 45-56.

[5] J. Feigenbaum *et al.*, "Systematizing 'Accountability' in Computer Science," YALEU/DCS/TR-1452, Yale University, New Haven CT, February 2012.

[6] R. Grant and R. Keohane, "Accountability and Abuses of Power in World Politics," *American Political Science Review* **99:1** (2005), pp. 29–43.

[7] B. Lampson, "Privacy and Security: Usable Security: How to Get It,'' *Communications of the ACM* **52:11** (2009), pp. 25-27.

[8] J. Mashaw, "Structuring a 'Dense Complexity': Accountability and the Project of Administrative Law," Article 4 in *Issues in Legal Scholarship: The Reformation of American Administrative Law*, 2005.

[9] R. Mulgan, **Holding Power to Account: Accountability in Modern Democracies**, Palgrave MacMillan, Basingstoke, 2003.

[10] H. Nissenbaum, "Accountability in a Computerized Society," *Science and Engineering Ethics* **2:1** (1996), pp. 25–42.

[11] D. J. Weitzner *et al.*, "Information Accountability,'' *Communications of the ACM* **51:6** (2008), pp. 82-87.