Abstract
We analyze prior work in social cybersecurity and present a structuring of this literature based on its pertinence to four S&P-relevant social behaviors: (1) negotiating access to shared resources, (2) shared and social authentication, (3) managing self-presentation, and (4) influencing others' S&P behaviors. We further break down these domains into four scales of social distance—intimate, personal, social, and public— showing that desired access control policies, authentication methods, and privacy and sharing preferences vary across these social scales. We evaluate the current landscape of work through the lens of Ackerman's social-technical gap in social computing systems, finding that while social behaviors clearly impact S&P preferences and needs, existing S&P systems are designed with little understanding of these behaviors. This mismatch forces users to choose between implementing their ideal S&P policies or reducing social friction. To address this mismatch, we outline a research agenda for social cybersecurity work that better aligns S&P goals with social needs, preferences and behaviors.