Applications of ECIR Modeling Work to Cyber Policy Problems

Cindy Williams
Principal Research Scientist
Security Studies Program at MIT
March 10, 2011

One element of core research underway in Explorations in Cyber International Relations (ECIR) at MIT is dynamic modeling, simulation, and analysis. During 2010 and 2011, this research has pushed forward theoretical frontiers in the modeling of resilient mechanisms to explore the interactions of players involved in multi-player auctions and games, under assumptions that are substantially more realistic than those underlying more traditional models. In the coming year, the team hopes in addition to expand on earlier research in the area of fair electronic exchange. This paper explores three examples of future cyber IR policy applications of the work in dynamic modeling, simulation, and analysis.

Negotiations Among Private-Sector Firms on the Sharing of Cyber Risk and Responsibility

One of the most important policy challenges facing the U.S. government is the role that it will play in the protection of privately-owned, critical cyber infrastructure. The Department of Defense identifies the protection of such critical infrastructure as one are in which it is likely to become increasingly involved in the future.

Individual private-sector firms—including banks, investment firms, power plant operators, Internet service providers, and others—have important motivations to improve their own security from cyber threats. Collective action problems can make it hard for them to act individually in ways that will benefit their industry or the nation as a whole, however. Even individually, it may be difficult for them to convince their shareholders that investments in cyber protection are their responsibility or worth the cost. Thus in the future, it may be beneficial for the government to act as the neutral arbiter in negotiations among private-sector players.

Traditional frameworks for understanding how such negotiations work make simplifying assumptions that are inconsistent with the real world. Silvio Micali and his team are examining new frameworks for auctions and negotiations that are resilient, even when the simplifying assumptions do not hold. For example, in their frameworks, those negotiating on behalf of their firms care deeply about the firms' privacy, and do not want to divulge more information than is absolutely necessary to meet their own negotiating aims. They may even be motivated to dissemble, rather than reveal too much about their own operations, vulnerabilities, plans, or costs. The reality of privacy concerns and the potential for false information must be assumed in any government-led negotiation among firms regarding the allocation of risk and responsibility in the cyber arena.

Using the sort of mechanisms being developed by the Micali team, the government could ultimately devise negotiating frameworks in which each firm could keep most of its

information to itself—including information about its goals for the negotiation and the risks about which it is most deeply concerned. Instead of releasing such private information, the firms can act on information that they already hold about each other, and the government can make use of public and government-held information about individual firms' goals and risks. Firms would not be required to divulge private information. They would be rewarded for negotiating in the collective interest. They would be sanctioned within the context of the negotiation for acquiescing to a stipulation, but later renouncing it. The negotiation, which would occur in steps, would allow private information to inform outcomes gradually, without having to be aired publicly among the firms or between the firms and the government. Even without the airing of private information on risks and goals, the negotiation would ultimately settle on outcomes that lowered the collective risk and improved collective progress toward goals.

Similarly, Professor Micali's team relaxes the traditional assumption that the firms will not collude amongst themselves. In fact, the frameworks that the team is developing assume that some of the firms will work together to achieve common aims and lower shared risks, potentially at the expense of firms outside their coalitions. By experimenting with such frameworks in a theoretical context, the team is laying important groundwork that can ultimately help the government—and others setting up the frameworks for step-by-step, round-by-round negotiations—to devise strategies to improve collective cyber security by aggregating information in the face of privacy concerns and subgroup collaboration.

Collaborative Detection of Cyber Attacks

An important challenge in dealing with attacks on the Internet is that individual users are generally aware only of cyber anomalies that affect them directly. If detection information could be aggregated across numerous users, Internet security experts could accelerate the work to identify the source and nature of the attack.

For most users, however, shutting down the computer and starting over is easier than filing a report on the anomalous event. Professor Micali's work lays a theoretical foundation for the development of a collaborative detection regime that would reward Internet users who contribute information that would accelerate the understanding of attacks or other malicious behavior.

A key question in devising such a regime is what level of reward might be needed to induce individuals to be alert to and report anomalies that are not otherwise of interest to them. Professor Micali and his team are exploring the size of such rewards by simulating auctions in which individuals are asked to contribute information about others, under a variety of assumptions related to rationality and the value of privacy.

Certified Transmission of Messages

For many activities of the Department of Defense, it is crucial for the senders of messages to know that their transmissions were received intact. In some arenas, the

traditional method of acknowledgement was a simple as the “Roger that” over voice radio. In other areas, purpose-built systems provide for automated acknowledgment that messages were delivered intact.

As the Department shifts to web-based systems for much of its work, validating the receipt of transmitted orders and messages can be more complicated. Professor Micali’s work on fair electronic exchange with virtual trusted parties lays important theoretical foundations for such validation.

Micali’s research identifies protocols that ensure that a message can be read by the recipient if and only if the sender gets a receipt that acknowledges the message was received. Micali’s protocols are known as “optimistic,” because they induce most senders and receivers to act properly most of the time, and thus require little actual intervention by an electronic post-office to arbitrate disputes about whether a message got through. As a result, in contrast to earlier protocols, Professor Micali’s frameworks require little computing power and are inexpensive to run.

Professor Micali’s fair exchange protocols are also extremely secure, making them especially suitable for Department of Defense applications. Moreover, despite their simplicity, low computational requirements, and cost effectiveness, they are resilient in the face of arbitrarily adversarial behavior.

Since Professor Micali’s pioneering work in the area, others have extended the research to suggest protocols that also ensure the identity of senders and receivers. With such extensions, the research lays the theoretical groundwork for improving the assurance of messaging over DoD and intelligence community Intranets, DoD-to-contractor systems, and wider government Intranets.

Guaranteed receipt of messages can be of obvious benefit in its own right. In addition, the Micali protocols can facilitate the automated development of records of messages sent and received.

Other potential applications of this work include secure bank-to-bank communications within a banking subnet, secure records of intradepartmental or intergovernmental funds transfers, secure records of warnings of cyber events, and secure records of access to intelligence information.