Interference in e-Contracting

Patrick Legros* Andrew F. Newman†

March 13, 2003

Abstract

The recent advent of e-contracting – examples include industry marketplaces and e-procurement systems of US automakers, e-auctions, and e-commerce – provides a natural stimulus for the study of the interaction of security and economic incentives. As security theorists have noted, (1) communication networks are only imperfectly secure and (2) the degree of insecurity depends on economic incentives. We amplify the latter point by

*ECARES, Université Libre de Bruxelles

†Institute for Advanced Study, Princeton; and Department of Economics, University College London

noting that in the e-contracting context, the incentives themselves are endogenous to the degree since they emanate from the contract design itself. At the same time, security considerations clearly place limits on what can be accomplished via e-contracts. In other words *security and incentives are determined simultaneously.*

We incorporate these two insights to develop a theory of mechanism design under insecure communication, which in turn can help to assess the possibilities and limits of e-contracting. The traditional theory, which is meant to determine the allocational possibilities under asymmetric information, makes heavy use of the assumption that information that is transmitted from participants to the mechanism enforcer is perfectly secure: whatever message is sent by a party reaches the center with probability one. In the e-contracting environment, this assumption is untenable because it is typically possible (albeit costly) to interfere in the communication network by "spoofing," or other forms of internet fraud.

We address this issue by developing a formal framework in which agents may invest in the security of their communication channels, and then may "spoof" by sending messages along *all* channels: the more secure another agent's channel, though, the more likely the spoofing attempt will fail. The

implication of this framework is that the incentives to invest in security as well as those to misrepresent other agents' messages (as well of course as one's own preferences) are dependent on the contract stakes. Thus, one must trade off security costs with the gains from high-stakes contracting.

For the general framework we set up, we derive a *revelation principle*: it is enough to consider mechanisms in which each agent truthfully reveals the state of the world along every channel while attaching his signature to each version of his message. Armed with this result, we can examine the feasible and optimal e-contracts, and we do so for a simple environment.

The results of this analysis suggest

- In general there will be limits to what can be accomplished via e-contracts, in particular the sensitivity of product specifications cannot be too high and the parties interests cannot be too far apart, or some efficiency loss must result.

- Efficiency losses assume two distinct forms: distortions (relative to the first-best) of the contracts, and costs of securing the communication network; in general these will have to be traded off to determine the optimal configuration.

- In some cases it will optimal to secure only one agent's channel and let him decide how the product should be produced.

We then turn our attention to the costs of security. The principal may expend the resources for securing the communication network, but if this is large this may get too expensive to be worthwhile, in which case agents may have to contribute as well. This leads to a well-known free rider problem (Varian, 2002). On the other hand, the benefit of interfering is decreasing in the number of participants, as agents who interfere have to be "heard above the din": the chance that enough spoofed messages are received by the center to implement the interferer's preferred outcome becomes vanishingly small as the market becomes large. Thus, there is a well defined trade-off between free-riding on security and the cost of interfering that leads to a determinate extent of the e-contract market.

References

Anderson, R. (2001), "Why Information Security is Hard: An Economic Perspective," http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf .

Varian, H. (2002), "System Reliability and Free Riding," http://www.idei.asso.fr/Commun/Conferences/Internet/OSS2002/Papiers/Varian.pdf