Journal of Computer Security 5 (1997) 111–112
IOS Press

Guest editor's preface

This issue of the Journal of Computer Security contains two papers selected from the 9th IEEE Computer Security Foundations Workshop (CSFW-9), held (for the second year) in idyllic Kenmare, County Kerry, Ireland, June 10–12, 1996.

The workshop meets yearly to bring together researchers to explore fundamental issues in computer security. Papers and panel discussions explore issues in access control, cryptographic protocols, database security, integrity and availability, information flow, and formal methods for security.

Among the papers accepted for CSFW-9, it was my privilege as program chair to invite some particular favorites to be submitted to JCS. These papers were reviewed again under JCS's normal review process, and eventually two papers were accepted for publication in JCS.

These two papers represent distinct poles within the range of workshop topics. Jane Sinclair's paper, "Action systems for security specification" is an exploration and explication of important work in formal methods applied to security. In particular, Sinclair develops an action-system formulation of determinism and security, translating Roscoe's investigation from his process-algebraic formulation in CSP. This scholarly work provides an independent view into formal notions of determinism and security. In addition, as an extended and cogently discussed example, it provides insight into the relationships between process algebras and action systems, and their applications. I hope this work will contribute to bridging the communications and cultural barriers separating distinct communities.

The second paper in this pair is Dahlia Malkhi and Michael Reiter's "A high-throughput secure reliable multicast protocol". This paper extends the notion of acknowledgement chaining from benign faults to cryptographic settings. It presents a technique for amortizing the expense of digital signatures over multiple messages, by allowing an acknowledgement for message M to also acknowledge messages acknowledged in M. The focus of the paper is on (rather elegant) algorithmic and performance issues of a specific protocol.

Hence, Sinclair's paper presents a general formalism for expressing and reasoning about secure systems, and Malkhi and Reiter's paper studies a specific problem instance. The juxtaposition of these papers inevitably raises questions: Could an action-system formulation capture the important properties of the multicast algorithm? Would such a formulation remove ambiguities and provide insight into the interesting algorithmic and performance issues?

This juxtaposition echoes a principal value of small conferences and workshops like CSFW. At large conferences, narrow communities reach critical mass and inevitably sequester themselves in independent sessions and out-of-band discussions. In smaller forums like CSFW, people from different communities can meet, understand each others' points of view and research programs, and identify opportunities

and benefits of bridging. General theories can be tested against individual examples, specific algorithms can be appreciated in broader contexts. The common-place in one community may be revolutionary, when understood and appreciated in another. Cross-pollination of ideas invigorates and enriches the broader community.

In closing, I would like to thank the authors, for submitting their work to first CSFW-9 and then JCS, the program committee, for helping me to identify papers of particular interest, and the anonymous referees, whose comments were particularly prompt and useful.

Michael Merritt
AT&T Labs–Research