Proceedings

SAP 2007

2007 IEEE Symposium on Security and Privacy

20-23 May 2007 Berkeley, California



2007 IEEE Symposium on Security and Privacy

Table of Contents

Message from the Program Chairs	
Conference Organizers	
Program Committee	
External Reviewers	x
Network Security	
Accurate Real-Time Identification of IP Prefix Hijacking	3
DSSS-Based Flow Marking Technique for Invisible Traceback	18
On the Safety and Efficiency of Firewall Policy Deployment	33
Authentication	
The Emperor's New Security Indicators: An Evaluation of Website Authentication and the Effect of Role Playing on Usability Studies	51
Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer	
Cryptanalysis of a Cognitive Authentication Scheme (Extended Abstract)	66
A Systematic Approach to Uncover Security Flaws in GUI Logic Shuo Chen, José Meseguer, Ralf Sasse, Helen J. Wang, and Yi-Min Wang	71
Extended Abstract: Forward-Secure Sequential Aggregate Authentication	86

in Kerberos	92
Alexandra Boldyreva and Virendra Kumar	
Privacy	
Endorsed E-Cash	101
Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems	116
Improving the Robustness of Private Information Retrieval	131
Access Control and Audit	
Beyond Stack Inspection: A Unified Access-Control and Information-Flow Security Model	149
Usable Mandatory Integrity Protection for Operating Systems	164
Enforcing Semantic Integrity on Untrusted Clients in Networked Virtual Environments (Extended Abstract)	179
Information Flow	
Information Flow in the Peer-Reviewing Process (Extended Abstract)	187
A Cryptographic Decentralized Label Model	192
Gradual Release: Unifying Declassification, Encryption and Key Release Policies	207
Fuzzy Multi-level Security: An Experiment on Quantified Risk-Adaptive Access Control Extended Abstract	222



Message from the Program Chairs

The twenty-nine papers within this book were presented at the IEEE Symposium on Security and Privacy, held at the Claremont Resort in Oakland, California on May 20-23, 2007. This year's symposium is the 28th in the series sponsored by the IEEE Computer Society's Technical Committee on Security and Privacy, and in cooperation with the International Association for Cryptologic Research.

While this symposium is already one of the most selective venues in Computer Science, this year's 246 submissions represented one of the most successful calls in the history of the conference. In submitting these works the authors provided many deep, interesting, and novel works in security; so many so that it made the job of selecting just twenty-nine works very difficult.

The program committee worked tirelessly over the 2006 holidays to complete as many as 20 reviews each. On January 19, the program committee met continuously for eleven and a half hours to compare notes and select the program you see herein. We cannot express our gratitude enough to the members of the program committee for their many long hours reviewing papers and sitting through what must have seemed like a lifetime in that meeting.

In addition to the conference organizers, the program committee, and the many authors who submitted papers, we would like to thank the external reviewers, as well as Kevin Butler, Will Enck, Patrick Kellenberger, Michael Steiner, and Patrick Traynor for their endless assistance in coordinating the paper review process and symposium organization. Furthermore, we are honored that Peter G. Neumann agreed to give a keynote talk at the conference. Microsoft Research generously provided a grant supporting student conference travel.

This year's program keeps up the broad and exciting history of the symposium so well known and respected it is simply known as "Oakland" (from the city in which it has always been held). The papers that make up that program represent an engaging mix of systems security, program language security, cryptography, hardware design, and more. In short, there is something here for everyone--we hope you enjoy experiencing it as much as we enjoyed putting it together.

Birgit Pfitzmann Patrick McDaniel
Program Co-chairs