In Computer Security in the 21st Century, eds. D. Lee, S. Shieh, and J. D. Tygar, Springer, 2005

Chapter 1

INTRODUCTION

D. T. Lee
Academia Sinica, Taiwan

S. P. Shieh
National Chiao Tung University, Taiwan

J. D. Tygar
UC Berkeley

Computer security has moved to the forefront of public concern in the new millennium. Hardly a day passes where newspaper headlines do not scream out worries about "phishing" , "identity theft" , "browser exploits" , "computer worms" , "computer viruses" , "online privacy" , and related concerns. The major vendor of computer operating systems has announced that computer security is now its top priority. Governments around the world, including most major governments in North America, Europe, and East Asia continue to worry about "cyber-terrorism" and "cyber-war" as active concerns.

It was in this charged environment that we decided to hold a workshop in December 2003 on emerging technologies for computer security. The workshop was held in Taipei in conjunction with several other conferences (notably Asiacrypt) and featured leading researchers from the Asia-Pacific region and the United States. What followed was three days of exchange of ideas that led to a number of significant developments. This book attempts to share some of the research trends that were reflected in the best papers published at the conference.

The first section deals with the classical issue of cryptographic protocols. How can we build secure systems that need to exchange private data, while guarding against eavesdroppers who listen in on attacks? Dieter Gollmann examines five case studies that show challenges in cryptographic protocol design and argues for a new framework for viewing the problem. Yaping Li, J. D.

Tygar, and Joseph Hellerstein show how private matching can be used to exchange database information while still protecting the privacy of individuals. Jonathan Millen brings formal analysis to bear, showing that current techniques of analyzing protocols still fail to protect against a number of problems. And Tzong-Chen Wu and Yen-Ching Lin argue for a a new key agreement method based on self-certification .

We next turn our attention to networking, and examine the rapidly expanding fields of peer-to-peer networking and ad hoc networking. These clearly introduce a number of new security challenges, and are especially relevant in light of recent studies suggesting the peer-to-peer networking now comprises the majority of networking over the Internet. Nitesh Saxena, Gene Tsudik, and Jeong Hyung Yi present a new system, Bouncer , that provides arguably the most fundamental element of peer-to-peer security: secure admissions control. They also discuss its actual implementation in several real peer-to-peer networks. And Shih-I Huang, Shiuhpyng Shieh, and S. Y. Wu present key distribution systems for an important emerging type of ad hoc network : wireless sensor networks .

A fundamental change in thinking about security has been the change of emphasis from building impenetrable systems to building systems that rapidly respond when attacks commence. Michael Howard, Jon Pincus, and Jeannette M. Wing report on work at Microsoft that proposes a completely new way of thinking about the vulnerability of systems: “relative attack surfaces ”. Pei-Te Chen, Benjamin Tseng, and Chi-Sung Laih give a new may of modeling intrusion detection systems . Fu-Yuan Lee, Shiuhpyng Shieh, Jui-Ting Shieh, and Sheng-Hsuan Wang propose a new type of system for actively responding to distributed denial of service attacks; and Chang-Hsien Tsai, Shih-Hung Liu, Shuen-Wen Huang, Shih-Kun Huang, and Deron Liang discuss their BEAGLE system that allows security faults to be reproduced for debugging purposes.

Finally we turn our attention to perhaps the hottest single topic in the set of emerging security concerns: protecting multimedia content. Yao-Wen Huang and D. T. Lee discuss issues in Web Application Security. Robert H. Deng, Yongdong Wu, and Di Ma discuss their work in securing a new standard for photographic images, JPEG2000 . And Chin-Chen Chang, Tzu-Chuen Lu, and Yi-Long Liu discuss a new method of “watermarking” information in documents: a secret information hiding scheme.

Together, these works present an agenda of important security topics for computer security in the new century.

1. Acknowledgments

Support for this book came from Academia Sinica, National Chiao Tung University, and the University of California, Berkeley. D. T. Lee received ad-

ditional support from National Science Council, and Science and Technology Advisory Group of Executive Yuan, Taiwan. Shiuhpyng Shieh received additional support from National Science Council, Ministry of Education, Taiwan. and Industrial Technology Research Institute. J. D. Tygar received additional support from the US National Science Foundation and the US Postal Service. The opinions in this book are those of the authors and do not necessarily reflect the opinions of the funding sponsors or any government organization.