Chapter 1
Introduction and Overview

Tyler Moore, David Pym, and Christos Ioannidis

1.1 Introduction

The Workshop on the Economics of Information Security (WEIS) is the leading forum for interdisciplinary research and scholarship on information security and privacy, combining ideas, techniques, and expertise from the fields of economics, social science, business, law, policy, and computer science.

In 2009, WEIS was held in London, at UCL, a constituent college of the University of London. The papers included in this volume were all presented at WEIS 2009, having been carefully reviewed by a program committee composed of leading researchers. The presented papers were grouped into nine sessions — identity theft, modeling uncertainty's effects, future directions in the economics of information security, economics of privacy, options, misaligned incentives in systems, cyber-insurance, modeling security dynamics — and we follow the same organization in this volume.

The program of WEIS 2009 included four Keynote Addresses, described below in order of presentation.

- Hal Varian (Google and UC Berkeley): 'Computer Mediated Transactions'. Starting from a discussion of computed-mediated transactions placed in an historical context, Hal Varian gave an insight into his current thinking on topics such as accountability, trust, and enforceability in computer-mediated contracts and transactions. He emphasized the importance of customization and personalization, trade-offs enhanced service and privacy, and the expected impact of cloud computing.

Tyler Moore
Harvard University, USA, e-mail: tmoore@seas.harvard.edu

David Pym
HP Labs, Bristol and University of Bath, UK, e-mail: david.pym@hp.com

Christos Ioannidis
University of Bath, UK, e-mail: c.ioannidis@bath.ac.uk

T. Moore et al. (eds.), *Economics of Information Security and Privacy,*
DOI 10.1007/978-1-4419-6967-5_1,

- Bruce Schneier (BT Counterpane): 'Security and Human Behavior'. Bruce Schneier gave a lively presentation of his view of the rôle of psychology in information security. He emphasized that psychological issues and perspectives impact upon security design, risk perception, attack strategies, and usability. He described how security is both a 'feeling' and a 'reality', and discussed the significance and detection of differences between feeling and reality,
- Martin Sadler (HP Labs, Bristol): 'From Mathematical Modeling to Automation: Turning Research on the Economics of Security into Economic Value'. Martin Sadler gave an illuminating discussion of some key research with HP's Systems Security Lab. He explained why modeling, from a range of economic and mathematical perspectives, is necessary if the management of information security investments is to evolve into a more rigorous engineering science. He emphasized the need for innovative thinking to support effective interactions between researchers and practitioners, be they in academia, industry and commerce, or government.
- Robert Coles (Bank of America): 'Information Security — Art or Science?'. Robert Coles gave an informative and reflective account of practical concerns of a CISO in large organization. He described the strategic issues and budgeting processes, in the contexts of constraints such as Basel II, and standards such as ISO27001 and COBIT. He explained how a range of example incidents might be handled, and, from the perspective of developing a science of information security, the difficulties involved in obtaining useful data.

The program also included a Panel Session, entitled 'A Broader View of Cyber Security Economics'. The panel members were Lance Hoffman (George Washington University, USA), Shari Lawrence Pfleeger (RAND Corporation), David Good (University of Cambridge, UK), Ann Cavoukian (Information and Privacy Commissioner, Province of Ontario, Canada), and Alessandro Acquisti (Carnegie Mellon University, USA).

The discussion in the Panel Session was primarily concerned with privacy, with a focus on the concerns of the citizen in dealing with the state, particularly in the context of the provisions of services using cloud computing.

1.2 The Economics of Information Security and Privacy

Since its inception in 2002, the research appearing at WEIS has steadily evolved. In its formative years, papers at WEIS used economics to explain longstanding challenges to information security: concepts such as incentives, game theory, externalities and information asymmetries were applied to solve information security problems. Models of security investment, patch management and privacy-enhancing technology adoption were presented. The topics discussed at WEIS have continued to evolve. The scientific organizers of WEIS 2009 (Ioannidis, Moore, Pym, and Sasse) encouraged submissions emphasizing two particular aspects:

- First, a whole-systems view of information systems security problems, including human behavior, technological aspects of systems, and the integration of these with the economic environments within which systems exist and operate. Understanding the incentive structures that operate across the spectrum of information security actors is essential, ranging from attackers to those with system-level defensive-responsibilities to the remaining majority of users.
- Second, the use of empirical methods (including data collection, analysis and simulation methods) to support economic and social studies of information security policies and technologies.

One theme common throughout the papers comprising the conference program has been use of methods of risk assessment and control, of the kind found in economics and finance, to model threats to information security as well as the timing and size of investments in information security operations.

Several included papers investigate privacy. The association between the concerns and management of privacy and information security is quite strong. Privacy is a valuable commodity, so individuals and organizations are are increasingly prepared to invest to protect it. Moreover, privacy is a matter of increasing concern for both national- and international-level regulators, as mandatory disclosure of privacy breaches has been adopted in many US states and is under consideration in Europe and beyond.

There is an inherent contradiction between the development of the web, which encourages the sharing of information, and stated preferences for privacy. Social networking sites sites solicit and distribute private information, but must (or, at least, should) take account the implicit requirements for privacy protection assumed by the providers of information.

The relationship of privacy to security is also important. For example, the users of social networking sites choose to promote the availability of the information that they own, but they also expect that the operators of the site will maintain its integrity and protect the confidentiality of their information by restricting access to legitimate members of the site. When citizens disclose private information to governments, by contrast, a different set of incentives, preferences, and trade-offs apply.

Informed by the perspective sketched above, we next introduce the papers included in this volume.

1.3 Overview of the Book's Contributions

The subsequent chapters in the book are broken down in seven sections, as indicated in Table 1.1.

The first two chapters consider the key role uncertainty plays when making security decisions. Uncertainty can take several forms — whether a firm will be targeted by attack, whether an attack will be successful or even detected, and so on. Firms are presented with a choice of spending money on security defenses and taking a small but certain loss, or skipping investment into protection but face an uncertain

Table 1.1 Chapters within each major section.

Modeling Uncertainty's Effects
The Price of Uncertainty in Security Games
Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty & the Underground Economy
Misaligned Incentives in Computing Systems
Security Economics and Critical National Infrastructure
Internet Multi-Homing Problems: Explanations from Economics
Threat Assessment
Modeling the Security Ecosystem — The Dynamics of (In)Security
Modeling the Economic Incentives of DDoS attacks: Femtocell Case Study
Privacy
The Privacy Jungle: On the Market for Data Protection in Social Networks
The Policy Maker's Anguish: Regulating Personal Data Behavior
Applications of Options Theory
Valuating Privacy with Option Pricing Theory
Optimal Timing of Information Security Investment: A Real Options Approach
Cyber Insurance
Competitive Cyber-Insurance and Internet Security
Potential Rating Indicators for Cyberinsurance: An Exploratory Qualitative Study
Risk Analysis
The Risk of Risk Analysis-And its relation to the Economics of Insider Threats
Competition, Speculative Risks and IT Security Outsourcing

but potentially higher loss. In Chapter 2, Grossklags, Johnson and Christin use game theory to compute the 'price of uncertainty' under different scenarios: the difference between the worst expected payoff under incomplete information and the payoff with complete information. In Chapter 3, Herley and Florêncio consider uncertainty from the perspective of miscreants participating on the underground economy. They note that stolen banking credentials are sold on the open market for a pennies on the dollar, and argue that such a low market-clearing price reflects a severe lemons market. Would-be fraudsters cannot tell whether the stolen credentials they are buying are real or fake. Chapter 3 also points to a more fundamental uncertainty, namely, the size and scope of the underground economy itself.

The next two chapters point out the existence of misaligned incentives for two computing applications. In Chapter 4, Anderson and Fuloria examine economic factors affecting critical national infrastructures, such as the IT systems that control power plants and chemical refineries. They argue that the systemic weaknesses present in these infrastructures can be explained by economic factors rather than technical ones. In Chapter 5, Richard Clayton examines the networking protocol SHIM6. He argues convincingly that SHIM6, while perfectly suitable from a technical perspective, is likely to be a commercial failure because the designers have failed to consider that would-be adopters have no short-term incentives to do so.

In Chapter 6, Frei, Schatzmann, Plattner, and Trammell continue the trend of arguing that poor incentives, flawed design and neglected implementation explain why security fails. They use empirical analysis to inform a model of organizational

response to vulnerability disclosure. The authors develop a methodology of how the 'security ecosystem' can be analyzed quantitatively using statistical analysis.Segura and Lahuerta develop and estimate an economic model of extortion by distributed denial-of-service (DDoS) attacks in Chapter 7. They put forward a model of the behavior of attackers as agents responding to economic incentives. Collecting relevant data on advertised prices in underground fora, the authors compute econometric estimates of the model parameters to understand the risk posed by DDoS attacks and develop appropriate responses. On the basis of their econometric evidence, the authors undertake a number of scenario simulations to explore the solution space for mitigating extortion attacks in the context of a wireless telecommunications service.Chapters 8 and 9 address the issue of privacy preservation from the points of view of policy makers and individual agents. A great deal of private information is lodged under the stewardship of social networks. In Chapter 8, Bonneau and Preibusch, undertake a comprehensive study of practices and policies with respect to the protection of privacy. They evaluate 45 social networking sites operating in a vigorously competitive environment as they seek additional users for their services. They find evidence that some of these sites are making a sustained effort to protect the privacy of their users, albeit with substantial diversity in the policies adopted. Privacy protection does not constitute a strong selling point and the relevant policies are often not conveyed clearly to the users. They conclude by suggesting a model of a privacy communication game, where the sites reveal in detail their privacy protection protocols to avoid criticism while hiding the privacy control interface to attract users.

In Chapter 9, Compañó and Lusoli conduct a cross-country on-line survey to identify differences in attitudes towards electronic identity across Europe. They identify a number of behavioral paradoxes which present governments with policy dilemmas. Most important is what the authors coin *the privacy paradox*, whereby young people happily provide a range of personal information despite awareness to the privacy risks. In protecting their privacy the participants reveal that they are asking for 'technology' that provides them with the means to protect their own identity data. At the same time, however, they are not confident in their expertise and organizational skills to keep their personal data safe and safeguard their privacy. Policy action faces systemic constraints as there is an apparent internal contradiction between the promotion and protection of privacy as public good and private sector interests. Cultural differences across EU Member States add to the difficulties of sound policy formation.

Chapter 10 proposes an innovative way to assess the long-term value of maintaining the privacy of personal data in the face of uncertainty. Berthold and Böhme apply a methodological tool from finance, the binomial option pricing model, to the valuation of personal information. By varying uncertainty surrounding future information disclosures as well as the agents' behavioral characteristics, the authors develop scenarios for the efficient pricing of 'privacy options'. In contrast to standard financial theory, the authors postulate stationary stochastic processes regarding the change in the value of information. The key idea of this work is that disclosing a single attribute value can be interpreted as writing an option for exploiting the at-

tribute in the future. Here, 'to exploit' refers to the act of using the attribute to draw inference on the data subject's identity or preference, and to base decisions on this information that may affect the data subject.

'Project valuation using real options' is a modern capital-budgeting technique that accounts for the explicit uncertainty inherent in all investment projects. Unlike traditional methods, where project managers are 'passive' once the investment decisions have been made, real options assume that managers maintain an active role in decisions regarding both the timing and size of the investment. In Chapter 11, Tatsumi and Goto apply the real options approach to firms' investment activity in information security technology and then provide a dynamic analysis of information security investment. They conclude that the statistical characteristics of threats to information security are important determinants of both the size and the timing of investment expenditure. Improvements in efficiency of vulnerability reduction technology encourages firms to undertake investment in information security earlier rather than later.

The question of how competitive cyber-insurers affect network security and welfare of the networked society is addressed by Shetty, Schwartz, Felegyhazi, and Walrand in Chapter 12. The existence of an efficient equilibrium insurance contract depends upon two different assumptions regarding the ability of the cyber-insurer to monitor the user's security. If insurers are unable to monitor the security of their clients, then under the existence of asymmetric information, it is unlikely that efficient cover contracts can be written. When user security is enforceable and costless, full-cover contracts are available. From numerical simulations, they conclude that a competitive cyber-insurance market improves both the welfare of users and network security.

Continuing the cyber-insurance theme in Chapter 13, Innerhofer-Oberperfler and Breu explore in a qualitative study the suitability of different rating indicators. The paper summarizes 36 semi-structured interviews with experts from Germany, Austria and Switzerland. The study's goal is to establish rating indicators for cyber-insurance, rank their importance, and explore the relationships between them. An initial list of 198 indicators is reduced to 94, which have subsequently been ranked in terms of importance by 29 experts. The results of this undertaking can aid cyber-insurers seeking to refine their premium-rating models with additional variables.

In Chapter 14, Probst and Hunker answer the question why organizations, given the significance of insider threats, choose policies that allow insider threats to proliferate. They examine how an organization's risk analysis and its assessment of trust in an insider develop over time. Insiders acquire more knowledge and vital information about the organization over time and thereby pose increasing risk. Faced with such a dynamic process, organizations have two choices for mitigation. The organization could choose to enhance the trust placed in insiders as they pose a bigger risk; alternatively, the organization must enforce an ever-increasing number of policies to regulate and monitor the insider's actions. The authors argue that since insiders with malicious intentions can alter their behavior to circumvent control systems, prevention becomes prohibitively expensive.

In the final chapter, Cezar, Cavusoglu and Raghunathan establish conditions for the efficient outsourcing of IT security. They show that the suitability of IT security outsourcing depends crucially upon the firm's perception of competitive externalities. When competitive externalities are ignored, firms choose to outsource provided the Managed Security Service Provider (MSSP) offers a quality (or a cost) advantage over in-house operations. However, when firms take externalities into account the quality improvement is no longer required for outsourcing to make sense. Even if the likelihood of a breach is higher under the MSSP, the expected benefit from the competitive demand externality may offset the loss from the higher likelihood of breaches.