5th International Conference on Trust, Privacy, and Security in Digital Business
(TrustBus'08)

On the Design Dilemma in Dining Cryptographer Networks

Jens O. Oberender[1] * and Hermann de Meer[1,2]

[1] Chair of Computer Networks and Computer Communications,
Faculty of Informatics and Mathematics
[2] Institute of IT-Security and Security Law,
University of Passau, Germany
oberender|demeer@uni-passau.de

Abstract. In a Dining Cryptographers network, the anonymity level raises with the number of participating users. This paper studies strategic behavior based on game theory. Strategic user behavior can cause sudden changes to the number of system participants and, in consequence, degrade anonymity. This is caused by system parameters that influence strategic behavior. Additionally, conflicting goals of participants result in dilemma games. Properties of message coding, e.g. collision robustness and disrupter identification, change the game outcome by preventing dilemmas and, therefore, enhance anonymity. Properties of anonymity metrics are proposed that allow for strategic user behavior.

1 Introduction

Anonymity systems protect the identities of communicating subjects disclosed. Beyond this coarse characterization, anonymity is seen as continuum – often related to a specified attacker model, e.g. an observer of network communications. Another definition of anonymity of a subject says, that the attacker cannot 'sufficiently' identify the subject within a set of subjects, the anonymity set [1]. The anonymity measure can be quantified as probability that the attacker correctly identifies a subject.

Because anonymity techniques are costly, users consider cost and benefit of anonymous communication, before they participate. In consequence, the design of anonymity systems must consider economically acting users. The benefit of participation in an anonymity system scales with the level of anonymity received. This paper identifies properties of anonymity measures necessary for strategic acting. Another open question is adjustment of design parameters for operating an anonymity system. The designer faces the dilemma, whether to maximize anonymity against powerful adversaries or minimize the cost of operation. The cost of countermeasures has an effect on the number of participating subjects, i.e. size of the anonymity set, which influences the level of anonymity.

* This work has been partly supported by the EuroFGI and EuroNF Networks of Excellence (IST-028022, 216366).

Game theory is a branch of applied mathematics. It attempts mathematical modeling of strategic behavior. The objective of an iterative game is to maximize the average payoff per round. Nash Equilibria define game outcomes, in which none of the player can further increase its payoff. They are computed deterministically. Many participants in anonymity systems act strategically to enhance anonymity. In a DC-net, coding schemes enable identification of irrational adversaries (cf. Section 5). Therefore behavior of DC-net participants can be modeled using utility functions. These games can be studied using game theory. In practice, user preferences and aims of the adversary are unknown. Games with incomplete knowledge respect unknown strategies of other players.

This study evaluates behavior in a Dining Cryptographers network using a game theoretic model. The model considers properties of the coding schemes such as collision robustness and disrupter identification, and the anonymity preference of a user. The designer can apply an efficient and a collision robust design, the user participate or leave, and the adversary can disrupt or conform. We evaluate the Nash Equilibria and identify design parameters, where the level of anonymity is sufficiently high, users participate because of reasonable cost, and an adversary has low incentive to disrupt.

The paper is structured as follows: Section 2 outlines related work. Section 3 describes the system model attackers, and anonymity estimation. Section 4 discusses system parameters, game theory concepts and the modeling paradigm. Section 5 evaluates adversary, designer, and user strategies in DC-nets. Then we analyze anonymity metrics according to their underlying assumptions in Section 6. Finally, the paper is concluded in Section 7.

2 Related Work

The effectiveness of anonymity techniques is measures using anonymity metrics. Such measures refer to the probability that a powerful adversary becomes able to identify subjects of an anonymous communication. The measures make strong assumptions on available data, e.g. the a posteriori knowledge of an adversary [2] and involve the number of (honest and dishonest) users. Díaz, et. al examine probabilistic attacks, where an attacker weakens anonymity by concluding statements like 'with probability p, subject s is the sender of the message'. Their measure aggregates probabilistic information using information entropy [3]. Tóth, Hornák and Vajda stress the diverse anonymity levels of system participants. They define a metric of local anonymity, which refers to messages of a specific user. Therefore their prediction is more fine-grained than the anonymity computed in average for the whole system. Their paper shows the relevance of user-specific anonymity measures [4].

Other research studies the economic dimension of anonymity systems. Fulfilling security goals often relies on correct behavior of multiple parties, e.g. users. Dingledine and Mathewson review the influence of participants' habits on the anonymity received [5]. Acquisti, Dingledine, and Syverson explore privacy preferences in an anonymity system using game theory. E.g. volunteering as a

mix node enhances the level of anonymity. If operating a mix is too costly, the anonymity system can be used as proxy. Cost has an impact on the participant behavior and, in consequence, on the size of the anonymity set. The duality between secure anonymity and communication reliability is introduced [6]. While they consider the impact of strategic users to the anonymity system, it is left open how design parameters facilitate sufficient anonymity to the users.

3 Modeling Dining Cryptographer Networks

The *Dining Cryptographers* (DC) protocol provides anonymity of the sender [7]. In each communication round, each participant either sends a message or contributes an empty frame. The coding scheme superimposes the message content with additional data. For this reason, the DC protocol establishes pairwise one-time pads (OTP). Each receiver of the broadcast decodes the superimposed message, that is assembled from all messages sent in this communication round. At that stage, the message sender is indistinguishable among the DC-net participants.

Attacker Models. Anonymity is threatened by several kinds of attack rendered against the DC protocol. We assume that any attacker prevents being identified as adversary, e.g. conceals its activity. A *global passive adversary* (GPA) is able to observe all communications. If all other participants of the anonymity set collude ($n-1$ attack), sender anonymity is broken. If an anonymous sender is linkable in multiple observations, the *intersection attack* narrows down the set of possible candidates. For this reason, the anonymity set must not be available to system participants.

Strategic User Behavior. In our experiments, a user decides strategically whether to join the DC-net or not. The cost of participation is additional traffic, both for contributing cover traffic broadcasts and for subscribing to the broadcast. If bandwidth usage had not been subject to economical considerations, a multitude of cover traffic sources would establish network anonymity on the Internet. Any user of an anonymity system considers the following questions: How much traffic will be received during participation in the DC-net? What level of sender anonymity will the user gain?

An adversary can also abuse the economical considerations of a user. The *disrupter attack* raises the cost of participation. If the message coding is not robust to collisions and a slot carries multiple messages at a time, message decoding fails. The disrupter attack provokes random collisions. This increases delay and requires retransmissions, which increases bandwidth consumption. Thus, an adversary can control cost of participation and cause users to leave the DC-net. This degrades sender anonymity of the remaining participants as the anonymity set size decreases.

Estimate Anonymity. The GPA is able to compute the anonymity set using the transitive closure using the relation of observed traffic. Anonymity metrics measure the knowledge of an adversary, e.g. the probability distribution within the candidate set of subjects. Without further knowledge, a uniform probability

distribution is given: $p_i = (|\text{anonymity set}|)^{-1}$. This probability estimates the level of sender anonymity. Because of the lack of identification, distributed estimation of the anonymity set cannot be protected against malicious tampering. In general, users are not able to determine the anonymity currently received (cf. Section 6). The DC broadcast messages allow for anonymity estimation, because all participants contribute cover traffic. DC-nets hereby fulfill the necessary requirement for strategic behavior of users.

4 Strategic DC-net Design

The anonymity of a Dining Cryptographers network results from the behavior of three players: designer, user, and adversary. An earlier study showed that varying cost together with individual anonymity preferences has an effect on the participant number [6] and, in consequence, also has an impact on the anonymity level. The players in the design game of an anonymity system have individual goals and therefore differing utility functions.

Design Dilemma. In our model, users aim for anonymity at a reasonable cost. According to the individual threshold, a user leaves the system if the cost of participation exceeds its benefit of sender anonymity. The designer wants to establish a high anonymity level for the system users. Sender anonymity is enhanced if the system attracts many users, i.e. has low cost of participation. Therefore, we expect that facilitating algorithms with low bandwidth usage result in a raise of participants. On the other hand, such coding schemes are vulnerable to attacks. Our study evaluates possible strategies, since no trivial solution exists. The objective of the adversary is to hinder anonymous communications or raise the cost of participation. An malicious participant can disrupt communications by generating collisions.

How should the designer set system parameters? The strategic behavior of all participants aims to enhance utility. *Nash equilibria* (NE) defines a set of game outcomes, where none of the players is able to improve its utility by changing its own strategy. Strategic behavior always results in a NE, if one exists. The utility functions correspond to anonymity set size (designer), sender anonymity at reasonable cost (user), and disrupting communications without being identified (adversary). Unfortunately, these optimization goals conflict with each other. In games containing such a *dilemma*, strategic behavior of all participants leads to utility loss. This is similar to the prisoner's dilemma, where lack of cooperation degrades utility of all participants. Earlier studies characterized utility functions that cause dilemmas in non-cooperative games [8]. The coding scheme used in the DC-net and anonymity preference of the user influence the utility functions and, possibly, neutralize the dilemma. Our study computes NE of *non-cooperative* games, where players know the utility functions of each other and consider strategies for maximum utility. Access to the utility functions is commonly assumed in game theoretic studies of cooperative systems, e.g. [9]. The analysis concludes parameter settings that avoid dilemma games. Then we relate the results to *sequential games*, where incomplete knowledge requires players to

act defensively. Sequential games provide better models of anonymity systems because users and adversaries have perfect information about the design parameters.

Game theoretic modeling. Game theory studies the results of game strategies. Each player i chooses a strategy $s_i \in \Sigma_i$ from its strategy set, e.g. a user can either participate in the DC protocol or leave. A game with three players is defined as a tuple $G = ((\Sigma_i)_{i=1..3}, E, (u_i)_{i=1..3})$ with the strategy set Σ_i, the outcome set $E = \Sigma_1 \times \Sigma_2 \times \Sigma_3$, and the utility function $u_i := E \to \mathbb{R}$. Interaction between players influences the outcome $e \in E$ of a game. If NE are not unique, as in our study, the choice of strategy has no effect to the payoff.

In an iterated game, strategic behavior considers information about recent behavior of other players. The objective in iterated games is to maximize the average utility. This behavior is different to one-shot games, where strategies maximizes utility of a single round. The corresponding notion is the *mixed strategy* $x = (x_1, \ldots, x_n)$ with $\sum_{i=1..n} x_i = 1$ and n pure strategies. It executes each pure strategy s_i with a given probability $x_i \geq 0$.

Anonymity Design Parameters. The strategy sets Σ_i of designer, user, and adversary are listed in Table 1. A major design question is the choice of the algorithm, i.e. how messages are encoded for broadcast. The first parameter, α, defines collision robustness. Parameter β controls the ability to identify a disrupter. The third parameter, γ, defines the user anonymity preference. Chaum's XOR-based coding [7] consumes little bandwidth, but is highly vulnerable to collisions. For $\alpha = 0$ our simulation uses XOR coding. Between honest participants collisions can be avoided using slot reservation. After a collision, senders wait for a random time before they retry. Disrupter attacks can maliciously hinder any communication. Novel coding schemes have come up. Collisions in DC broadcasts can be recognized using bilinear maps [10]. The DC protocol becomes non-interactive with this coding ($\alpha = 1, \beta = 0$), as multiple senders can concurrently transmit messages. An alternative coding identifies disrupters, who repeatedly interfere with ongoing communications [11]. As an adversary hides from identification, the design parameters $\alpha = 1, \beta = 1$ counter disruptions from strategic adversaries. Another parameter models the anonymity preference of a

Player	Property	Description
Designer	Objective	Provide high level of anonymity
	Σ_1	Efficient ($s_1 = 0$) vs. adversary-robust ($s_1 = 1$)
	α	Preference for defense rather than attractiveness to users
	β	Capability to identify malicious disrupters
User	Objective	Communicate anonymously with low cost
	Σ_2	Participate ($s_2 = 0$) vs. leave ($s_2 = 1$)
	γ	Demand for sender anonymity
Adversary	Objective	Disrupt DC communications, but remain unidentified
	Σ_3	Conforming ($s_3 = 0$) vs. disrupt ($s_3 = 1$)

Table 1. Overview of players, their strategy sets and system parameters

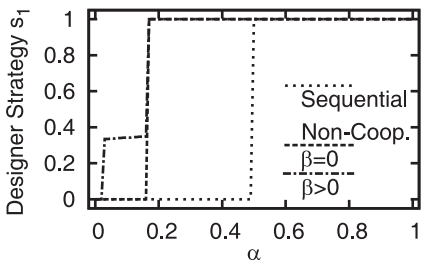


Fig. 1. Comparison of designer strategies by collision robustness with $\gamma = 1$

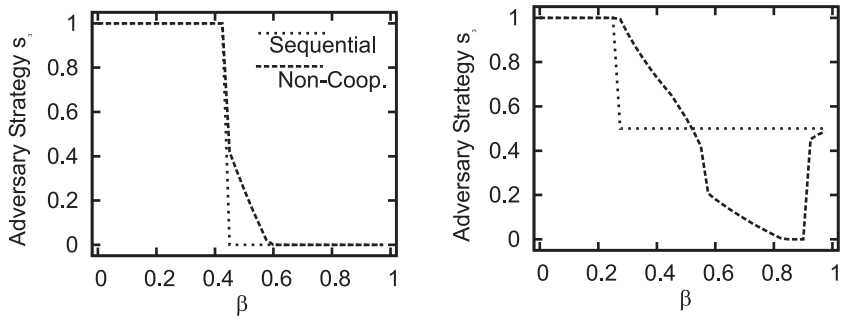
specific user, i.e. what effort is considered reasonable to sender anonymity (large effort $\gamma = 1$, no effort $\gamma = 0$).

5 Evaluation

For the study of anonymity design parameters, utility functions are derived from the prisoner's dilemma ($T = 5, R = 3, P = 1, S = 0$) and involve the design parameters described in Table 1. Strategic players in non-cooperative games maximize their own utility, considering the behavior of other players. Our analysis is based on Nash Equilibria (NE) of the corresponding game, which define mixed strategies with maximum utility for each player. In sequential games, a defensive strategy minimizes utility loss (max-min algorithm). The system should be parameterized using α, β so that many users contribute to sender anonymity and strategically behaving adversaries do not disrupt anonymous communications.

Design Parameters. The first design choice is between cost-efficient anonymity or robustness against collisions. The study evaluates maximum utility strategies under a disrupter attack $s_3 = 1$. The designer's strategy s_1 resulting from the Nash Equilibria in non-cooperative games with ($\beta > 0$) and without ($\beta = 0$) disrupter identification and the sequential game strategy are shown in Figure 1.

The major trend is that sender anonymity benefits from attack countermeasures, unless there is a strong preference for low-bandwidth utilization. This preference together with disrupter identification is best answered by a $1 : 2$ mixture of efficient coded rounds and collision-robust rounds. A mixed strategy NE is a typical result in dilemma games. When comparing a non-cooperative and a sequential game, the designer's strategy deviates for $0.2 \leq \alpha < 0.5$. This originates in the lack of feedback from user and adversary. In the sequential game, the designer benefits from low preference $0 < \alpha < 0.15$, which results in good anonymity, as many users join. In a non-cooperative game, the designer considers strategies of the other players. An adversary can impact communication efficiency by disrupting and wasting bandwidth. Therefore, in the non-cooperative game, an attacker-robust coding scheme is more beneficial.



(a) $\alpha = \gamma = 0.5$ (b) $\alpha = 1, \gamma = 0$

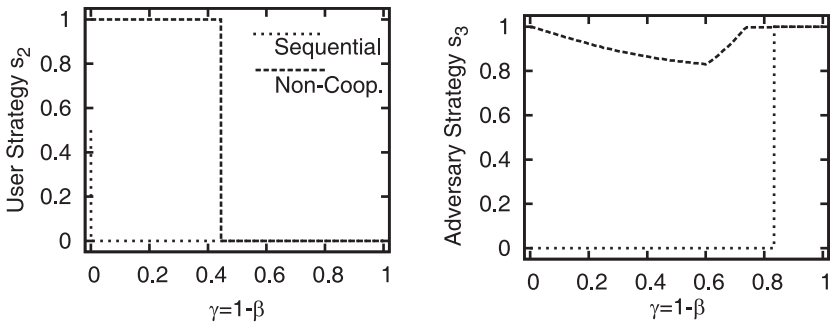
Fig. 2. Impact of a disrupter-identifying algorithm β.

The capability of disrupter identification indeed influences the adversary's strategy. The best adversary's strategy corresponding to disrupter identification β is shown in Figure 2(a). Here, the designer balances robustness and efficiency $\alpha = 0.5$. If the adversary does not fear identification $\beta < 0.42$, it will disrupt communications. The strategy of the sequential game differs from the non-cooperative game NE for $0.42 < \beta < 0.6$. The adversary will omit disruption when it considers the designer's strategy, due to the enabled disrupter identification.

Does a collision-robust coding scheme make disrupter identification obsolete? Figure 2(b) shows the NE with varied disrupter identification. The adversary's strategy in a non-cooperative game adapts to a broad set of mixed strategies, 50% attacks for both $\beta = 0.5$ and $\beta = 1.0$ and no attacks for $\beta = 0.825$. This results from negotiation with the low-anonymity demand user strategies $\gamma = 0$. The underlying dilemma becomes also visible in the sequential game. The adversary achieves best utility by alternating disrupting and conforming behavior for $\beta > 0.3$. These results indicate that disrupter identification is necessary, as it influences the adversary to throttle its attack rate. The adversary exploits the countermeasure, which requires multiple collisions for correct disrupter identification.

Summarizing, control of the parameters α, β limits malicious disruptions. The overall design recommendations for equivalent utility functions are $\alpha > 0.5$ and $0.825 < \beta < 0.9$. Using this parameter set the designer can cut down the additional workload for the robust coding scheme. The mixed strategy of the adversary indicates the probability to randomly interfere with communications. The disrupter's defense against being identified is to attack from multiple DC-net participants. In this case, a low setting of β may fail to maintain communications.

Our results show how to resolve the game-theoretic dilemma. If the anonymity system is designed accordingly, strategic behavior increases utility (at least for designer and user). This facilitates that strategic behavior enhances a



(a) User Strategy (b) Adversary Strategy

Fig. 3. Impact of user anonymity demand γ and disrupter identification $1-\beta$ ($\alpha \geq 0.5$)

Category	Trust	Prediction	Example
Assured Anonymity	N	N	mix queue state with cover traffic
Policy-enforced Anonymity	Y	N	number-triggered pool mix
Reported Anonymity	N	Y	state externally aggregated
Perceived Anonymity	Y	Y	broadcast networks

Table 2. Categories of anonymity measures

player's payoff. Then, strategic behaving participants have positive impact on the anonymity.

User Strategies for Anonymity. How do users behave if the design parameter mismatches their anonymity preference? This is the case for low-anonymity users with cost intensive disrupter identification $\beta = 0, \gamma = 1$ and users with high anonymity preference without disrupter identification $\beta = 1, \gamma = 0$. For the next experiment we choose $\beta := 1 - \gamma$ and examine resulting NE in Figure 3. User and adversary form a dilemma in the non-cooperative game for $\gamma = 0, \beta = 1$, where the user leaves the system and the adversary disrupts. The user participates for $\gamma > 0.45, \beta < 0.55$, but the adversary disrupts with high probability. In the sequential game, the user participates if a robust coding is used. Figure 3(a) displays the adversaries strategy in non-cooperative and sequential games. The adversary clearly benefits from negotiation of strategies, while pre-established strategies hinder attacks for $\gamma = 1 - \beta < 0.85$. This is an encouraging result, as the designer is able to mitigate attacks by choosing system parameters accordingly. Furthermore, the sequential game indicates that users benefit from participation, unless they do not value sender anonymity at all – $\gamma > 0$.

6 Requirements for Strategic User Behavior

A strategic user decision considers cost and benefit of participating in the anonymity system. While the cost is determined through design parameters, the

anonymity level results from participation of other users. We propose four categories of anonymity measures shown in Table 2.

Perceived anonymity provides a prediction based on own experience in the past, i.e. the user has acquired knowledge directly. Externally provided information is not involved. DC-net participants receive all broadcasts and can compute the anonymity set of that round. Sender anonymity only fails if an adversary pools enough keys to reveal a DC message. Because a sender shares OTP keys with all other participants, changes to the anonymity set are actively distributed; otherwise the broadcasts cannot be decoded.

A superior choice is a *policy-enforced* anonymity mechanism, where the suggested level of anonymity is reached or messages will not be delivered. This requires trust into a third party, who has to enforce the policy. E.g. amount-triggered pool mixes queue incoming messages until a certain message count is reached. This weakens the adversary's knowledge if the mix is under observation.

Reported anonymity assumes trust into the reported anonymity set, which refers to a past system state. The anonymity prediction only holds if the system does not change many before the resulting strategy is executed. Reported anonymity is applied in large anonymity systems, where the anonymity set is expected to change only marginally over time. An example is the AN.ON system, which reports the number of participating users [12].

From an analytical viewpoint, only a non-predictive level of anonymity, whose evaluation does not rely on trusted third parties enables strategic reasoning. *Assured* anonymity determines the anonymity level of a message to be sent in the future. The evaluation must be independent from external influences. If cover traffic is contributed from multiple, non-colluding participants, a pool mix is able to determine assured anonymity. In peer-to-peer anonymity systems, each node acts as mixer [13]. The number of queue messages defines the lower bound of the anonymity set.

Concluding, the actual user behavior depends on design parameters, but also the user's ability to determine the anonymity level that the system provides. If an anonymity system participant cannot determine the anonymity level, it may prefer to leave the system. The ability to determine the anonymity level of future messages is suggested as future work.

7 Conclusions

If a user considers sender anonymity as a large advantage, he will accept the cost of participation. Dining Cryptographer networks rely on the willingness of many users in order to establish a good level of sender anonymity. Our work considers design parameters and analyzes the impact of participant strategies on the anonymity level. Parameters in the design of DC-nets contain dilemmas, where strategic behavior does not enhance anonymity. Our approach tunes system parameters to resolve strategic dilemmas and enhance anonymity. We classify measures that predict and guarantee a certain anonymity level and explicitly model trust relationships. Strategic behavior of participants must take these criteria

into account in order to determine utility. In non-cooperative games, strategic players predict the behavior of other participants to evaluate their maximum benefit. In sequential games, the knowledge about adversaries is incomplete and their strategy cannot be predicted. Our simulation compares strategies of non-cooperative games with strategies in sequential games. We identify system parameters, which allow for dilemma-free games in DC-nets and, therefore, allow that strategic behavior enhances anonymity.

References

[1] Pfitzmann, A., Hansen, M.: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management - a consolidated proposal for terminology. (2008) http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.

[2] Serjantov, A., Newman, R.E.: On the anonymity of timed pool mixes. In: SEC – Workshop on Privacy and Anonymity Issues. Volume 250, Kluwer (2003) 427–434

[3] Díaz, C., Seys, S., Claessens, J., Preneel, B.: Towards measuring anonymity. In: Privacy Enhancing Technologies. Volume 2482 of LNCS, Springer (2002) 54–68

[4] Tóth, G., Hornák, Z., Vajda, F.: Measuring Anonymity Revisited. In Nordic Workshop on Secure IT Systems (2004) 85–90

[5] Dingledine, R., Mathewson, N.: Anonymity loves company: Usability and the network effect. In: Workshop on the Economics of Information Security. (2006)

[6] Acquisti, A., Dingledine, R., Syverson, P.: On the economics of anonymity. In Financial Cryptography. Number 2742 in LNCS, Springer (2003)

[7] Chaum, D.: The dining cryptographers problem: unconditional sender and recipient untraceability. In: Journal of Cryptology. Volume 1., Springer (1988) 65–75

[8] Delahaye, J.P., Mathieu, P.: The iterated lift dilemma or how to establish metacooperation with your opponent. Chaos & Society (1996)

[9] Mahajan, R., Rodrig, M., Wetherall, D., Zahorjan, J.: Experiences applying game theory to system design. In: ACM SIGCOMM workshop on Practice and theory of incentives in networked systems (PINS), ACM (2004) 183–190

[10] Golle, P., Juels, A.: Dining cryptographers revisited. In: EUROCRYPT. Volume 3027 of LNCS, Springer (2004) 456–473

[11] Bos, J.N., den Boer, B.: Detection of Disrupters in the DC Protocol. In: Workshop on the theory and application of cryptographic techniques on Advances in cryptology. (1989) 320–327

[12] Berthold, O., Federrath, H., Köpsell, S.: Web MIXes: A system for anonymous and unobservable Internet access. In: Designing Privacy Enhancing Technologies. Volume 2009 of LNCS., Springer (2000) 115–129

[13] Rennhard, M., Plattner, B.: Introducing MorphMix: peer-to-peer based anonymous internet usage with collusion detection. In: ACM workshop on Privacy in the Electronic Society (WPES) (2002) 91–102