http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 4 (4): 342-347, 2005
ISSN 1812-5638

The Unknown Workforce: Supporting Anonymous Employees

Bezalel Gavish and [1]John Gerdes, Jr.
Eugene J. and Ruth F. Constantin Distinguished Chair in Business, Edwin L. Cox School of Business,
Southern Methodist University, Dallas, P.O. Box 750333, TX 75275-0333
[1]The A. Gary Anderson Graduate School of Management,
University of California, Riverside, California, 92521

Abstract: Certain positions may be difficult to fill because they impose indirect costs that prospective employees are unwilling to bear. These costs could be due to some stigma associated with the position or employer (i.e., taking the job of an accountant in a strip club). Accepting a controversial position, or one opposed by some radical group may place the individual, his/her family and property at risk. It could be that taking the job may jeopardize future hiring and earning potential. The support of anonymity could potentially increase the applicant pool, potentially reducing costs and improving the process outcomes. Unfortunately, traditional contractual mechanisms do not support anonymity. We developed mechanisms that mirror the traditional contractual mechanisms yet allow individuals to remain anonymous. Using blind certificates we show it is possible to verify applicant's credentials. Additionally, this approach avoids the creation of an alternate, pseudo-identifier that can link individuals across multiple data sources, as is the case with the social security number today. Using fair blind signatures we also address the case where it may be necessary to revoke credentials. The governmental income reporting requirements must be addressed if anonymous employment is to be possible. Three alternatives are presented, each with a different degree of anonymity. If the government's goal is to ensure that the appropriate taxes are paid, this could be satisfied by paying the maximum applicable tax on the amount earned. The employer would withhold income taxes at the maximum marginal tax rate before dispersing the net income to the employee, similar to what is currently done with FICA. If the government wants to track money flow, the government could issue the employee an encrypted version of their social security number, the validity (but not the actual contents) of which could be verified by the employer. The employer would then submit the required reports using this encrypted identifier in place of the social security number. The use of multiple versions of this encrypted identifier would prevent it from being used as a pseudo-identifier. This approach blinds the employee's identity to the employer but not to the government. This approach does impose some administrative overhead for the generation and decryption of the encrypted identifiers. If the government is unwilling to incur this overhead, an outsourcing model could be employed. In this case, a trusted intermediary could shield the individual's identity while satisfying the reporting and accountability requirements. Employee anonymity is less secure since the intermediary now knows his identity.

Key words: Anonymity, blind certificate, anonymous credentials, accountability, employment

INTRODUCTION

Recent regulatory changes and technological innovations have impacted the competitive landscape. The emergence of Internet-based firms such as Amazon.com and the proliferation of free trade agreements around the world are increasingly opening local markets to global competition. At the same time, some firms are finding qualified workers overseas to satisfy their staffing needs at lower costs. In response to these business pressures, companies have adopted innovative staffing strategies, including increased reliance on temporary and contract workers, outsourcing of non-mission critical corporate activities, reliance on virtual teams and increased use of technology. Each of these staffing approaches implicitly assumes that the worker's

Corresponding Author: Bezalel Gavish, Eugene J. and Ruth F. Constantin Distinguished Chair in Business, Edwin L. Cox School of Business, Southern Methodist University, Dallas, P.O. Box 750333, TX 75275-0333

Digital Signatures and digital certificates[2]

Given: Individual X's Knowledge-u_x, v_x; where, $u_x(v_x(M)) = M$
Certifying Agency Knowledge-u_a, v_a; where, u_a is also publicly known
Digital Certificate = (DC, v_a(DC)), where, DC contains u_x and uniquely identifies Individual X
Digital Signature = (M, v_x(M))

Validation: If $u_a(v_a(DC)) = DC$ then the certificate is valid, which confirms that X owns u_x. Individuals can trust that X generated message if $u_x(v_x(M)) = M$

Blind Signatures[3,4]

Given: Individual X's Knowledge $-u_x^s, v_x^s, u_b, v_b$

Accreditation Agency Knowledge $-u_a^s, v_a^s, u_b\left(u_x^s\right)$

Blinded certificate = $\left(M, v_a^s(M)\right)$ where, $M = u_b\left(u_x^s\right)$

Unblinded certificate = $\left(u_x^s, \hat{M}\right)$ where, $\hat{M} = v_a^s\left(u_x^s\right) = v_b\left(v_a^s\left(u_b\left(u_x^s\right)\right)\right)$

Validation: If $u_x^s = u_a^s\left(\hat{M}\right) = u_a^s\left(v_a^s\left(u_x^s\right)\right)$ then the certificate is valid

If $msg = u_x^s\left(v_x^s(msg)\right)$, certificate ownership is verified.

Fair blind signatures[5,6]

Incorporates an additional trustee into the signing process. The trustee has the ability to break the anonymity of a signed token and identify the owner of the certificate.

Fig. 1: Public key encryption technologies

identity is known. There is no provision in existing practices for the support of anonymity within the traditional employer-employee or business-business relationship.

The ability to hide one's identity can be beneficial and even necessary for certain activities (Fig. 1). Consider noted food critics who make reservations under assumed names and even wearing disguises in order to evaluate the dining experience as others would. Anonymity can be useful in protecting strategic economic interests. Knowledge of the buyer's (or seller's) identity can influence contract terms. For example, developers may use multiple intermediaries to buy land for an unannounced project. If the purpose of these purchases becomes known, a holdout landowner can demand a premium, or may even refuse to sell at any price. Corporate marketers will at times strive to achieve a degree of anonymity through multi-tier branding. Some firms treat their brands as an integrated family of products, as is the case with GM and Ford. Alternatively, some firms strive for brand separation, as is the case with Toyota and Lexus, a division of Toyota.

Anonymity can also be beneficial in an employment context. Some individuals may be reluctant to be associated with certain positions or organizations, for there may be a stigma attached. Taking the job may limit the future set of positions that they can be considered for (for example taking a simple programming job which closes their potential for managerial or project leadership positions), it also imposes increased costs/risks, or have some negative impact on future earning potential. For example, an underemployed, high priced consultant may decline a job below her normal rate, for it could make it harder to command the higher rate on future jobs. Anonymous employment may help alleviate these concerns, thereby increasing the size and quality of the application pool and ultimately improving the hiring decision (Fig. 1 and 2) detailing various rationales for anonymous and fully identified interactions).

There are significant obstacles to the support of contractual anonymity, namely:

- How can each party evaluate the capabilities and veracity of the other? How can claimed expertise be verified and references checked if the identity is not known?
- How can payment be assured after contracted work is complete? In an anonymous environment the traditional legal avenue of suing for breach of contract is unavailable. Even if the anonymity is asymmetric (i.e., the employee knows the employer, but the employee's identity is unknown to the employer), it is undesirable to require someone to relinquish anonymity to enforce the contract's terms.
- The employer needs a mechanism to prove all payments have been made and that they have been made to the person who earned them.
- There is the issue of accountability and warranty. If the work quality is unsatisfactory, or a problem emerges later, what recourse does the employer have to hold the employee responsible for work completed if his/her identity is unknown?

RATIONALE FOR THE SUPPORT OF ANONYMITY

Privacy
- To protect identity (i.e., avoid identity theft), protect one's time, space, person and resources
- To encourage reporting, information seeking and self-help (i.e., drug and alcohol, AIDS, pregnancy)

Confidentiality
- To facilitate the flow of information (i.e., encourage whistle blowers to come forward and protect identity of media sources such as Watergate era 'Deep Throat')
- To obtain sensitive personal information for research (i.e., behavioral and medical research)
- To provide for unbiased medical research (prevent bias of the results)
- To obtain a resource or encourage action involving illegality ('no questions asked' amnesty programs, needle exchange)

Secrecy
- Protect strategic economic interests (i.e., developer buying up land through third parties for an unannounced development)
- To encourage experimentation and risk-taking

Security
- To protect donors or those taking controversial but socially useful action (anouymous donations and protecting identity of birth parents giving a child up for adoption)
- Protecting from reprisal (Witness Protection Program, Special Reaction Forces concealing their identity)

Neutrality
- To avoid bias and persecution (i.e., authors using a pen name to improve acceptance and avoid stereotyping, as with Mary Shelley's Frankenstein and Charlotte Bonte's Jane Eyre)
- Relative anonymity of the Internet levels the playing field, "On the Internet, nobody knows you're a dog"[7]
- Encourage attention to message content (anonymous author of Primary Colors "wanted the book to be reviewed, not the author")
- Provide impartiality and facilitate judgements based on specified criteria (i.e., blind reviews of proposals, blind trusts for elected or appointed officials)

Reduce inhibitions
- To encourage broader exploration or issues (i.e., reduce 'group think', allow position change without appearing indecisive)[8,9]
- Allowing individuals to present novel, but poorly developed ideas, unpopular or politically risky ideas[10]
- Address self-conscience behavior, fear of embarrassment

RATIONALE FOR IDENTIFIABLE INTERACTIONS

Accountability
- To hold individuals accountable for their actions. To facilitate an equity based reward and punishment system
- To make possible insurance and guarantees (required to assess risk)
- Judge an individual's reputation (i.e., credit reports, background checks)
- Discourage anti-social behavior (i.e., 'flaming' in email, mob violence, 'deindividualization')

Verify eligibility
- To allow the checking of credentials (i.e., driver licenses, confirm education, work history and references)

Improve efficiency
- Development of individualized behavioral history can help improve service (i.e., Amazon.com's suggested book titles based on prior purchases)
- Longitudinal research linking multiple data sources (i.e., medical and marketing research and data mining)Address Social Welfare Concerns
- To protect the public health (i.e., containing the spread of communicable disease, such as hepatitis; tracking potentially dangerous individuals, such as sex offenders and potential terrorists)
- Concerns over genetic predisposition to illness may require identification of sperm and egg donors or birth parents of children given up for adoption
- Military's use of DNA to identify solders who die in battle
- Social Orientation and Relationship Building
- Provide a degree of social orientation to strangers. (i.e., sex, ethnicity, religion, lifestyle)
- Exchanging personal information can increase the bond between individuals

Fig. 2: Rationales for anonymous and identifiable interactions (Adapted from Marx[11])

Even if these technical issues are resolved, at least three governmental issues must be addressed. The first is the collection of income taxes, which depends on the ability to explicitly link individuals to the income they earn. Social security taxes pose another problem, for it splits taxes between the employer and employee. The second deals with the Security and Exchange Commission's fiduciary duty to protect stockholder interests. The SEC requires firms to file 8-K disclosures dealing with executive pay and anonymity could impact the paper trail that provides the basis for these reports. The third issue is that of social equity-either in the guise of enforcing equal opportunity and non-discrimination, or in support of affirmative action (i.e., contract set-asides, quotas and contracts with minority owned firms). Anonymity would tend to support equal opportunity,

since it explicitly hides the applicants' identity. If work is done off-site and all communication is done electronically, physical characteristics (i.e., sex, age, disability, race, ethnicity, etc.) are not observable, significantly reducing the potential for bias. (it may give the applicant the possibility to lie and tell the company that he is a handicaped minority employee while he/she is of a non-minority class and is not handicap). Unfortunately, it is exactly these physical characteristics that we want to track to support the goals of affirmative action.

MECHANISMS TO SUPPORT ANONYMOUS EMPLOYMENT

Existing business processes do not support anonymity. Consequently, to enable anonymous employment new processes are needed. Mechanisms that can support anonymous contractual agreements draw heavily on the public key encryption technology. Public Key Encryption (PKE) is a dual key encryption scheme, where individual X's two keys are referred to as her public and private key and designated as u_x and v_x, respectively. A message M encrypted with one key can only be decrypted with the other (i.e., $M = v_x(u_x(M)) = u_x(v_x(M))$). The system's integrity depends on the fact that only the key set owner knows the private key. Researchers have developed various mechanisms using PKE, namely (Fig. 2):

- Digital Signatures-provide proof of authorship and detect unauthorized modification of a message/document.
- Digital Certificates-a credential service, where a trusted third part attests to the fact that a particular public key belongs to a given party.
- Blind Signature-technique that supports credentials for anonymous individuals. Once signed by the certifying agent, the certificate can be validated, but can not be traced back to the individual to whom it was issued, even by the certifying agent.
- Fair Blind Signature-allows blind signatures to be invalidated under extra-ordinary circumstances. This is accomplished through the introduction of a trustee that can breach anonymity if required.

AUTHENTICATION OF ANONYMOUS CREDENTIALS

Employment contracts impose additional requirements beyond those found in other contracts. The government regulates who can legally be hired (i.e., age and residency limitations). Certain positions require special certifications or licenses. Beyond these regulatory requirements, employers often verify an applicant's background and qualifications to mitigate hiring risks. This could include the applicant's education, criminal background check, employment history and references. These certifications are often handled through third-party credentialing agents-universities give diplomas, engineers sit for their Professional Engineers (PE) license, doctors must be 'board certified', accountants earn their CPA, lawyers must pass the bar and in many states plumbers, electricians, truck drivers, beauticians, building contractors and even auto mechanics must be locally licensed. The applicant may also want to check into the background and reputation of the prospective employer, such as its financial strength, pending litigation and its environmental and social commitment.

To support anonymity the certifying/accrediting body must be able to validate the individual's claims, provide a verifiable certificate explicitly linked to the individual, yet not be able to trace it back to the person when it is presented for verification. A Blind Certificate can be generated using a Blind Signature, which uses a transitive encoding scheme to generate valid digital signatures for messages not seen by the signer. Under the blind signature scheme an individual supplies the certifying agent a blinded token represented as $u_b(T)$. After validating the individuals claim, the agent would digitally sign this blinded token without ever seeing the unblinded token (signature of blinded token = $u_a(u_b(T))$). The individual could then apply the appropriate key to unblind this signature resulting in the appropriate signature for the original Token (i.e., $v_b(u_a(u_b(T))) = u_a(v_b(u_b(T))) = u_a(T)$). The individual can now combine this signature with the unblinded token to generate an untraceable, yet verifiable certificate.

Unfortunately, this does not provide verifiable ownership of the certificate. This can be accomplished by incorporating a challenge/response mechanism into the certificate itself. Rather than a random token, the individual can provide a blinded public encryption key. After the certifying agent signs this blinded key, the signature and key are unblinded. Now the individual can demonstrate certificate ownership by proving access to the private key corresponding to the public key imbedded in the certificate (e.g., by properly decrypting a message encrypted with the public key).

This approach can be used to certify all manner of personal traits and accomplishment. Note that the token imbedded in the certificate does not define the certificate's significance-rather the certificate is defined by the key set used to generate the blind signature. Different key sets would be used to certify different traits.

When a certifying agent may need to invalidate a certificate, fair blind signatures are required. The trustee's ability to associate each signature with its owner provides the ability to invalidate a signed certificate, but unfortunately, also negates the guarantee of absolute anonymity.

ANONYMOUS PAYMENTS

Compensation in non-anonymous environments is commonly handled by issuing a check or through direct deposit. In either case, standard processes provide an auditable paper trail that can verify payment. Unfortunately, this straightforward procedure is not available with anonymous employees. Some mechanism that upholds the integrity of the anonymous compensation process is needed. This process must provide the usual safeguards found in conventional contractual situations[1]. It must permit:

- Employers to prove that all contractual payments have been made (provides protection against anonymous employee's claim that payment was not made)
- Anonymous employees to prove employer's non-payment of contractual fees (provides protection against employer's false claim of payment) and
- Verification of the proper flow of funds (prevents others from masquerading as the worker and usurping their compensation).

This can be done using a modified digital money scheme incorporating blind signatures. To verify payment, the non-traceable digital money can be blinded with the anonymous employee's public key. Since only the employee knows the corresponding private key, she is the only person that can access the payment. To provide a proof of payment, the employee must sign a receipt with her private key when cashing the payment. An inability to produce the signed receipt indicates that the funds have not been distributed properly.

TAXATION

The IRS has established specific reporting requirements to allow them to track salary payments and crosscheck reporting compliance. Regulations require the identification of the employee's social security number and the amount distributed. To support true anonymous employment yet still address the government's need to track individual income requires a scheme whereby:

$$M_i = (u_i, u_s(v_i), u_g(SSN+u_i))$$
$$SSC_i = (M_i, v_g(M_i))$$

Where: u_i, v_i are the individual's certificate-specific public and private keys
u_g, v_g is the government's public and private keys
u_s is the individual's primary secret key and $M = u_s(u_s(M))$
SSN is the individual's Social Security Number

Fig. 3: Social Security Certificate using personalized key escrow to reduce key management problem

- Government can readily access an individual's unique identifier (i.e., social security number)
- Employers can verify that an blinded identifier supplied by the employee is valid
- Non-governmental parties cannot associate records derived from different data sources.

Instead of reporting the employee's Social Security Number (SSN), a digital Social Security Certificate (SSC) generated by a government or trusted agent could be used (Fig. 3).

The validity of the SSC_i is checked using the government's public key, thus validating the blinded SSN. Note that the employer does not have access to the unblinded SSN. This precaution is added to address the third criteria-i.e., that it must not be possible to uniquely associate an individual across multiple data sources, as is currently done with the SSN. Consequently, each SSC_i can only be used once (otherwise it would become a surrogate key), individuals require multiple, distinct certificates. This can be accomplished by concatenating the SSN with the individual's certificate-specific public key prior to encrypting with u_g. This imposes a slight overhead on the government since the SSC_i must be decrypted to determine the individual's SSN, however it improves system integrity since certificate ownership can now be verified, a feature not available with the current SSN. Unfortunately, it also imposes a significant key management problem on the user, for it requires a new public and private key for each certificate. This problem can be addressed using a personalized version of key escrow. The individual can imbed in the certificate an encrypted version of the private key (i.e., $u_s(v_i)$) corresponding to the imbedded public key u_i. The individual can now reclaim the certificate-specific decryption key for multiple certificates while only having to manage the single secret key.

ANONYMOUS EMPLOYMENT PAYING MAXIMUM TAX RATE

Ensuring appropriate tax payments could be accomplished by deducting the tax directly from the gross

pay, as is currently done with Social Security (FICA). But at what tax rate should taxes be withheld? If all revenue was fully disclosed, the appropriate marginal tax rate can be determined. If the marginal rate is bound by some maximum value, the joint objectives of collecting all appropriate taxes while simultaneously supporting the taxpayer anonymity could be accomplished by withholding at this maximum tax rate. Under this scheme the employee would have to decide if the anonymity provided is worth the added cost of being taxed at this maximum rate.

ANONYMOUS EMPLOYMENT THROUGH OUTSOURCING CONTRACT

Outsourcing is another approach to achieve a limited degree of anonymity. A firm could contract with a service bureau or employment agency, which then contracts with the individual doing the work. The employer now has an identifiable entity (i.e., the service bureau) to which payments are made. The service bureau is responsible for reporting payments to the IRS for the 'anonymous' worker and can shield her identity from the employer. Under this scenario the employee's anonymity is not guaranteed. The service bureau knows (and subsequently could disclose) the employee's identity.

ACCOUNTABILITY OF ANONYMOUS EMPLOYEES

The last area that needs to be addressed is the issue of accountability for work done by anonymous individuals. Depending on the nature of the work, productivity and quality may be immediately obvious, or may only become evident over time. When work can be objectively evaluated and progress monitored, accountability is less of a problem. If the output is unsatisfactory, the contract can be terminated. It is when productivity and quality cannot be closely monitored that other remedies are needed.

Again, we look to traditional environments to see how this issue has been addressed. One approach is for the worker/employees to guarantee the work quality. Payment may be withheld or put in escrow until satisfactory performance is demonstrated or, partial payments can be made based on verifiable deliverables. Alternatively, the employee could post a bond as a guarantee. Under either scenario contract negotiations would establish the obligations and penalties for both parties. The contract would be digitally signed to demonstrate knowledge of and agreement with these terms. If parties are anonymous and untraceable, the introduction of a known, trusted arbitrator would be required to oversee and ensure the agreement's integrity (e.g. anonymous escrow services). In the most straightforward case, objective, observable metrics would be used to verify compliance with the contract terms. Absence of such metrics increases the risk because contract resolution is indeterminate, being subject to the arbitrator's decision. Once the arbitrator reaches a decision, funds would be distributed through an anonymous payment scheme.

REFERENCES

1. Gavish, B., J.H. Gerdes and J. Kalvenes, 2000. Reward allocation in an anonymous GDSS environment. Group Decisions and Negotiation, 9: 393-413.
2. Rivest, R.L., A. Shamir and L.M. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 21: 120-126.
3. Chaum, D., 1983. Blind Signatures for Untraceable Payments. Advances in Cryptology-Crypto '82, Springer-Verlag, pp: 199-203.
4. Chaum, D., A. Fiat and M. Naor, 1988. Untraceable Electronic Cash. Advances in Cryptology-Crypto '88, Springer-Verlag, pp: 319-327.
5. Stadler, M., J.M. Piveteau, J. Camenisch, 1995. Fair Blind Signatures. Advances in Cryptology Proc. of Eurocrypt '95, LNCS 921, Springer-Verlag, pp: 209-219, 1995.
6. Camenisch, J., U. Maurer and M. Stadler, 1996. Digital Payment Systems with Passive Anonymity Revoking Trustees, ESORICS '96, LNCS 1146, Springer-Verlag, pp: 33-43.
7. Steiner, P., 1993. <http://www.unc.edu/depts/jomc/academics/dri/idog.html>http://www.unc.edu/depts/jomc/academics/dri. The New Yorker, 69: 61.
8. DeSanctis, G. and B. Gallupe, 1987. A Foundation for the Study of Group Decision Support Systems. Management Science, pp: 589-609.
9. Jessup, L.M., 1990. The effects of anonymity on GDSS group process with an idea-generating task. MIS Quarterly, Minneapolis,14: 313-321.
11. Marx, G., 1999. What's in a name? Some reflections on the sociology of anonymity. The Information Society 15: 99-112. http://web.mit.edu/gtmarx/www/anon.html
10. Shepherd, M.M., R.O. Briggs, B.A. Reinig, J. Yen, J.F. Nunamaker, 1996. Invoking Social Comparison to Improve Electronic Brainstorming: Beyond Anonymity. J. Manage. Inform. Sys., 12: 155-170.