On the Risks of IBE

Himanshu Khurana and Jim Basney

National Center for Supercomputing Applications, University of Illinois
{hkhurana, jbasney}@ncsa.uiuc.edu

Abstract. Identity-based encryption (IBE) techniques promise to solve the key distribution problem for secure email. We argue that before this technology is adopted for the important application of secure email it needs to be critically examined in terms of its benefits and risks. To that end our analysis summarizes the unique benefits of IBE and also the significant assumptions and limitations behind it. We then argue that all of these benefits can be achieved with RSA without any additional assumptions and limitations by developing IB-MKD (Identity Based - Message Key Distribution).

1 Introduction

Since the seminal work on Identity Based Encryption (IBE) by Boneh and Franklin [4] and Cocks [6], identity based cryptography is now flourishing within the research community. Secure email was the first critical application for IBE identified by its developers, and IBE's application to secure email has been studied and developed extensively[1] [1], [4], [14], [16]. The promise that IBE brings to secure email is the ability to solve the key distribution problem, which is a well known hurdle to widespread deployment and use of secure email. For secure email, IBE enables the sender to compute a public encryption key for a recipient using the recipient's email address and to encrypt the message offline using this public key, and IBE enables the recipient to decrypt this message after obtaining the private key from a Private Key Generator (PKG).

It is our contention that before the secure email with IBE solution is widely deployed and used it needs to be examined critically. What are its true benefits? What are the associated costs and trust implications? What are the alternatives? In this paper we study these questions and compare IBE with a traditional RSA based approach for email encryption. Our examination leads us to conclude that IBE for secure email comes with significant risks. First, the promise of eliminating user key distribution comes with stronger trust assumptions. Second, even if an organization is willing to accept these trust assumptions for the benefits of IBE they will be adopting an unnecessarily complex cryptosystem because all of the propounded benefits of IBE can be achieved with traditional RSA. We demonstrate the second conclusion by developing Identity-Based Message Key Distribution (IB-MKD) that associates an identity with a message key and then employs a trusted key distribution center to distribute the message key.

The rest of this paper is organized as follows. Section 2 provides an overview of IBE and RSA for secure email. Section 3 analyses the trust assumptions behind IBE,

[1] Including a commercial implementation by Voltage Security (http://www.voltage.com).

and Section 4 discusses the benefits of IBE. Section 5 presents our IB-MKD solution that achieves the benefits of IBE, and Section 6 concludes the paper.

2 Secure Email with IBE and RSA

Encrypted email with IBE. In designing a world-wide system for secure email it is unlikely that users would be willing to trust a single PKG. Therefore, a domain-based administration approach where each domain maintains a PKG for its users is appropriate [16]. Consider two such domains, A and B, with the sender S residing in domain A and receiver R in domain B. Each domain has its own PKG, which, upon initialization, creates a public/private key pair (PK, SK). The public parameters of the public key of domain B's PKG, PK_{PKG_B}, need to be made available to the sender. When the sender wishes to send an email to the receiver it can compute a public key for the receiver, PK_R, using a function that combines the identity of the receiver (in this case, the receiver's email address) and the public parameters of PK_{PKG_B}. In addition, the sender can include a *policy* in this key generation function that would be associated with the encrypted message. The sender then encrypts the message using PK_R with IBE and sends the encrypted message to the receiver along with the *policy*. On receiving the message the receiver authenticates herself to her domain's PKG and sends the policy, if included, to the PKG. If the policy is valid, the PKG uses her identity and the message policy to generate the corresponding private key SK_R to send back to her. Using this private key the receiver can now decrypt the message.

Encrypted email with RSA. For encrypted email exchange with RSA the domain's PKG is replaced with a Certificate Authority (CA). During registration the CA's role is to sign public key certificates for users after they generate their public/private key pairs. The public key of the receiver's domain CA needs to made available to the sender so he can use it to trust end user certificates. When the sender wishes to send an email to the receiver she must first obtain the receiver's public key PK_R encoded in a certificate (e.g., from a directory service) and verify the certificate using the CA's public key. The sender then encrypts the message with PK_R and sends it to the receiver. Since the receiver already has the corresponding private key she can now decrypt the message. An example of a standardized system for using RSA and the X.509 based Public Key Infrastructure (PKI) is S/MIME [15].

3 IBE Trust Assumptions

In choosing any security system, we must recognize and accept the associated trust assumptions. How do the trust assumptions of IBE differ from those we have come to accept for RSA-based PKIs? In both systems, we place trust in the correctness of the cryptographic algorithms and their implementations. We must also place trust in the management of cryptographic keys: how the sender determines the correct public key for a recipient and how the recipient's private key(s) are secured, so both parties have confidence that the communication is private. As IBE provides a novel key distribution mechanism, we should closely examine the trust assumptions associated with that mechanism.

As described previously, we believe that practical deployment of IBE and/or RSA requires domain-based administration of keying material, where each domain manages its own PKG or CA. In either case, the sender must obtain the PKG public key/parameters or the CA certificate for the recipient's domain in a trustworthy manner to allow the sender to determine the public key of the recipient. For IBE, this enables the sender to compute the public key. For RSA, this enables the sender to lookup the recipient's certificate in a directory [12], [13], and by verifying the CA's signature on the certificate, obtain the recipient's public key. In this aspect, IBE and RSA have similar trust assumptions. In practice, PKG parameters and CA certificates can both be distributed via DNS/DNSSEC [1], [8], [16].

We must also trust that the PKG/CA private key is known only to the PKG/CA. Compromise of the PKG private key compromises the private keys of all users in that domain. In contrast, compromise of the CA private key enables the attacker to sign and publish new compromised public keys, tricking senders into encrypting new messages to these public keys, though it does not compromise existing private keys or messages encrypted to those keys. In RSA-based PKIs, this risk is typically addressed by keeping the CA private key offline so it is not subject to online attacks. Keeping the PKG offline is feasible only if long-lived keys are used. However, IBE must use short-lived keys to support revocation [4], as there is no revocation method for IBE analogous to X.509's CRLs or OCSP. So, in practice, the PKG must remain online, with the associated increased risk of compromise. Thus, in this aspect, IBE requires stronger trust assumptions than RSA, requiring a fully-trusted, online entity (the PKG), as opposed to a partially-trusted (with respect to secrecy of user private keys), offline entity (the CA).

We also require a trustworthy process by which recipients obtain and manage their private keys. For modern RSA PKIs, recipients typically generate and maintain sole control over their private keys. As part of the certificate request and issuance process, the CA requires the keyholder to authenticate and prove posession of the private key, typically by signing the certificate request. For IBE, the PKG generates the private key and sends it to the recipient via a private, authenticated channel. Thus, in both cases, we must trust the user authentication to the PKG or CA, so private keys are not associated with the wrong recipients. For IBE, however, we must also trust that the private key is not compromised at the PKG or on the network. Again, IBE requires stronger trust assumptions than RSA.

It is well understood that IBE includes a type of key escrow, because the PKG generates the user's private keys [2], [5]. The PKG is a fully-trusted entity that could decrypt all messages in the domain, unlike a traditional CA which has no access to user private keys. IBE provides a weaker form of end-to-end security for encryption than traditional RSA-based PKIs, with the PKG as a possible man-in-the-middle. Thus, we can consider IBE trust assumptions to be in between solutions that provide strong end-to-end security and gateway-based systems, where the sender must trust the recipient's domain administrators to properly handle encrypted messages [3], [7].

Thus, we conclude that, to solve the key distribution problem for secure email, IBE requires us to accept stronger trust assumptions, when compared with RSA-based PKIs. The IBE PKG is a fully-trusted entity which must remain online in practice to support the use of short-lived keys for revocation. Unlike an offline CA, the PKG can decrypt all messages destined for recipients in the domain, providing a weaker form of end-to-end security than traditional RSA-based PKIs.

4 Benefits of IBE

We identify three unique benefits of IBE that are not provided by today's RSA based secure email systems such as S/MIME.

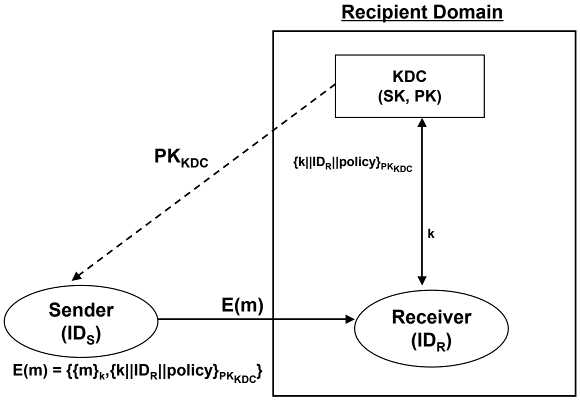
1. **Eliminate user key distribution.** In IBE once the sender obtains the parameters of a particular domain's PKG, he can compute the public key of any user in that domain. That is, instead of requiring one online (public) key fetch operation per recipient as in RSA, IBE only requires one online key fetch operation per domain (the PKG's key). By effectively eliminating the need to distribute end user public keys, IBE addresses a major hurdle in widespread deployment and use of secure email. This is perhaps the most important benefit of IBE.
2. **Policy based encryption.** Using IBE the sender can associate arbitrary policies with the encrypted email message. It can do so by concatenating the *policy* with the recipient's ID prior to computing the public key. When the message is encrypted using this key, the PKG can enforce the sender's policy regarding the release of the private key. For example, the sender can postdate the message by including a specific date in the encryption key, and the PKG will then release the corresponding key only on or after that date. This benefit is beginning to gain value as email messaging is being used increasingly for formal communication and is being incorporated into workflow systems. For example, in secure role based messaging for healthcare [14] a patient can compose a message to "*cardiologist on duty*". However, in such applications the policy itself might be sensitive; e.g., this example policy could indicate that the patient has a heart problem. In IBE, this policy is accessible in the cleartext as the message travels from the sender to the recipient.
3. **Implicit client mobility.** In IBE the receiver can contact the PKG whenever it needs a private key. Therefore, as long as the receiver can contact the PKG, IBE provides seamless client mobility as the recipient can use any device from any location to access private keys for email decryption. This benefit is very valuable as users often check email using a variety of devices such as PDAs and laptops and do so from a variety of locations. In RSA users can utilize smartcards or online credential repositories to provide client mobility but this benefit is not provided implicitly.

5 RSA-based Alternatives to IBE

From the previous two sections we see that IBE has unique benefits but also additional trust assumptions when compared to RSA. This leads to an interesting question of whether an RSA based approach can be devised to achieve the benefits of IBE and address its limitations. Ding and Tsudik [9] developed an identity-based mediated RSA (IB-mRSA) system that provides an identity-based encryption capability using conventional RSA with support for fine-grained revocation. However, they do not provide policy based encryption or support for implicit client mobility. Callas [5] proposes an online PKG solution for identity-based encryption that can replace IBE cryptography with RSA. However, his solution still requires the sender to undertake an online key fetch operation per recipient (rather than once per domain for IBE or IB-mRSA) and does not support policy based encryption.

We present an alternative solution, which we call identity-based message key distribution (IB-MKD). IB-MKD works with conventional RSA and achieves all the benefits of IBE that we have identified. IB-MKD is similar to the object-based key distribution scheme of Ford and Weiner [11] [10]. However, their work predates practical IBE schemes and was intended as a general-purpose key distribution scheme for various applications including email. In contrast, IB-MKD was designed to illustrate how RSA based solutions can achieve the benefits of IBE for secure email.

The IB-MKD solution is illustrated in Figure 1. Here each domain establishes a Key Distribution Center (KDC), which upon initialization creates a public/private key pair (PK_{KDC}, SK_{KDC}). In the figure we only show the KDC for the recipient's domain and assume that the sender is outside this domain. The public key of each KDC is assumed to be made available to all users; in particular, available to the sender; e.g., via DNS.


Recipient Domain
KDC (SK, PK)
PK_{KDC}
$\{k||ID_R||policy\}_{PK_{KDC}}$
k
Sender (ID_S)
E(m)
Receiver (ID_R)
$E(m) = \{\{m\}_k, \{k||ID_R||policy\}_{PK_{KDC}}\}$

- KDC = Key Distribution Center
- $\{m\}_k$ denotes symmetric encryption; e.g. AES
- $\{x\}_{PK}$ denotes asymmetric encryption; e.g. RSA

Fig. 1. Identity-Based Message Key Distribution (IB-MKD)

When the sender wishes to send a private email to receiver R with email address ID_R, he encrypts the email using hybrid encryption as follows. The sender first encrypts the email message m with a randomly generated symmetric key k (called the *message key*), which is unique for every message.[2] The sender then encrypts k concate-

[2] This is typically done for encrypted email today in S/MIME where this key is called the *content encryption key*.

nated with ID_R and an optional *policy* using the public key of the KDC, PK_{KDC}:

$$E(m) = \{\{m\}_k, \{k||ID_R||policy\}_{PK_{KDC}}\}$$

(The symbol "||" denotes concatenation.) This hybrid encryption therefore binds the recipient's identity to the message key k. For the symmetric encryption any standard scheme such as AES may be used, and for the asymmetric encryption RSA can be used. When R receives this message it sends a message key request to the KDC, which includes the second part of the encrypted message:

$$\{k||ID_R||policy\}_{PK_{KDC}}$$

The KDC first decrypts this part of the message using its private key SK_{KDC} and then authenticates the user (e.g., using a password). The KDC then ensures that the message is intended for R by checking against ID_R embedded in the decrypted message. If the match succeeds KDC sends the message key k back to the user over a secure channel. That is, the KDC distributes the message key only after it verifies the identity of the requesting user. Optionally, if a policy is specified in the encrypted message then the KDC can enforce that policy prior to releasing the message key. The user can now decrypt the message with this message key.

5.1 Analysis

Our very simple approach achieves all the practical benefits of IBE that we have identified and eliminates the need for key revocation. IB-MKD (1) eliminates user key distribution as the sender only needs the public key of a domain's KDC to send a message to any recipient in that domain, (2) provides policy based encryption as an arbitrary *policy* can be associated with the encrypted message, and (3) provides implicit client mobility as the recipient can contact the KDC to obtain the message key for message decryption from any location and on any device. Furthermore, since IB-MKD does not have the notion of end user key pairs it obviates the need to revoke any use keys. If, for any reason, the recipient is deemed unauthorized for a particular message the KDC can simply refuse to release the message key to the recipient.

We now analyze four differences between IB-MKD and other identity-based encryption schemes. A comparison of these schemes is provided in Table 1. First, a major difference between IB-MKD and other approaches including IBE, IB-mRSA and Callas's approach is that in our solution the sender encrypts the message with the domain public key (i.e., the KDC's public key) instead of a specific user's public key. We believe this distinction only highlights the weak notions of end-to-end security of identity based encryption systems because the security properties remain the same. That is, in IB-MKD even though the KDC has the private key required to decrypt the message intended for R, it never receives the encrypted message $-$ only the encrypted message key. This is very similar to IBE where the PKG has access to the private key for decrypting messages but only receives the public key from R and not the encrypted message.

A second difference between IB-MKD and IBE is that we encrypt the message policy (with PK_{KDC}) while IBE does not. Therefore, our solution provides privacy for the policy, which in some cases may be sensitive.

A third difference between IB-MKD and IBE is that in IBE the message is encrypted with the policy (in addition to the identity and PKG parameters) while in IB-MKD the policy is simply associated with the message key. One implication of this difference is that in IBE the receiver can verify the correct satisfaction of the sender's policy after it has access to the corresponding private key. In IB-MKD this verification capability can be provided by requiring the sender to include the policy in the message key encrypted message as well; i.e., by requiring the first part of the encrypted message to be $\{m||\mathit{policy}\}_k$.

A fourth difference between IB-MKD and IBE is that in IB-MKD the recipient has to contact the KDC for every message rather than once per policy duration as in IBE. This has two implications. First, this can potentially add a lot of overhead on the KDC. However, we argue that distribution of the message key from the KDC is comparable to the distribution of email from the mail server in a secure manner (e.g., POP over SSL), which involves establishment of a secure connection using public key cryptography and network times for transmitting potentially large messages. While the KDC would incur higher computation costs than the SSL email server because it would have to do a public key decryption per message as opposed to per session, it would incur lower communication costs because the message size containing the message key(s) will be significantly shorter than the email(s). Furthermore, these costs are amortized in practice for both the KDC and the SSL mail server by having users contact these servers periodically (say, once every 10 mins). So, we believe that the load imposed on the KDC in our solution is reasonable. Second, this difference also implies that IB-MKD supports timely policy evaluation where the sender is assured that the policy she specified is evaluated and enforced on every single message even if the policy has not been changed. In contrast, in IBE the sender has to change the policy to ensure its timely evaluation and enforcement.

6 Related Work

Table 1 below summarizes the differences between our solution and four others, namely, IBE, S/MIME, IB-mRSA [9] and Callas [5]. We evaluate these schemes against the trust assumptions and unique benefits of IBE identified in this paper. Our evaluation shows that IB-MKD achieves all the benefits of IBE without any additional trust assumptions while all other schemes fail to do so.

For trust assumptions we identify (1) the entities that are fully trusted by each scheme, and (2) whether or not the schemes provide strong end-to-end security guarantees for encryption. For unique benefits we first evaluate each scheme's ability to eliminate user key distribution. This evaluation has several aspects: (1) how many keys the sender needs to fetch (via a network operation) for encryption, (2) how many keys the recipient needs to fetch for decryption, and (2) how revocation of user keys is supported. We then evaluate the benefits of policy based encryption and client mobility. An additional evaluation parameter is the target encryption key that illustrates a unique feature of IB-MKD.

	S/MIME	IBE	IB-mRSA	Callas	IB-MKD
Trusted Entities	CA is partially trusted for public key distribution.	PKG is fully trusted.	CA and SEM are fully trusted.	PKG is fully trusted.	KDC is fully trusted.
End-to-end Encryption	CA can't decrypt messages.	PKG can decrypt messages.	CA can decrypt messages but SEM cannot.	PKG can decrypt messages.	KDC can decrypt messages.
Encryption Key fetch	One key fetch per recipient.	One key fetch per domain.	One key fetch per domain.	One key fetch per recipient.	One key fetch per domain.
Decryption Key fetch	Offline. Recipient generates the private key.	One key fetch per policy.	Contact SEM for partial decryption of each message.	One key fetch per policy.	Obtain symmetric key from KDC for each message.
Revocation	OCSP/CRLs.	Short-lived keys.	Immediate revocation via SEM.	Could support short-lived keys.	Immediate revocation via KDC.
Policy-based Encryption	No direct support.	Policy included in key generation.	No direct support.	Could be extended to support.	Policy associated with message key.
Recipient Mobility	Requires smartcard or key repository.	Implicit. Recipient fetches key from PKG.	Requires smartcard or key repository.	Implicit. Recipient fetches key from PKG.	Implicit. Recipient fetches key from KDC.
Encryption Key/Target	Recipient key.	Recipient key.	Recipient key.	Recipient key.	KDC public key.

Table 1. System Comparison

7 Conclusion

We began this study with two questions in mind. First, what are the benefits of using an IBE system for the critical application of world-wide secure email as well the necessary assumptions in achieving these benefits? Second, can these same benefits be achieved (without increased assumptions) with conventional mechanisms such as RSA?

In answering the first question we have identified three unique benefits of IBE, namely, reducing the key distribution requirement from once per recipient to once per domain, providing policy based encryption, and providing implicit client mobility. However, these benefits have significant costs associated with them. First, they come with weaker notions of end-to-end security where an entity besides the recipient (the PKG) has the necessary secrets for decrypting messages. Second, the PKG is a fully trusted entity representing a single point of trust failure whereby its compromise allows an adversary to compute the private keys of all the users of that domain. Third, this fully trusted entity is always online and thereby vulnerable to attacks. Interestingly, these same negatives have been carefully weighed over time by the research community resulting in norms that require strong notions of end-to-end security, CAs that only sign public keys but do not generate user private keys, and CAs that remain largely offline. Therefore, we argue that considerable thought must be given to these costs before adopting IBE.

In answering the second question we propose a simple solution that achieves all the benefits of IBE. Table 1 compares the solution with existing systems. Our solution uses simpler and widely-understood RSA mechanisms. Furthermore, the solution ensures privacy of the policy in policy-based-encryption where the policy itself might be sensitive. Therefore, we argue that even if one is willing to incur the costs associated with identity based encryption, simpler alternatives to IBE are available. As an example one could easily design a secure role based messaging system with IB-MKD that satisfies the requirements identified by Mont *et al.* [14].

Acknowledgements

We would like to thank Virgil Gligor for his comments on a previous version of this paper. We would like to thank Robert Zuccherato for pointing us to the work of Ford and Weiner. This material is based upon work supported by the Office of Naval Research (ONR) grant N0001404-1-0562. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of ONR.

References

1. B. Adida, S. Hohenberger, and R. L. Rivest. Lightweight Encryption for Email. In *Usenix Symposium on Reducing Unwanted Traffic on the Internet (SRUTI)*, pages 93–99, 2005.
2. J. Baek, R. Safavi-Naini, J. Hindmarsh, and W. Susilo. A Survey of Identity-Based Cryptography. In *Identification and Authentication Issues in Computing, Proceedings of 10th Australian Unix User Group (AUUG) Conference*, pages 95–102, 2004.
3. D. Bentley, G. G. Rose, and T. Whalen. ssmail: Opportunistic Encryption in sendmail. In *13th Usenix Systems Administration Conference (LISA)*, pages 1–8, 1999.
4. D. Boneh and M. K. Franklin. Identity-Based Encryption from the Weil Pairing. *SIAM J. Comput.*, 32(3):586–615, 2003.
5. J. Callas. Identity-Based Encryption with Conventional Public-Key Infrastructure. In *4th Annual PKI R&D Workshop*, number 7224 in Interagency Reports, pages 102–115. NIST, 2005.
6. C. Cocks. An Identity Based Encryption Scheme Based on Quadratic Residues. In *IMA International Conference on Cryptography and Coding, Lecture Notes in Computer Science vol. 2260, Springer-Verlag*, pages 360–363, 2001.
7. T. Dean and W. Ottaway. Domain Security Services using S/MIME. RFC 3183, October 2001.
8. M. Delayney. Domain-based Email Authentication Using Public-Keys Advertised in the DNS. IETF Internet Draft, July 2006.
9. X. Ding and G. Tsudik. Simple Identity-Based Cryptography with Mediated RSA. In *CT-RSA, Lecture Notes in Computer Science 2612, Springer*, pages 193–210, 2003.
10. W. Ford and M. J. Weiner. Computer Network Cryptographic Key Distribution Systems. United States Patent 5481613, January 1996.

11. W. Ford and M. J. Wiener. A key distribution method for object-based protection. In *CCS '94: Proceedings of the 2nd ACM Conference on Computer and communications security*, pages 193–197, New York, NY, USA, 1994. ACM Press.
12. P. Gutmann. Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP. RFC 4387, February 2006.
13. R. Housley and P. Hoffman. Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP. RFC 2585 (Standards Track), May 1999.
14. M. C. Mont, P. Bramhall, and K. Harrison. A Flexible Role-based Secure Messaging Service: Exploiting IBE Technology for Privacy in Health Care. In *DEXA '03: 14th International Workshop on Database and Expert Systems Applications*, pages 432–437, 2003.
15. B. Ramsdell. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification. RFC 3851, July 2004.
16. D. K. Smetters and G. Durfee. Domain-based Authentication of Identity-based Cryptosystems for Secure Email and IPsec. In *12th Usenix Security Symposium*, pages 215–230, 2003.