CPSC 557
Broadcast Encryption
Proposal

March 22, 2005

1 Introduction

1.1 Motivation

Broadcast encryption allows for a convenient way to distribute data in a secure manner over an insecure channel. For example, suppose Alice wishes to broadcast a message to her friends and only have the message intelligible to them. Further, suppose that the channel of communication is insecure, such as the Internet or public access network. A possible solution would be to encrypt the message using a symmetric keying system, such as the Advanced Encryption Standard (AES), for each person Alice wishes to communicate with. This however, requires that Alice keep track of all her friends' keys and encrypt the same message multiple times for each user.

Broadcast encryption provides a different solution where the broadcaster, Alice in our case, is only required to encrypt the message once, according to a predetermined key. The message can then be sent out to everyone on an open network, but only the intended recipients will have the proper corresponding key required to decrypt the message.

Satellite television, Pay-Per-View and distributions of copywrited material are obvious applications of broadcast encryption. Only paying customers will be granted access to the media. Now the focus turns to preventing unauthorized users from combining their efforts to decrypt the message. This is know as *collusion*, and systems that are *collusion-resistant* will be looked at in this paper.

1.2 Broadcast Encryption Schemes

Broadcast encryption schemes can be typically broken down into two phases. The first is the *key pre-distribution phase*, in which a trusted authority (TA) distributes some secret information to each user of a given system. This information allows each user to compute their corresponding key for future broadcasts. The second phase is where the TA actually encrypts messages in such a manner that only a specific subset of all users can correctly decrypt the message.

The first introduction of broadcast encryption was by Fiat and Naor [10] in 1993. Since 1993, considerable research has been focused on this area. Topics of interest, especially pertaining to digital media rights, include schemes which provide revocation

and *traitor tracing*, in which known 'pirates' can be tracked and punished.

Another important aspect is that of *stateless receivers*. That is, each user is given a fixed set of keys at the onset of his or her inclusion into a priviledged group. These keys remain constant and cannot change throughout the lifetime of the system. This scenario is not uncommon, consider the attitude "once-and-for-all" tamper-proof. For example, small devices like SmartCards may have limited memory capacity. This may reduce the capability to store and update many keys. In which case, a fixed set of keys may be 'hard-coded' into the device. Other devices such as DVD players may be required to decode DVDs encoded by a large production company, however it is currently infeasible to maintain and update a set of keys just to view the latest movies.

1.3 What this paper covers

This paper will formally define broadcast encryption and all relevant terminology in the next section. Following this, will be a brief look at the requirements any broadcast encryption scheme must meet including the limitations of key generation and storage. Also included, will be a discussion on the advantages and disadvantages broadcast encryption has over the classical encryption methods of symmetric key and public key encryption.

Next, this paper will briefly present the broadcast encryption scheme first introduced by Fiat and Naor [10]. This will provide the basis for looking at specific schemes which allow for stateless receivers, originally studied by Naor, Naor and Lotspiech [14]. Their scheme allows for broadcasts to $n-r$ authorized users, with n total users and r revoked users in the system. However, message headers are of size $O(r)$ and private keys of size $O(\log^2 n)$. The idea of stateless receivers were improved upon by Dodis and Fazio in [7], where the method allows for public key broadcasts with small public keys. Both of these schemes are based on the concept of *Subset-Covers* and *Subset-Differences*. They allow broadcasting to all users except a small subset whose keys may be comprimised.

Finally, this paper will look at the schemes proposed by Boneh and Waters in [5]. These schemes provide broadcast encryption which is collusion resistant against any number of colluders. As well, the system allows for ciphertext and public keys of size $O(\sqrt{n})$, where n is the number of users.

References

[1] Michel Abdalla, Yuval Shavitt, and Avishai Wool. Key management for restricted multicast using broadcast encryption. *IEEE/ACM Transactions on Networking*, 8(4), 2000.

[2] Scott A. Vanstone Alfred J. Menezes, Paul C. van Oorschot. *Handbook of Applied Cryptography*. CRC Press, first edition, 1997.

[3] Nuttapong Attrapadung and Kazukuni Kobara. Broadcast encryption with short keys and transmissions. In *DRM '03: Proceedings of the 2003 ACM workshop on Digital rights management*, pages 55–66. ACM Press, 2003.

[4] Carlo Blundo, Antonella Cresti, Alfredo De Santis, and Ugo Vaccaro. Fully dynamic secret sharing schemes. In *CRYPTO '93: Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology*, pages 110–125. Springer-Verlag, 1994.

[5] Dan Boneh and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. Cryptology ePrint Archive, Report 2005/018, 2005. `http://eprint.iacr.org/`.

[6] A. Cresti C. Blundo. Space requirements for broadcast encryption. *LNCS*, 950:287–298, 1995. Advances in Cryptology, Eurocrypt 94.

[7] Yevgeniy Dodis and Nelly Fazio. Public key broadcast encryption for stateless recievers, November 2002. ACM Workshop on Digital Rights Management.

[8] Yevgeniy Dodis and Nelly Fazio. Public key trace and revoke scheme secure against adaptive chosen ciphertext attack. Cryptology ePrint Archive, Report 2003/095, 2003. `http://eprint.iacr.org/`.

[9] Yevgeniy Dodis, Nelly Fazio, Aggelos Kiayias, and Moti Yung. Scalable public-key tracing and revoking. In *PODC '03: Proceedings of the twenty-second annual symposium on Principles of distributed computing*, pages 190–199. ACM Press, 2003.

[10] Amos Fiat and Moni Naor. Broadcast encryption. In *CRYPTO '93: Proceedings of the 13th annual international cryptology conference on Advances in cryptology*, pages 480–491. Springer-Verlag New York, Inc., 1994.

[11] Michael T. Goodrich, Jonathan Z. Sun, and Roberto Tamassia. Efficient tree-based revocation in groups of low-state devices. In *CRYPTO '04: Proceedings of*

the 24th Annual Interntional Cryptology Conference on Advances in Cryptology, pages 511–527, 2004.

[12] Dani Halevy and Adi Shamir. The lsd broadcast encryption scheme. In *CRYPTO '02: Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, pages 47–60. Springer-Verlag, 2002.

[13] Yvo Desmedt Mike Burnmester. A secure and efficient conference key distribution system. *LNCS*, 950:275–286, 1995. Advances in Cryptology, Eurocrypt 94.

[14] Dalit Naor, Moni Naor, and Jeff Lotspiech. Revocation and tracing schemes for stateless receivers. Cryptology ePrint Archive, Report 2001/059, 2001. `http://eprint.iacr.org/`.

[15] Carles Padr, Ignacio Gracia, Sebasti Martn, and Paz Morillo. Linear broadcast encryption schemes. Cryptology ePrint Archive, Report 2001/089, 2001. `http://eprint.iacr.org/`.

[16] Bruce Schneier. *Applied Cryptography*. John Wiley and Sons, Inc., second edition, 1996.

[17] Chung Kei Wong, Mohamed G. Gouda, and Simon S. Lam. Secure group communications using key graphs. In *Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication*, pages 68–79, 1998.