The Xzibit Key System Design

Jonathan Moroney

March 15, 2016

1 Introduction

Public key crypto-systems are well known and well respected as a method of securely passing messages and have been in use for a number of years. The most well known public key crypto-system is the OpenPGP message passing protocol which itself has a number of implementations ranging from the Free software GnuPrivacyGuard (GPG) to the commercial products developed by Pretty Good Privacy Corporation. For the purposes of this paper I will simply use the term OpenPGP to generically refer to this system and these programs. Further the reader is expected to either understand public key crypto-systems or to be able to research them. This is not a primer on public key cryptography.

1.1 OpenPGP

OpenPGP works on top of the SMTP mail network to pass messages and this obviates the need to redevelop a network of systems to pass messages; a pragmatic choice for a new system to be sure. However, OpenPGP is a public key crypto-system and thus requires users to have and to exchange keys in order for the system to work. Ideally it would be nice for the message passing infrastructure to all pass keys, but given that OpenPGP's origin in on the SMTP infrastructure this is not possible. So, the OpenPGP system originally tasked the user with key management and thus doomed itself to a niche of tech savvy users. The idea of key servers and automatic key retrieval has since been introduced, but the non-default nature of them has limited their adoption to the tech savvy niches and to corporations willing to pay for automation.

1.2 The technically illiterate

The technical challenge of deploying OpenPGP has prevented the non-technical user from adopting it and has left us with (E)SMTP as the standard used by the majority of email users. This is a obviously a problem for the non-technical user as all of their traffic is in the clear, but it is also a problem for the technical user who needs to be in contact with the non-technical user. It is this author's opinion that it is not that public key cryptography is difficult to use, but rather that it is difficult to setup and to maintain. It's a problem of infrastructure.

2 The Xzibit Key System

The Xzibit key system is designed to enable public key cryptography without the cognitive load often associated with it. As a component of the Cipher Mail Transport Protocol (CMTP), Xzibit key storage does not stand and the reader is encouraged to read the other design documents. The primary idea employed is that user need not be aware that they even have keys when using CMTP. Keys obviously need to be generated, but then they are stored and transferred as well. All steps are covered by the Xzibit key system.

2.1 Key Generation

Key generation is the single most implementation dependent of the Xzibit components. User key pairs should be generated randomly and should be of sufficient size so that the odds of two users obtaining the same key pair is improbable. CMTP uses Ed25519 keys which are 256 bits in size. Salting a random generation with a current time or some other system metric is acceptable, but users should not be trusted to be a source of entropy. Once the key pair has been generated the private key should be encrypted with a symmetric cipher using an ephemeral key such has a users password. Ideally some other information should be stored along with the private key such as a timestamp to defend against known plaintext attacks. Storing other user information like an address book is also a good idea and is planned for CMTP. This enciphered private package is hence forth called the xzibit.

2.2 Key Storage

Storing the private keys is of great importance in a system such as OpenPGP and a user is presented with many warning when using an OpenPGP client. The analog here is to store the xzibit and the public key with the users mail server for future retrieval. CMTP makes use of this to provide IMAP like login capabilities and to move the burden of storing the key from the user to the infrastructure. There is a risk here as the infrastructure can be attacked and the xzibit may be stolen. This system leverages symmetric key cryptography quite heavily and should symmetric key cryptography fail so too will the Xzibit key system.

2.3 Key Transport

Simply given either the public key or the xzibit to anyone that asks for them. this should fit with the readers intuition for the public key; that is the nature of a public key to be public. But the reader may worry about the xzibit. This is the leveraging of symmetric key cryptography. As long as symmetric key cryptography is strong the only person that can decrypt the xzibit is the user to whom it belongs.