POSTER: Towards name-based trust

Nikos Fotiou and George C. Polyzos

Mobile Multimedia Laboratory
Athens University of Economics and Business,
Athens, Greece
{fotiou,polyzos}@aueb.gr

Abstract. Nearly all secure communications in the Internet are based on the public-key infrastructure (PKI). Although it "still works", PKI is a fragile ecosystem and various replacements are investigated. In this poster, we propose a trust system solely based on names. To this end we leverage contemporary hierarchical identity based encryption schemes and we propose a solution that can be used to build name-based trust.

1 Motivation

The public-key infrastructure (PKI), which is at the heart of almost every secure communication system, is as strong as the weakest Certificate Authority (CA). In this poster we propose a chain of trust built directly on names. Such an approach has many advantages, including: (i) the main trust primitives are human readable (therefore memorable) (ii) CAs can be replaced with naming authorities and key resolution can be performed during name resolution, therefore the information required in order to verify the identity of a remote entity is known before the initiation of the communication (iii) trust systems can be built using various types of identities (e.g. email addresses and content identifiers) and (iv) identity hierarchy allows failure isolation (in contrast to PKI where a malicious CA may jeopardize the whole trust system). Our scheme can be deployed by leveraging the existing DNSSEC infrastructure.

2 Approach

We propose a solution based on Hierarchical Identity Based Encryption (HIBE). Using HIBE, a plaintext can be encrypted using any (real world) identity and some public, well-known, System Parameters (SP) as a key. The resulting ciphertext can be decrypted using the secret key (SK) that corresponds to the identity that was used in the encryption key, as well as, the SKs that correspond to this identity prefixes. SKs and SP for a "top level" identity are generated by a trusted Private Key Generator (PKG), whereas an owner of an identity ID_A can generate the SKs for the identities that use ID_A as a prefix; the SP can be the same for all identities that share the same prefix. A HIBE based solution has many applications including verification of digital signatures using identities, authenticated key exchange, content distribution delegation with support for content provenance verification and fine grained access control. Recent advances in HIBE has led to practical schemes, such as the solution proposed by Lewko and Waters [2] which supports arbitrary identity length as well as arbitrary identity hierarchy depth, with constant SP. In this scheme the number of identities and the identity depth does not have to be pre-configured. This comes with the cost of some overhead since the length of secret keys, the length of ciphertexts and the number of operations required to encrypt/decrypt a message are proportional to the depth the identity they concern. Nevertheless we believe that this overhead is acceptable since encryption/decryption operations will be applied over small amount of data (usually over symmetric encryption keys and digital signatures)

As a migration strategy we propose the coupling of HIBE with DNSSEC [1]. In this hybrid solution each leaf DNS server acts as a PKG, with its own SP. Moreover each DNS server has a legacy public/private key. The public key of each DNS server is transmitted to its parent DNS server, which in return digitally signs it (i.e., DNSSEC). Finally all DNS clients are pre-configured with the public keys of the root (only) DNS servers. It should be noted here that these certificates are self-generated and no CA is required: DNSSEC trust model bootstraps from the well-known public keys of the root DNS server. SP are stored as a prefixed DNS name (e.g., `SP.aueb.gr`). The resolution of this name follows the standard DNSSEC procedure the last step of which results in the transmission a "special" record which contains the SP. From this point on, a user is able to encrypt a message or verify digital signatures of any identity which uses as a prefix the given name.

In order to mitigate the problem of identity/key revocation we propose the usage of different identities as identifiers and different identities as keys. The identities used as identifiers can be legacy domain names, content URIs, email addresses and so forth. The identities used as keys then would be the identifier appended with a *serial number* (e.g., `gr.aueb0034`). In order to learn the current serial number of an identity the following solutions can be applied: (i) resolve the serial number using DNSSEC (e.g., perform a DNS lookup for `SN.www.aueb.gr` (ii) have the communicating endpoints to agree out-of-band for a serial number (e.g., use as a serial number the current date) (iii) have the client generate the serial number and force the owner of the identity to generate a new SK.

References

1. Arends, R., Austein, R., Larson, M., Massey, D., Rose, S.: DNS security introduction and requirement. RFC 4033, IETF (2005)
2. Lewko, A., Waters, B.: Unbounded HIBE and attribute-based encryption. In: Advances in Cryptology EUROCRYPT 2011, *Lecture Notes in Computer Science*, vol. 6632, pp. 547–567. Springer Berlin Heidelberg (2011)