Extending Trusted Computing as a Security Service

Chunhua Chen*, Chris Mitchell and Shaohua Tang*
Information Security Group, Royal Holloway, University of London

Abstract

We extend the Trusted Computing (TC) security infrastructure in a Generic Authentication Architecture (GAA)-like framework to ensure the provision of security services, such as key establishment, to network applications.

Background

Generic Authentication Architecture:
- Standardised by 3GPP and 3GPP 2.
- A general framework that extends the cellular authentication infrastructure (includes UMTS and GSM) to enable the provision of security services to network applications.
- Consists of two procedures, GAA bootstrapping and use of bootstrapped keys.

Trusted Computing (TC) Security Infrastructure:
A Trusted Platform (TP) compliant with the Trusted Computing Group (TCG) specifications is a computing platform with a tamper-proof and built-in Trusted Platform Module (TPM).

Properties of TPM:
- Protected capabilities, such as random number generation, asymmetric key generation, digital signing, encryption, capabilities, etc.
- A unique Endorsement Key (EK) pair and a set of derived keys, such as an Attestation Identity Key (AIK).
- Other properties:
  - TPM, associated keys, protected capabilities, and the underlying Public Key Infrastructure (PKI) comprise a security infrastructure.

Core work

We make the TC security infrastructure play the role of the cellular authentication infrastructure in the GAA framework, and hence extend the TC security infrastructure to provide a security service, which we call TC GAA.

- Specify the architecture and components of TC GAA.
- Specify the interfaces and protocols between components.
  - Specify bootstrapping procedure of TC GAA, including an authenticated key agreement protocol.
  - Specify the derivation of an application-specific session key.
  - Specify use of bootstrapped key of TC GAA.

Architectural Overview of TP-GAA

BSF Server
1. TP: Derives an application-specific symmetric key SK as follow: SK = KDF(MK, Rpub, NAF-I'd, B-TID).
2. BSF: Verifies SK, lifetime of SK, etc.
3. TP: Generates a new temporary asymmetric encryption key pair (T(public) and T(private)) and certify the public key T(public) with an identity of T(public) chosen by TP user, namely, TIDpub.
4. BSF: Derives SK = KDF(MK, Rpub, KIDpub(Tprivate) || Tpublic)IDpub.
5. BSF: Verifies SK = KDF(MK, Rpub, KIDpub(Tprivate) || Tpublic)IDpub.
6. BSF: Verifies Rpub, to ensure the message is fresh and verifies that the message was intended for BSF.
7. BSF: Assumes the signature from TP verifies correctly, the values of Rpub and TIDpub are expected, then BSF extracts T(public).
8. BSF: Generates a symmetric key SK as master session key, and sets lifetime of SK according to local policy.
9. BSF: Generates an identifier B-TID of MK which consists of Rpub and the domain name of BSF.
10. BSF: Generates an authenticated key agreement protocol.

Use of bootstrapped key

1. TP: Derives an application-specific symmetric key SK as follow: SK = KDF(MK, Rpub, NAF-I'd, B-TID) where KDF is a key derivation function. TIDpub is the identity of T(public), and NAF-I'd consists of the Fully Qualified Domain Name (FQDN) of the intended NAF and the identifier of the application protocol.
2. TP: TIDpub and msg. msg is the application request data secured using SK.
3. NAF: TP: B-TID and msg. NAF extracts SK and sets lifetime of SK according to local policy.
4. NAF: TP: SK = KDF(MK, Rpub, TIDpub, NAF-I'd), and sets lifetime of SK according to local policy.
5. NAF: BSF, lifetime of SK, etc.
6. NAF: Verifies the request using SK, if SK is valid.

Contact information

Name: Chunhua Chen
Address: Morea 106, Information Security Group, Royal Holloway, University of London, Egham, TW20 0EX, UK
Chunhua Chen is a PhD student under supervision of Prof. Shaohua Tang in School of Computer Science and Engineering, South China University of Technology. This work was performed during a visit to the Information Security Group at Royal Holloway, University of London, sponsored by the Chinese Scholarship Council.