IMAGE ORIGIN CLASSIFICATION BASED ON SOCIAL NETWORK PROVENANCE

ABSTRACT

Authenticated key exchange (AKE) is one of the most important applications in applied cryptography, where a user interacts with a server to set up a session key where pre-registered information (aka. authentication factor), such as a password or biometrics, of the user is stored. While single-factor AKE is widely used in practice, higher security concerns call for multi-factor AKE (MFAKE) schemes, e.g. combining both passwords and biometrics simultaneously. However, in some casually designed schemes, security is even weakened in the sense that leakage of one authentication factor will defeat the whole MFAKE protocol. Furthermore, an inevitable by-product arise that the usability of the protocol often drop greatly.

EXISTING SYSTEM

User authentication is a very important part for many information systems. In practice, it is often done via the following methods:

- **Password-Based Authentication:** Which is the most popular way, while quite insecure in some cases. E.g., in the Worst Password List compiled by Splash Data among 3.3 million passwords used for test, almost 20,000 were in fact ”123456”. The statistics show that most passwords in use are not so hard to guess.
- **Hardware-Based Authentication:** With storage space for long secret keys and computation power for authentication, hardware provides higher security than password. But if it was stolen or lost, which happens in daily life occasionally, the authentication fails completely.
- **Biometrics-Based Authentication:** Which utilizes the unique and life-long invariant property of the biometrics.

But it is not so reliable, e.g., biometric characteristics such as fingerprint can be easily “copied” without the awareness of the owner. Single-factor authentication only provides limited security, then combining these methods together is considered as a good way to achieve higher security. But, in fact, many exiting multi-factor authentication schemes are quite insecure. For instance, in practice, SMS-based two-factor authentication was widely adopted and has been used in many applications, e.g., Gmail. But in the latest draft of the Digital Authentication Guideline, NIST announced its opinion, using SMS is deprecated, and may no longer be allowed in future releases of this guidance.

Disadvantages

Efficiency. Complex protocol design should be avoided, which may cause expensive computation and communication costs.

Robustness. Whenever there is one factor uncorrupted, the authentication scheme should remain secure, which is a basic security requirement for multi-factor authentication.

Privacy. Biometric characteristics are acknowledged as one kind of privacy information, so which must be protected to avoid leakage. In addition, the leakage of biometric will not only break the security in the authentication, but also can lead to further social damage.

PROPOSED SYSTEM

In this paper, we presented a security model for multi-factor authenticated key exchange protocols that allows a significant amount of information leakage for the adversary. We formally proved the security and robustness of our scheme in the model, in the sense that as long as one authentication factor remains unknown, the adversary cannot have any information regarding the agreed session key, and cannot impersonate a client or a server. We also implemented the scheme with practical parameters on a smartphone, and the results have showed that our scheme is highly efficient.

Advantages

- Provably secure under the Decisional Diffie-Hellman (DDH) assumption in this model. Compared with the existing schemes, the proposed scheme achieves good balances between efficiency and security.
- It select several authentication factors, such as passwords, biometrics (e.g. fingerprint) and hardware with reasonable secure storage and computation ability (e.g. smartphone).

SOFTWARE REQUIREMENTS

Front-end	:	JSP
Back-End	:	MySQL
Server	:	Tomcat Server
OS	:	WINDOWS 7/above

HARDWARE REQUIREMENTS

PROCESSOR	:	CORE i3
RAM	:	512MB-2GB
HARD DISK	:	40GB