Research on Wireless Network Security Technology

Wen-jing Yang[1, a], Zhi-yuan Li[1,b] , Huai-jun Zhou[1,c] , Ran Li[1,a] and Hai-yan Zhao[1,a]

[1] Department of Network service, Xi’an Communication Institute, Xi’an 710106, China

[a]51375908@qq.com, [b]813086903@qq.com, [c]583822272@qq.com

Keywords: Wireless Networking, Security Technology, Privacy Protection

Abstract: With the popularization and application of wireless networks, people are dependent on wireless networks is increasing, at the same time the security of wireless networks has become the focus of attention. In this paper, a wireless network security methods and technology were more in-depth study, since the wireless network transmission medium inherent openness, limited wireless terminal resources, mobility and dynamic network topology wireless terminal, not only makes wireless network face greater security risks, so many security methods wired network environment. User authentication is one of the most important security services are dependent on it to some extent all the other security services. Design a user authentication scheme, effectively reducing the cost of communications and computing participants. Consider security user domain is proposed based on Trusted Mobile Platform (TMP), combined with the current mainstream smart phone hardware architecture, given the construction of smart phones mainstream processor-based, and discussed on this platform TPM method.

Introduction of Wireless Network Security

Wi-Fi in its ease of installation, flexibility and economic advantages of expanded freedom of users, broadening the user space, but this freedom and convenience also brings new challenges and threats. All present in the conventional wired network security risks still exist in the wireless network, and since the wireless network has the following features, security threats it faces more security problems caused by more complex.

Terminal mobility makes wireless network security management more difficult, we must consider the mobile terminal security management and location management in roaming and switching situations. The mobile terminal easily stolen and lost, the attacker can abuse the legal end and where the leak confidential data. On many occasions, wireless communication technologies require mobile terminals and wireless network synchronization, including clock synchronization, synchronization and hopping sequence confidential information synchronization. Existing mobile terminal operating system is not safe, the lack of integrity protection and improvement of the access control policy, likely to be eroded by a virus, Trojan or malicious code, resulting in a user's confidential information being leaked or tampered with [1].

Mobile terminal security risks and threats, with the advent of smart phones and PDA's, mobile computing and storage capacity of the terminal growing, services and applications that can handle more and more complex, while the security risks posed is also growing, specific performance is as follows: due to lost or stolen mobile terminal which caused leakage of confidential information, the attacker abusing others to enjoy the mobile terminal network service or attack. An attacker defraud legitimate users using the mobile terminal malicious engineered to intercept the user's personal information and sensitive data, such as a password or fingerprint. Wireless network must provide for user authentication to prevent counterfeiting attacks.

Trusted Mobile Platform TPM

Trusted Computing Platform by introducing a safe and reliable in the underlying hardware modules and combined chain of trust to pass the way to achieve. The starting point of the trust chain is the root of trust, namely the introduction of a hardware security module. Trusted Computing can be understood in several ways: user authentication, which is the user's trust; platform hardware and software configurations correctness, and reflects the confidence of the user platform operating environment: integrity and application legitimacy, trusted applications run; verifiability platform, refer to the network environment of mutual trust between the platforms [2].

Authentication: include mutual authentication of users and platforms, as well as mutual authentication between the mutual authentication platform internal platform processes. Integrity Check: Based on the main characteristics of the performance of security mechanisms for the Safe Boot (Trusted boot) and remote authentication. Domain isolation and access control technologies: the main use process isolation technology and joint access control policies. Protected Storage: Includes direct protection of confidential information stored in the TPM memory inside, based on the extended storage key data protection, as well as conditional parsing seal-based storage (seal storage) technology. Trusted Computing by adding TPM (Trusted Platform Model), CRTM (Core Root of Trusted Measurement) and Trusted I/O hardware environment to provide the following security mechanisms to improve the security of the terminal. Fig.1 shows the trusted mobile platform structural system.

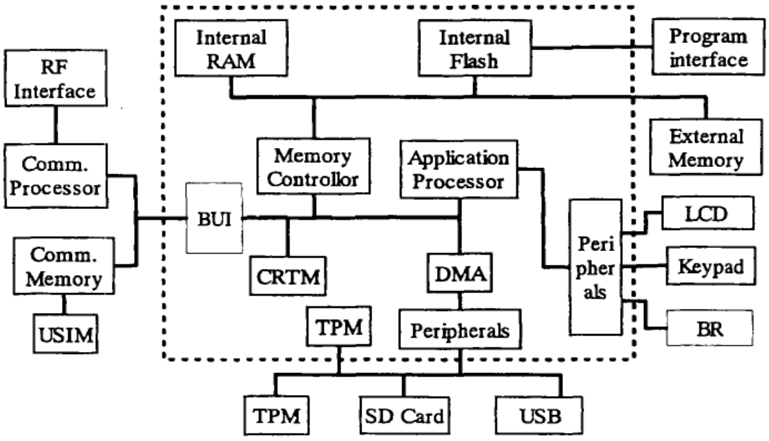

Fig. 1.The trusted mobile platform structural system

TPM is a core component of TMP, the main achievement of the following five areas: the use of random number generator provides an asymmetric key pair generation. Save private key and symmetric key, and complete the signature, public key encryption and symmetric key encryption features in its interior. PCR hash value stored configuration information to ensure the integrity of the platform and provides remote verification function. Storage platform certificate and apply for an identity certificate (Identity credential) with the certificate the remote authentication to ensure the privacy of internet identity. Initialization and management functions: allows the user the ability to configure the function, reset the chip and hold authority [3].

Wireless Network User Authentication

Wireless network of mobile devices gradually changed the way we live. In order so that people can network anywhere, anytime without having to limit the geographic coverage of the local network, you need to provide roaming services. A typical program includes three-way roaming: roaming user U, access to foreign servers and local servers, where U is the local server is H subscribers. When U is controlled in a foreign network, the roaming service assurance U to acquire their own subscription service through V. Roaming agreement in the user authentication phase, it may expose the identity of the account number and location information of the user, thus providing privacy roaming authentication technology is very necessary.

The wireless communication network, wireless LAN, and other network vehicle network can provide wireless access services. In order to overcome the limitations of the geographical coverage of each access point location and provides seamless access to services for the mobile node, using an efficient user authentication protocol is particularly important. Before the access network, MN to AS first registration and subscription services, and access to one AP, in order to access the network.

When the MN from the current AP (AP 1) to move to a new AP within) range, you need to perform user authentication on the AP2. User AP2 authentication reliability, denied access to any unauthorized user. Meanwhile, we need to establish keys between MN and AP2, in order to protect the confidentiality and integrity of communication contents [4]. Fig.2 shows the principles of wireless network user authentication.

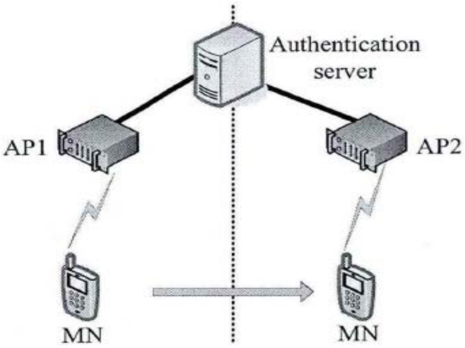

Fig. 2.The principles of wireless network user authentication

To prevent tampering and easy to manage password file, smart card-based password authentication for user authentication and session key establishment is one of the most simple and efficient way. To provide effective security, the use of digital signature technology in the user authentication is widely considered to be the most efficient way. The certificate must be sent along with the digital signature, a digital signature to authenticate each recipient each time to perform the signature verification operation two high consumption, because the certificate requires the same certification. In order to provide user anonymity, we propose a protocol based on the group signature. However, users need timely revocation list distributed to the entire network. In addition, in each of these agreements and the number of access requests delay revoked user authentication linear. Thus, when a large number of users have been revoked, the performance of these protocols will decline.

Wireless Network Protection Strategies

Due to the openness of wireless network transmission media, mobility and dynamic network topology wireless terminal and a wireless terminal computing power and storage capacity limitations, so many security programs and technical wired network environment can’t be directly applied to the wireless network, but also to implement safety programs increased the number of restrictions. Mobile Internet security policy will be based on mobile Internet architecture, business requirements, security threats and security needs analysis suggested that protection of mobile Internet architecture is based on the principles of security domain classification system covering infrastructure, network services, business applications overall security architecture. Fig.3 shows the divided view of the wireless network layer.

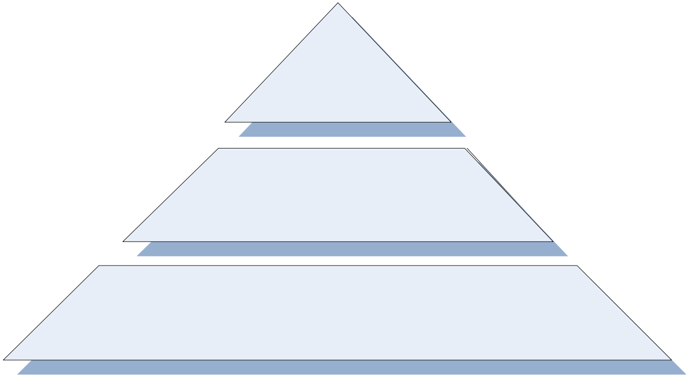

Fig. 3.The divided view of the wireless network layer

The Wireless Network security protection strategies will be used to monitor the precise protection technical route, bump cap Hua infrastructure layer, network service layer and application layer services, and research and validate key security technology. The mobile Internet is divided into basic equipment and facilities, network service level, the business application level. Eight security dimensions of analysis: controllability access, authentication of network integrity, non-repudiation, database confidentiality wins, secure communications, data, and service availability information privacy, and for safety analysis security architecture and design appropriate strategies [5].

Overall wireless network protection strategies include wireless network security policies are automatically audit, illegal invasion strategy, business security policy, security policy of false accounting. Automatically detect security inadequate security policies, automatic alarm; generate overall risk view of the mobile Internet security aspects. Full and enhance the mobile Internet security level to prevent security short board. Perceived attacks on mobile Internet and can identify, differentiate worm and hacker attacks and network detection tool: a probe centralized storage device to upload logs and correlation analysis; research honeypots own security technology, improve the overall mobile Internet security capabilities.

Conclusions

The advent of wireless networks to communicate with the perception of humanity from the shackles of time, place and objects, greatly improved the quality of human life and work. With the increasing complexity of wireless network environment, trust relationships between network entities, safety, security and non-repudiation services security system scalability wired link had to be reconsidered. In this paper, privacy protection, user authentication, trust management and secure communications infrastructure and other key technology research and exploration, creatively put forward a series of theories, designed and implemented a number of security programs. Based on the built hardware TPM programs at the expense of the cost of universal, we received the highest operation speed, minimum communication time and maximum security. We fully consider the mobile Internet network security requirements and security threats, give practical technical solutions.

References

[1] R Zhang, Y Zhang, and K. Ren. DP2AC: Distributed privacy-preserving access control in sensor networks. In Proceedings of the IEEE INFOCOM, pages 1251- 1259, 2009.

[2] M. Li, W. Lou, and K. Ren. Data security and privacy in wireless body area networks. Communications, 17(1):51-58, 2010.

[3] Leavitt N, Internet Security under Attack: The Undermining of Digital Certificates [J], computer, 2011, Volume 44, Issue 12, PP 17-20.

[4] Y.Ma, T. Houghton, A. Cruden and D. Infield. Modeling the Benefits of Vehicle to Grid Technology to a Power System. IEEE Transactions on Power Systems, 27(2):1012-1020, 2012.

[5] D. He, C. Chen, S. Chan, and J. Bu. Di-Code: DoS-resistant and distributed code dissemination in wireless sensor networks. IEEE Communications Magazine, Feb. 2013.