The introduction of Dissertation

At current age, overload notifications such as Facebook messages, text messages, emails, etc influence and detract people to a great extend. The general architecture of the dissertation is made up of three parts as followed.

Meta-date in the messages: Different type of messages can be sent to users randomly by second. There exist many security concerns such as the authentication, data integrity of pushed messages.

Context Transformation: these received needs to be delivered or pended depended on context like time, place, related people and the relationship. It can have security threats in the transmission and fake context information.

Last but not least, the user is involved into decide the status of messages implicitly and explicitly. Personal modeling comes from personal interests and habits. The major security consideration lies in user authentication and encryption, considering the attacks like sniffing password and phishing.

User authentication

Username and password is required when logging into a local-area network (LAN). The potential stacks are sniffing passwords by trying all possible keys or attacking database which contains plaintext. One-way Hash functions like MDx, SHA family to encrypt password and username can be adopted in this case. The benefits of SHA256 are that the hash size is 256bits, making hard to try every possible keys and collisions is small. In addition, there is another attack when the user is given a fake link with JavaScript. The user's password can be compromised. In this case, browser-based security must be plugged in to make protection.

Furthermore, user's access control needs to take another consideration. The system is rule-based system, user must not be granted to transform the system rules. However, it is possible that attacker sniffed the sys admins' password and enabled all the rules. The approach to resolve this attack is to authenticate users and then grant the access. Both shared keys cryptography for authentication (AES) and public key (RSA and Elliptic Curve cryptography) with digital certificates are acceptable.

Username and password is required when logging into a local-area network (LAN) and the use of digital certificates when sending or receiving secure messages over the internet.

Context security

Most context data are transferred to the system via sensors or other devices. The communication between devices is out of scope of dissertation, because it assumed that the data has been collected to the system. Similarly, personal relationship and environment situation is out of scope. The potential attacks, like making fake context are out of scope. But if attackers try to push messages by creating noise context, the system has many methods and filter algorithms to determine if the message should be pended or delivered.

However, for security concerns, some sensitive information like meeting notes, personal relationship must follow the policy and keep private to avoid eavesdropping. CBC block encryption can be adopted in this case.

Message

Messages like emails are sent from wide area network to local area network. Even though firewall can be configured to filter spam messages, 1.many messages have no authentication. 2. Some messages from social media can be HTTP-based, so it can pass firewall without barrier.3. some messages have been altered. The part of extranet is out of scope because much encryption and authentication should be handled by mail server or web server. It is highly possible that the messages passed through firewall are replayed, inserted or modified. It is encourage that messages are encrypted and transmission adopts SSL or TSL which protects connection based on PKI with MAC.

Similarly, email in wide area network lacks support for transport layer security and insufficient application layer security. Some emails replace SMTP with S/MIME to process end-to-end security or other transport layer authentications. Also, some mail server refuses to receive emails due to technical problem, which is out of scope.

In a word, the risk of messages from wide area network is of no authentication, fake messages, fake sources, compromised content, overflowed messages, etc. The approach is: configure firewall, filter by sensitive words, digital certificates and authenticate addressers.

Internal network is also unsafe. Messages can be replayed on the way to users. The risk can be solved by setting TTL or timestamp. If number is abnormal, the message can be replayed. Moreover, messages can be eavesdropped, altered or inserted in the transmission. it is encouraged to use TSL to make encryption, MAC to ensure data integrity. It is proved that encrypt-then-MAC is the safest approach.
Symmetric encryption can be adopted if there is enough network speed. Some symmetric encryption like RC-4 and Data encryption standard (DES) has been widely used. Even though asymmetric encryption is secure without shared keys, it requires good network performance. Diffie-Hellman(DH) and Shamir Adlemen (RSA) are popular asymmetric cryptosystems.

Denial of service

A set of ways can be adopted to avoid denial of service. First user logs in, authentication, and granted access. Then, messages are required digital certificates, correct MAC. And then, spam filtering based on sensitive words, and blackmail filtering. But it can happen the context is comprised and attacker still changed the policy by obtaining the access.

Meanwhile, it can have blind copies attack when users reply the messages. Addresses tjat do not appear in the message headers may appear in the RCPT commands. The approach is to avoid copying the full set of RCPT command to headers and users should get notice by “bcc”.

Last security consideration lies in incorrect time. In the system, the sent time and location of messages is

important to determine if the message needs delivering right now or pending. However, it is difficult for the system to take action. It is out of scope that a mail server or web server should check the time and location when receiving the messages. The question can be more difficult in distributed system.

Secure transmission. Inside of internal network, there are possibilities that the messages can be intercepted without the sender or receiver ever knowing the data was compromised.

[1] E. Rescorla, B. Korver. July, 2003.Guidelines for Writing RPC Text on Security Considerations
[2] Anon, 2015.[online] Available at: Http://www.ietf.org/html.charters/ipsec-charter.html.[accessed 23 Mar. 2015]