International Journal of Sciences

Research Article Volume 11 – September 2022 (09)

Introduction to Protocol Building Blocks in Cryptography

Maher Ali Rusho✍

Abstract: The Whole point of cryptography is to solve problems. It solves problems that involve secrecy, authentication ,integrity and dishonest people .A protocol Is a series of steps ,involving two or more parties designed to accomplish a task. A series of steps means that the protocol has a sequence, from start to finish. Analyzing stream ciphers is often easier than analyzing block ciphers. For example, one important metric used to analyze LFSR-based generators is linear complexity, or linear span. This is defined as the length, n, of the shortest LFSR that can mimic the generator output. Any sequence generated by a finite-state machine over a finite field has a finite linear complexity [1006]. Linear complexity is important because a simple algorithm, called the Berlekamp-Massey algorithm, can generate this LFSR after examining only 2n bits of the keystream [1005]. Once you've generated this LFSR, you've broken the stream cipher.

Keyword: Adjudicated Protocols,Self enforceing portals, One Way function, Massage Authentication Code (MAC), Publich Key

Dedicated to:
My Father Dr.prof. Mohammad Ali
My Mother and Teacher of all time Dr. Ruma Ali
My 2'nd Father: Engr.Ali Ahmed Jewel
My 2'nd mother and teacher of my early age Surraya Ahmed

Protocols have other characteristics as well
-Everyone in the protocol Must know the protocol and all of the steps to follow in advance
-Everyone involved in the protocol must agree to follow it.
The protocol must be complete there must be a specified action for every possible situation

Protocols provide rules that define how a message is transmitted across a network. Implementation requirements such as electronic and bandwidth details for data communication are specified by standards. Operating systems are not specified by protocols, but will implement protocols. Protocols determine how and when to send a message but they do not control the contents of a message. The paper is basically a sequence of synopsis of pure and applied cryptography Research module.

The players in cryptography are aid of several people
A arbiter is a disinterested third party trusted to complete a protocol

Adjudicated Protocol:

- Rely on the parties to be honest
- If someone suspect cheating, evidence exist so that a third party could determine if somebody cheated
- We would also like to know who the cheater are
- Detects cheating instead of preventing it

Self enforcing protocols:

- Protocol itself guarantees fairness
    - No arbitrator is necessary to complete the protocol
    - No adjudicator is required to resolve disputes
- The protocol is designed so there cannot be disputes
- Cheating can be detected, and the protocol aborted
- Self enforcing protocols does not exist for every situation

Attacks against Protocols

- Cryptographic attacks can be directed against the
    - Cryptographic algorithms used in protocols
    - Cryptographic techniques and implementations
    - Protocols them self
- When studying protocols we will assume the algorithms and implementations are secure

Attacks against Protocols

- Passive attacks
    - Someone not involved in the protocol tries to eavesdrop on some or all of the protocol
    - Hard to detect, so we try to prevent eavesdropping instead
- Active attacks
    - An attacker could try to alter the protocol to his own advantage

Published at: http://www.ijsciences.com/pub/issue/2022-09/
DOI: 10.18483/ijSci.2612; Online ISSN: 2305-3925; Print ISSN: 2410-4477

✍ ☎ Maher Ali Rusho (Correspondence)
+

    - Pretend to be someone else
    - Alter messages, introduce new messages, delete existing messages, replay old messages
- Cheaters
    - Parties involved in the protocol
    - Passive cheaters
        - Follows the protocol but try to obtain more information
    - Active cheaters
        - Disrupt the protocol in progress in order to cheat

Key Exchange with Symmetric Cryptography

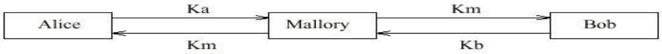
- Assumes Alice and Bob share a secret key with the Key Distribution Center, the KDC (Trent in our protocol)
    1. Alice calls Trent and request a session key to communicate with Bob
    2. Trent generates a random session key. He encrypts to copies of it; one with Alice's key and one with Bob's key. He send both copies to Alice
    3. Alice decrypts her copy of the session key
    4. Alice sends bob his copy of the session key
    5. Bob decrypts his copy of the session key
    6. Both Alice and Bob uses the session key to communicate with each other
- Relies on the absolute security of Trent
- If Mallory corrupts Trent, the whole network is compromised
- Trent is also a bottleneck

Key Exchange with Public-Key Cryptography

- Protocol:
    7. Alice gets Bob's public key from the KDC
    8. Alice generates a random session key, encrypts it with Bob's public key and sends it to Bob
    9. Bob decrypt the key with his private key
    10. Both Alice and Bob uses the session key to communicate with each other

Man-in-the-Middle attack

- Mallory can imitate Bob when talking to Alice and imitate Alice when talking to Bob
    11. Alice sends Bob her public key. Mallory intercepts this key and sends Bob his own public key
    12. Bob sends Alice his public key. Mallory intercepts this key and sends Alice his own public key
    13. When Alice sends a message to Bob, encrypted in "Bob's" public key, Mallory intercepts it. Since this message is really encrypted with his own public key, he decrypts it with his private key, re-encrypts it with Bob's public key, and sends it on to Bob
    14. When Bob sends a message to Alice, encrypted in "Alice's" public key, Mallory intercepts it. Since this message is really encrypted with his own public key, he decrypts it with his private key, re-encrypts it with Alice's public key, and sends it on to Alice
- Even if the keys are stored in a database this attack will work, since Mallory can intercept those messages too



Interlock Protocol

The Interlock protocol works roughly as follows:

1. Alice encrypts her message with Bob's key, then sends half her encrypted message to Bob.
2. Bob encrypts his message with Alice's key and sends half of his encrypted message to Alice.
3. Alice then sends the other half of her message to Bob, who sends the other half of his.

The strength of the protocol lies in the fact that half of an encrypted message cannot be decrypted. Thus, if Mallory begins her attack and intercepts Bob and Alice's keys, Mallory will be unable to decrypt Alice's half-message (encrypted using her key) and re-encrypt it using Bob's key. She must wait until both halves of the message have been received to read it, and can only succeed in duping one of the parties if she composes a completely new message.

The Bellovin/Merritt Attack[edit]

Davies and Price proposed the use of the Interlock Protocol for authentication in a book titled Security for Computer Networks.[2] But an attack on this was described by Steven M. Bellovin & Michael Merritt.[3] A subsequent refinement was proposed by Ellison.[4]

The Bellovin/Merritt attack entails composing a fake message to send to the first party. Passwords may be sent using the Interlock Protocol between A and B as follows:

```
 A            B
Ea,b(Pa)<1>------->
<-------Ea,b(Pb)<1>
Ea,b(Pa)<2>------->
<-------Ea,b(Pb)<2>
```

where Ea,b(M) is message M encrypted with the key derived from the Diffie–Hellman exchange between A and B, <1>/<2> denote first and second halves, and Pa/Pb are the passwords of A and B.

An attacker, Z, could send half of a bogus message—P?--to elicit Pa from A:

```
A             Z             B
Ea,z(Pa)<1>------>
<------Ea,z(P?)<1>
Ea,z(Pa)<2>------>
              Ez,b(Pa)<1>------>
              <------Ez,b(Pb)<1>
              Ez,b(Pa)<2>------>
              <------Ez,b(Pb)<2>
```

At this point, Z has compromised both Pa and Pb. The attack can be defeated by verifying the passwords in parts, so that when Ea,z(P?)<1> is sent, it is known to be invalid and Ea,z(Pa)<2> is never sent (suggested by Davies). However, this does not work when the passwords are hashed, since half of a hash is useless, according to Bellovin.[3] There are also several other methods proposed in,[5][6][7][8] including using a shared secret in addition to the password. The forced-latency enhancement can also prevent certain attacks.

Wireless sensor networks (WSNs) have been vastly employed in the collection and transmission of data via wireless networks. This type of network is nowadays used in many applications for surveillance activities in various environments due to its low cost and easy communications. In these networks, the sensors use a limited power source which after its depletion, since it is non-renewable, network lifetime ends. Due to the weaknesses in sensor nodes, they are vulnerable to many threats. One notable attack threating WSN is Denial of Sleep (DoS). DoS attacks denotes the loss of energy in these sensors by keeping the nodes from going into sleep and energy-saving mode. In this paper, the Abnormal Sensor Detection Accuracy (ASDA-RSA) method is utilized to counteract DoS attacks to reducing the amount of energy consumed. The ASDA-RSA schema in this paper consists of two phases to enhancement security in the WSNs. In the first phase, a clustering approach based on energy and distance is used to select the proper cluster head and in the second phase, the RSA cryptography algorithm and interlock protocol are used here along with an authentication method, to prevent DoS attacks.

Conclusion:

Cryptographic protocols provide secure connections, enabling two parties to communicate with privacy and data integrity. The Transport Layer Security (TLS) protocol evolved from that of the Secure Sockets Layer (SSL). IBM® MQ supports TLS.

The primary goals of both protocols is to provide confidentiality, (sometimes referred to as *privacy*), data integrity, identification, and authentication using digital certificates.

Although the two protocols are similar, the differences are sufficiently significant that SSL 3.0 and the various versions of TLS do not interoperate.

Resources

1. https://www.ibm.com/docs/en/ibm-mq/9.0?topic=mechanisms-cryptographic-security-protocols-tls
2. https://onlinelibrary.wiley.com/doi/10.1002/dac.4234
3. https://en.wikipedia.org/wiki/Interlock_protocol
4. http://www.quadibloc.com/crypto/mi060709.htm
5. http://www.sm.luth.se/csee/courses/smd/102/lek5/lek5.html
6. https://ccna7.org/what-is-the-purpose-of-protocols-in-data-communications/
7. Book Of Applied Cryptography Second Edition By Bruce Schneir