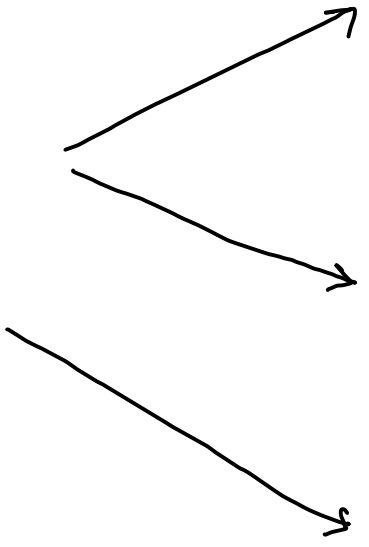
Authentication Protocols

1. One Way Authentication.

2. Mutual Authentication.



Authentication Protocols

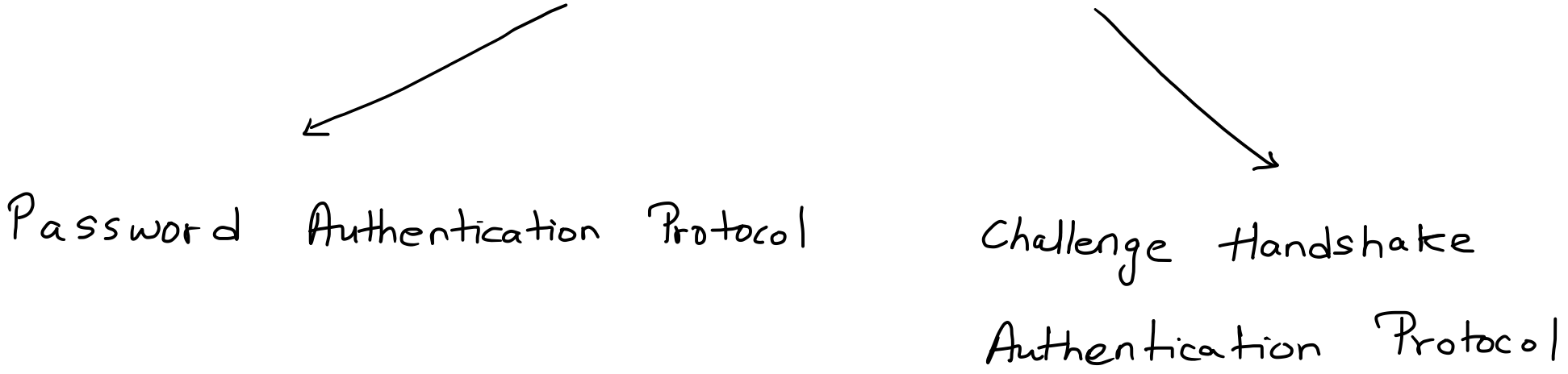
1. One Way Authentication.

This is required when sender and receiver are not in communication at the same time.

Eg. Email Messages

Authentication Protocols

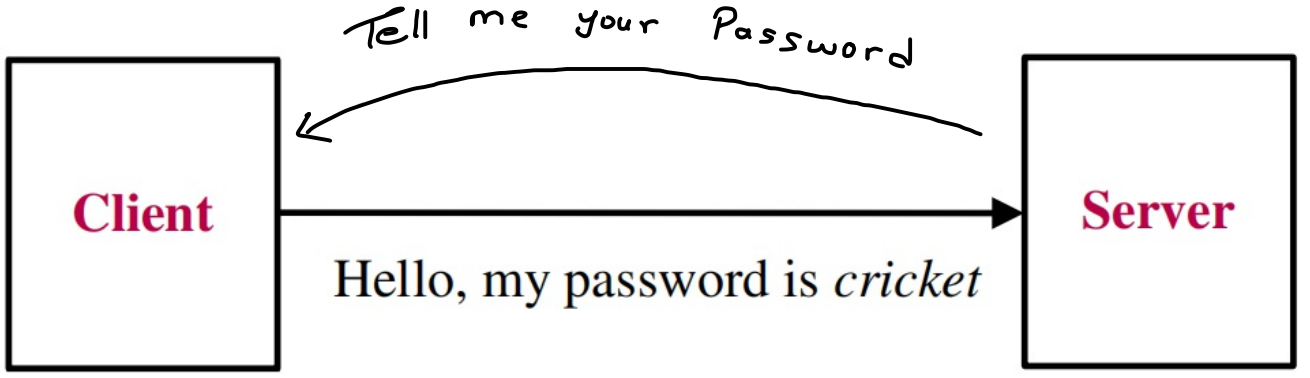
1. One Way Authentication.



Authentication Protocols

1. One Way Authentication.

Password Authentication Protocol

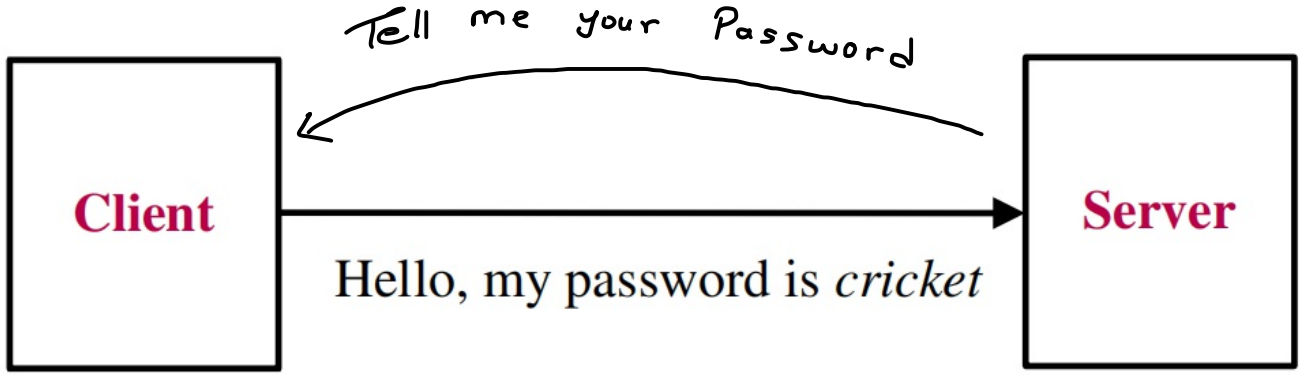


Authentication Protocols

1. One Way Authentication.

Not Secure , as Username and Password are usually sent in cleartext.

Password Authentication Protocol

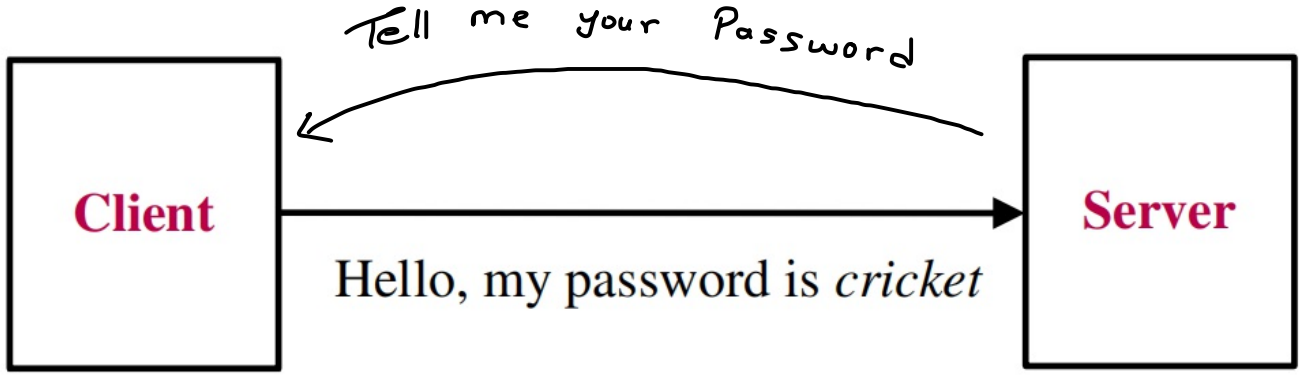


Authentication Protocols

1. One Way Authentication.

Not Secure , as Username and Password are usually sent in cleartext.

Password Authentication Protocol



Vulnerable to Username and Password Guessing

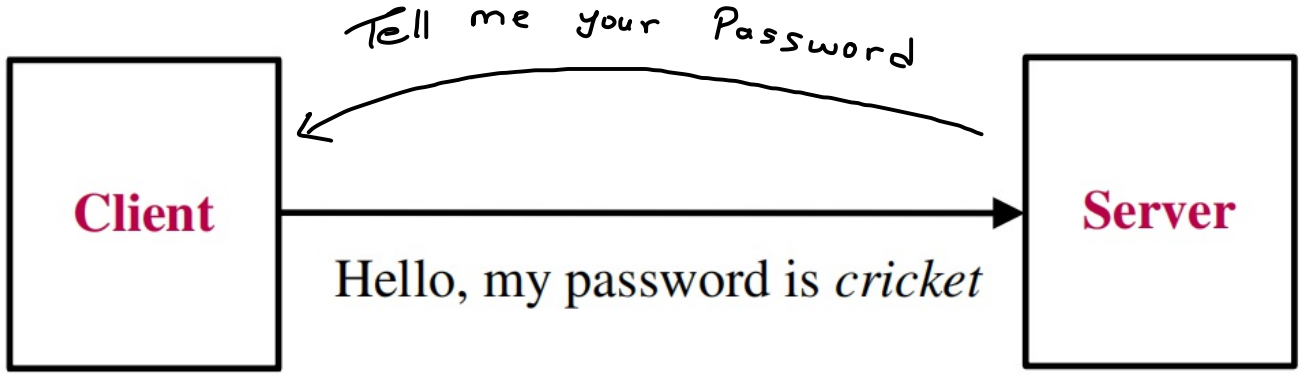
Authentication Protocols

1. One Way Authentication.

Not Secure , as Username and Password are usually sent in cleartext.

MiTM Attacks are easily possible

Password Authentication Protocol



Vulnerable to Username and Password Guessing

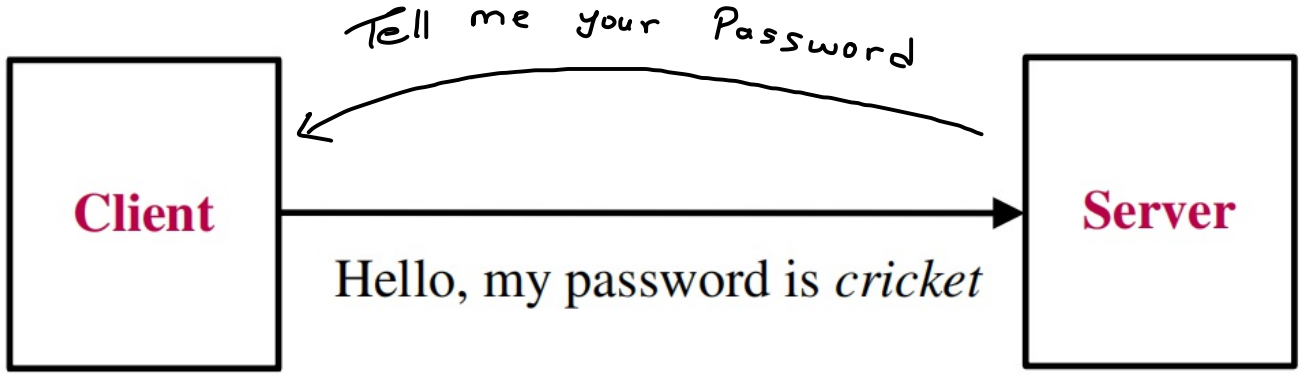
Authentication Protocols

1. One Way Authentication.

Not Secure , as Username and Password are usually sent in cleartext.

MiTM Attacks are easily possible

Password Authentication Protocol



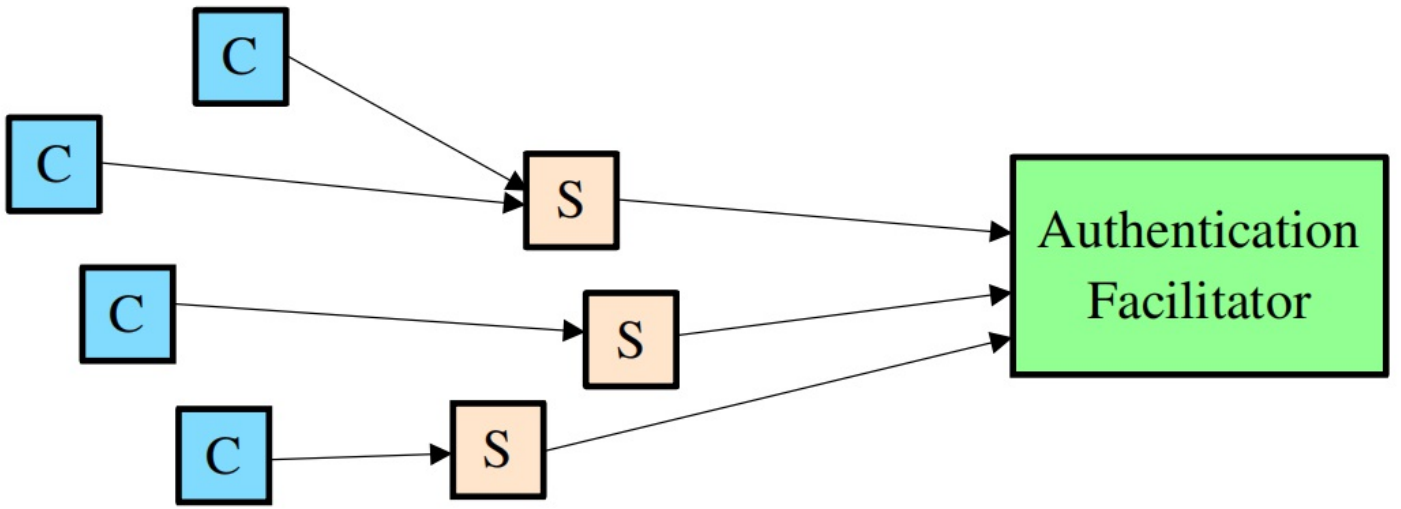
Vulnerable to Username and Password Guessing

Credential sharing is possible

Authentication Protocols

1. One Way Authentication.

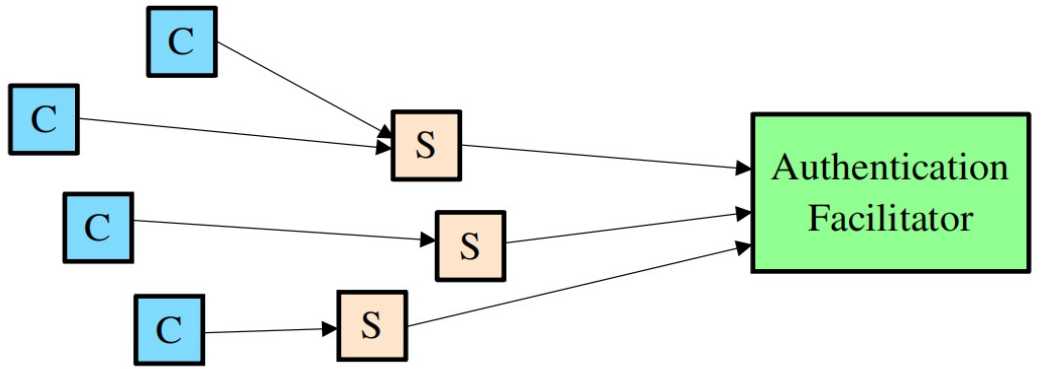
Challenge Handshake Authentication Protocol



Authentication Protocols

1. One Way Authentication.

Challenge Handshake Authentication Protocol



How to store password information: Cannot just store the password as that is too vulnerable. Perhaps use a hash of the password or encrypt.

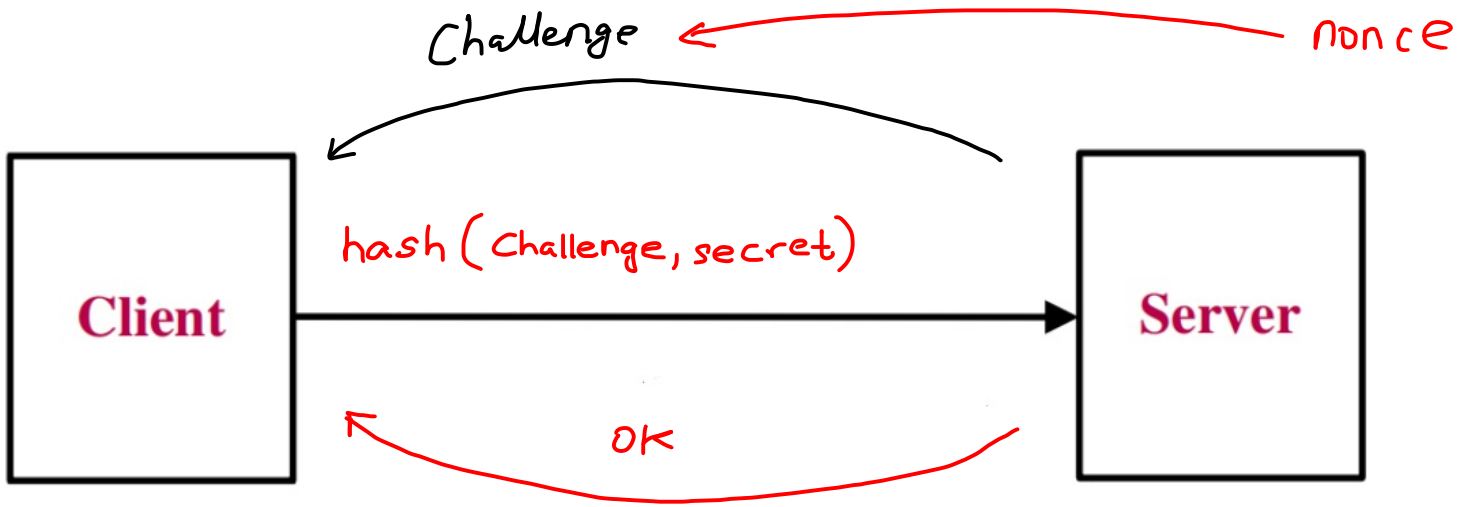
Should the hash be on every machine client accesses or on one?

If on one, server authenticates the storage node or authentication facilitator

Authentication Protocols

1. One Way Authentication.

Challenge Handshake Authentication Protocol



Authentication Protocols

2. Mutual Authentication.