PA2 Submission Report

HARSHIT GARG 1004422
MIHIR CHHIBER 1004662

Question: Fig. 1 Below gives the basis of a possible protocol. However, there's some problems with the protocol. What is/are the problems? Explain ONE problem (security vulnerability) in your handout for submission and give a fix for that problem you described in your implementation. Take note of the line numbers where you implement this fix. This will be handy for checkoff?

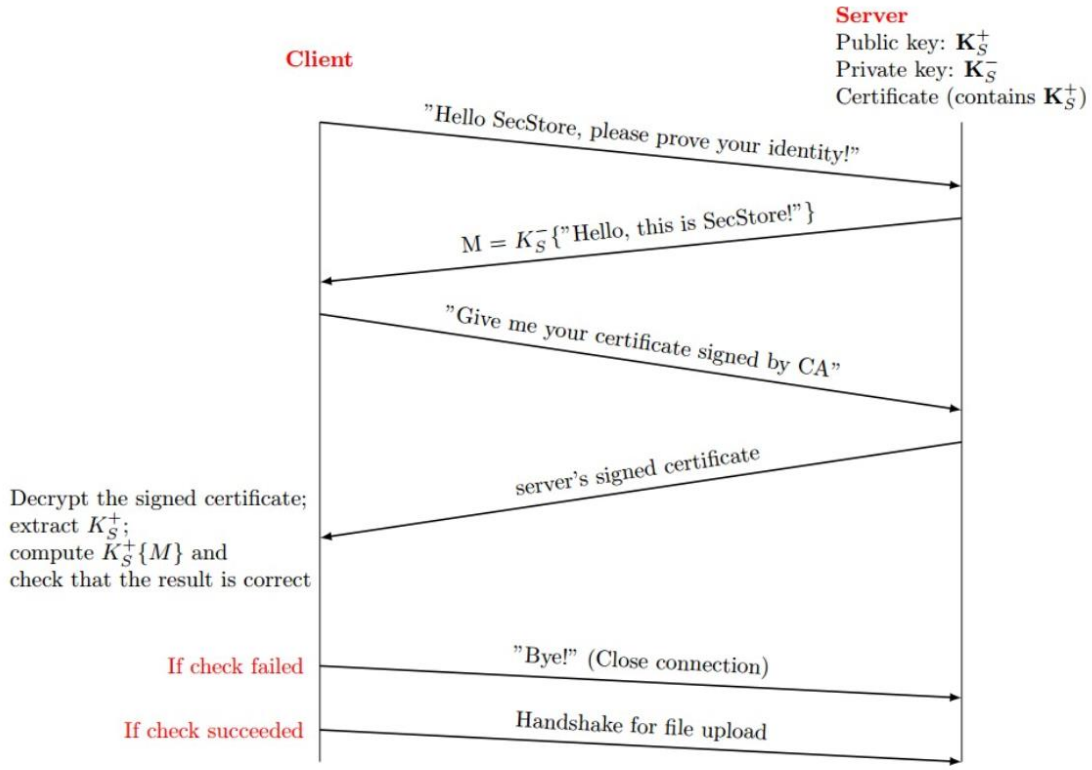


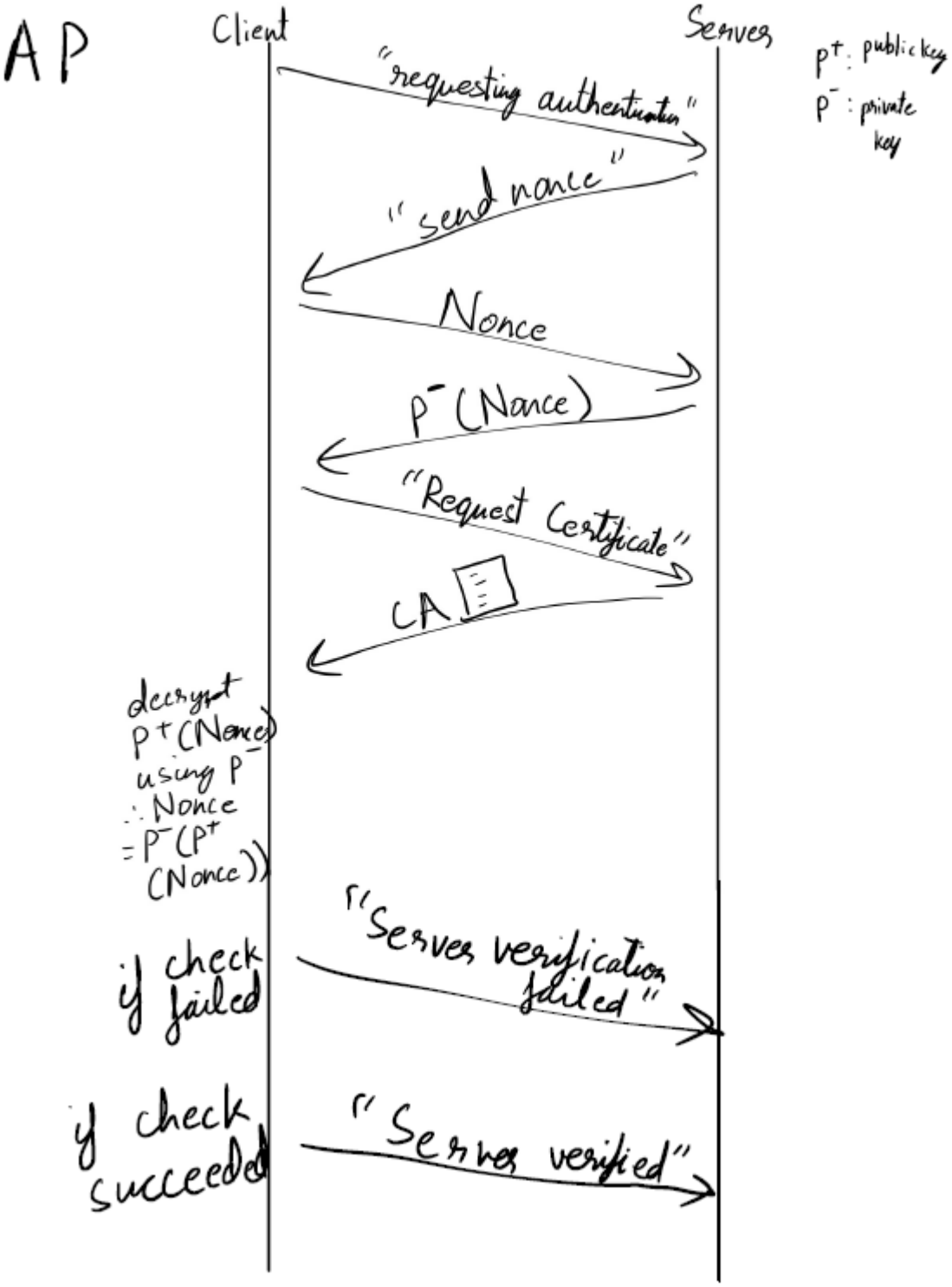
Fig. 1: Basis of Authentication Protocol

Solution: The original AP Protocol given is highly vulnerable to a replay attack, therefore any intermediate can access the encrypted message and spook the identity of the server by sending it to the client. To avoid this problem, we need to use a nonce that is generated by the client at the start of the connection, sent to server, and the server must encrypt the nonce using its private key and send it to client. The server sends it's CA which is used to verify server's identity and to get the public key of the server which is used to check if the nonce is valid. Since nonce is arbitrary numbers/ data generated randomly, this makes the connection unique therefore the integrity of the connection between the two is ensured making replay attack redundant.

PA2 Submission Report

HARSHIT GARG 1004422
MIHIR CHHIBER 1004662

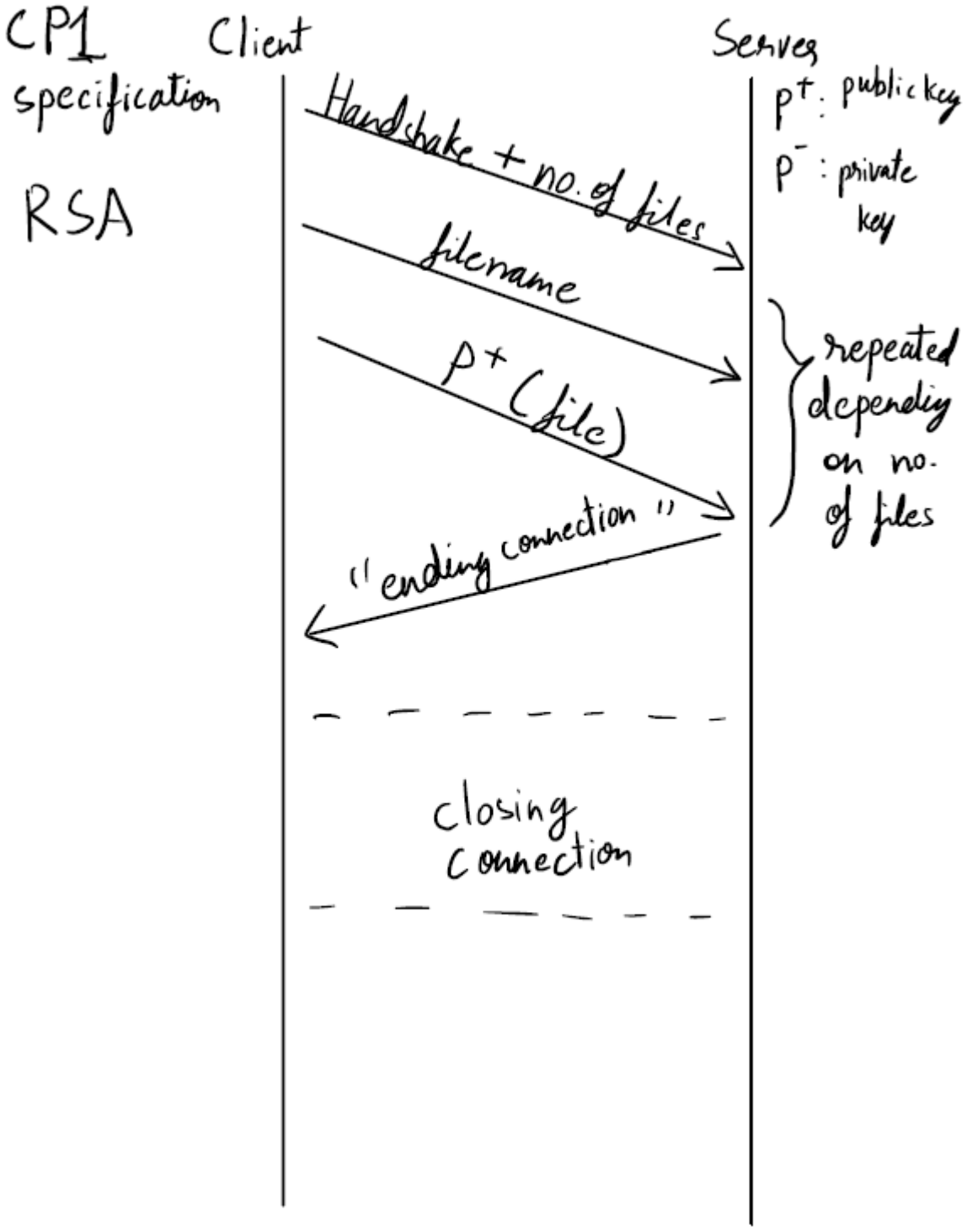
AP SPACE TIME DIAGRAM



PA2 Submission Report

HARSHIT GARG 1004422
MIHIR CHHIBER 1004662

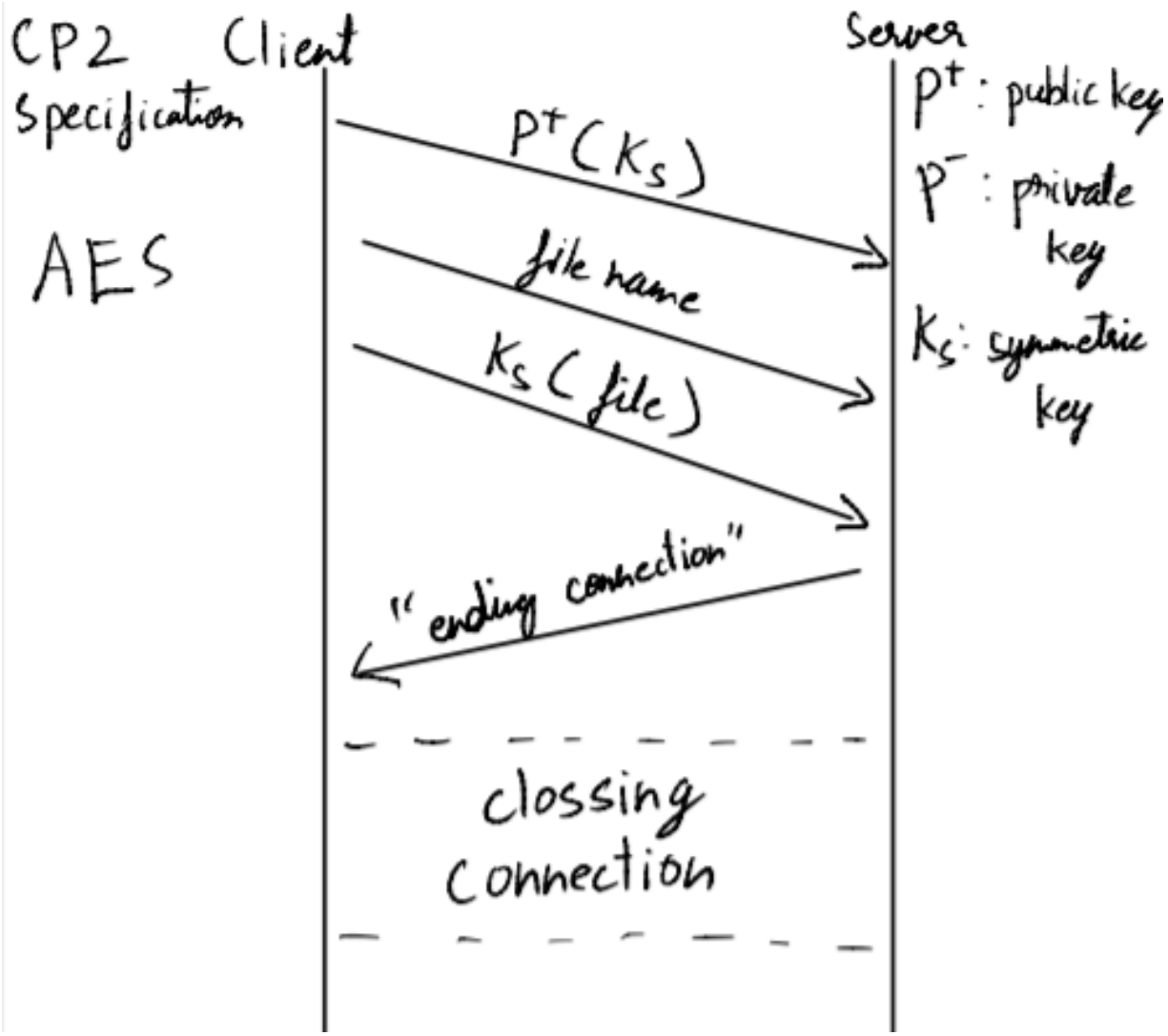
CP1 SPACE TIME DIAGRAM



PA2 Submission Report

HARSHIT GARG 1004422
MIHIR CHHIBER 1004662

CP2 SPACE TIME DIAGRAM



PA2 Submission Report

HARSHIT GARG 1004422
MIHIR CHHIBER 1004662

THROUGHPUT COMPARISON TABLE

File Name	Size(kb)	CP1 Time(ms)	CP1 Throughput(kb/ms)	CP2 time(ms)	CP2 Throughput(kb/ms)
100.txt	5	2089.7214	0.002392663	4.2169	1.185705139
200.txt	9	2094.124	0.00429774	5.29	1.701323251
500.txt	23	2155.603	0.010669868	3.9792	5.780056293
1000.txt	45	2192.3512	0.020525908	3.8245	11.76624395
5000.txt	225	2582.7491	0.087116476	6.0844	36.97981724
10000.txt	450	3019.6328	0.149024742	4.0215	111.8985453
50000.txt	2,247	6645.9085	0.338102759	19.0885	117.7148545
100000.txt	4493	10954.986	0.410132884	35.6931	125.8786712
1.mp3	121,972	243897.6663	0.500094986	941.3418	129.572489

CHART