

COMP3052.SEC Computer Security

Session 02: Motivating Example



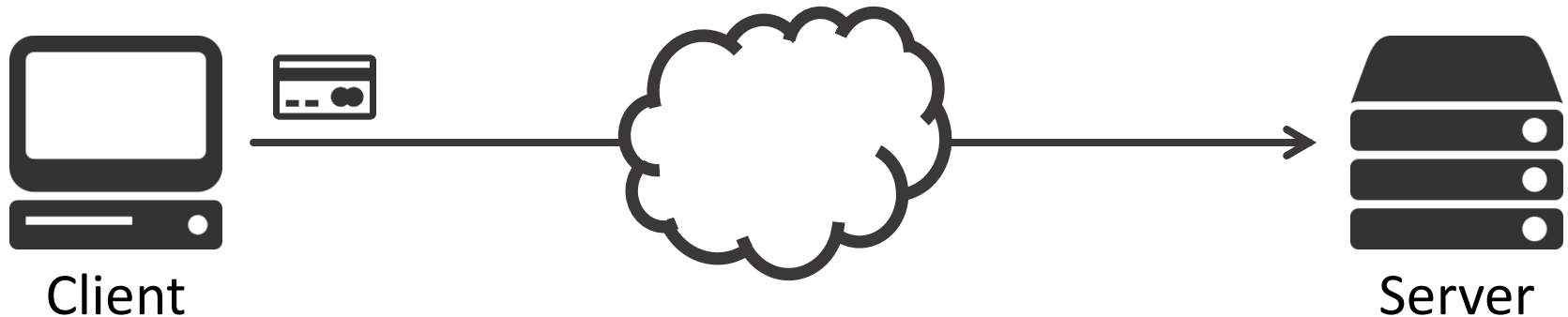
Acknowledgements

- Some of the materials we use this semester may come directly from previous teachers of this module, and other sources ...
- Thank you to (amongst others):
 - Michel Valstar, Milena Radenkovic, Mike Pound, Dave Towey,...

Who needs security anyway?

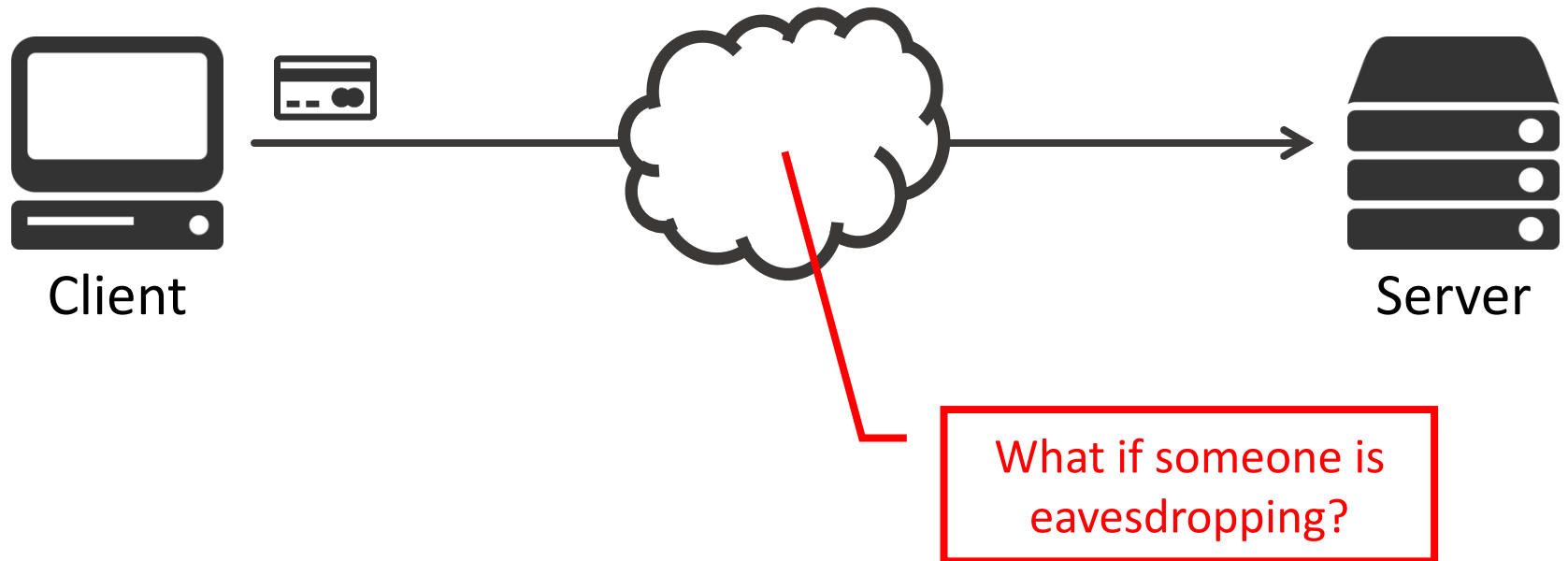
Who needs security anyway?

- People buy things online using card details all the time

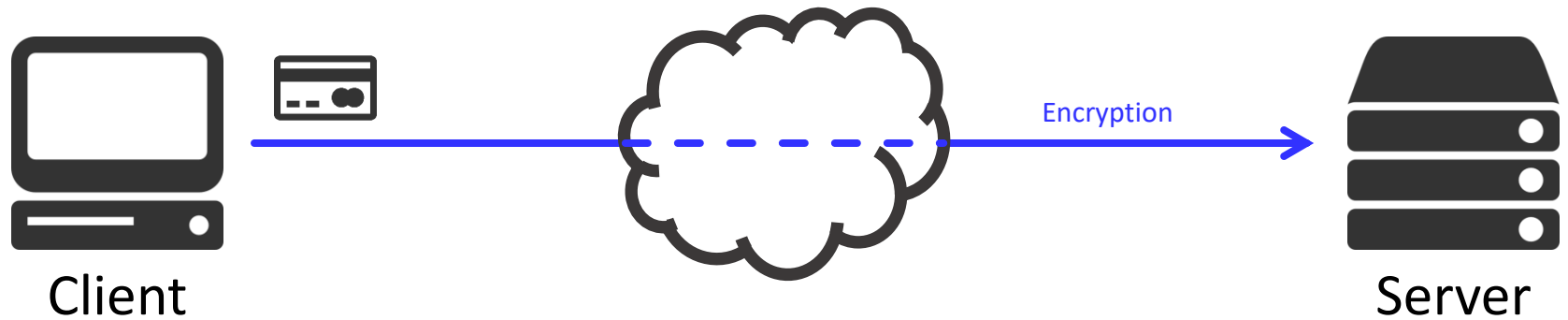


- What are the things that could go wrong here?

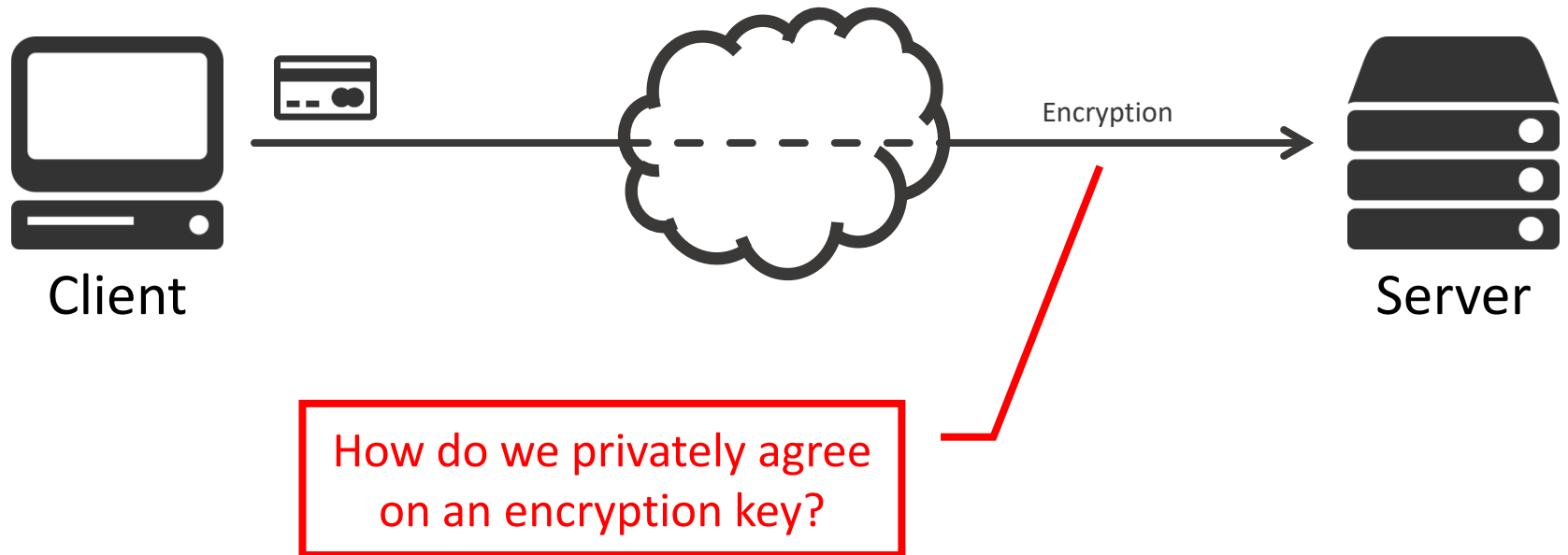
Eavesdropping



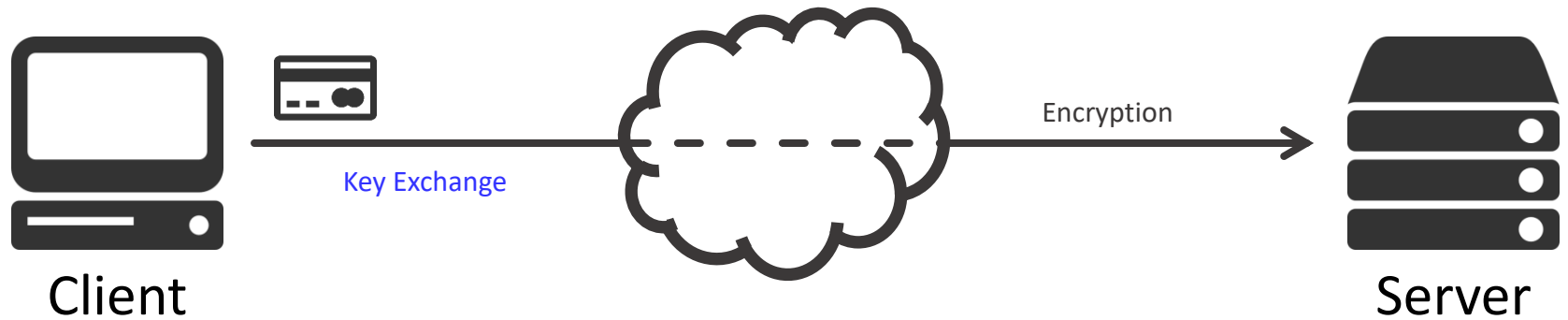
HTTPS / TLS



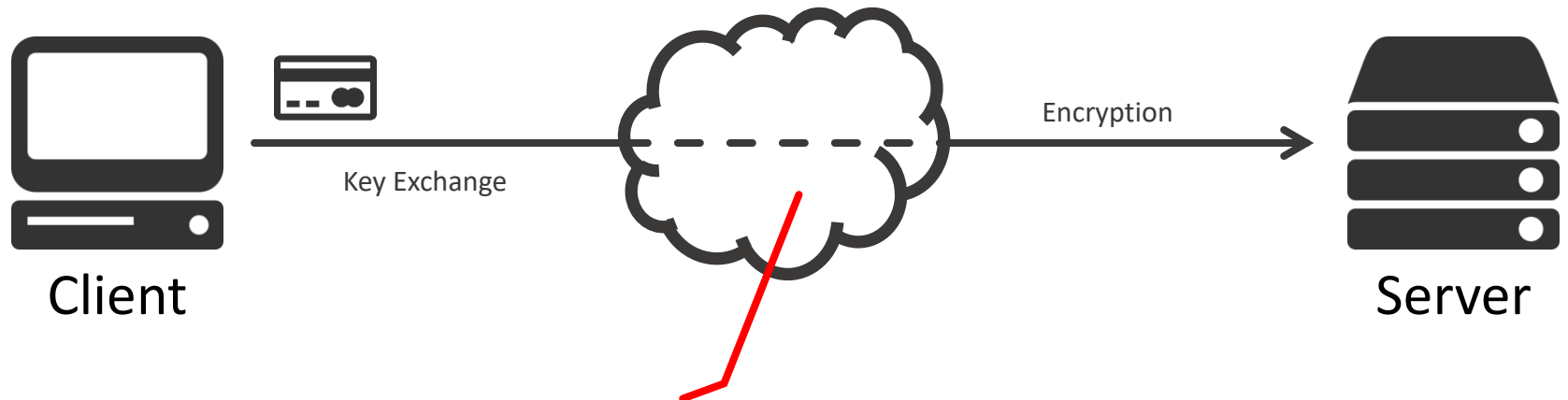
Shared Secrets



Shared Secrets

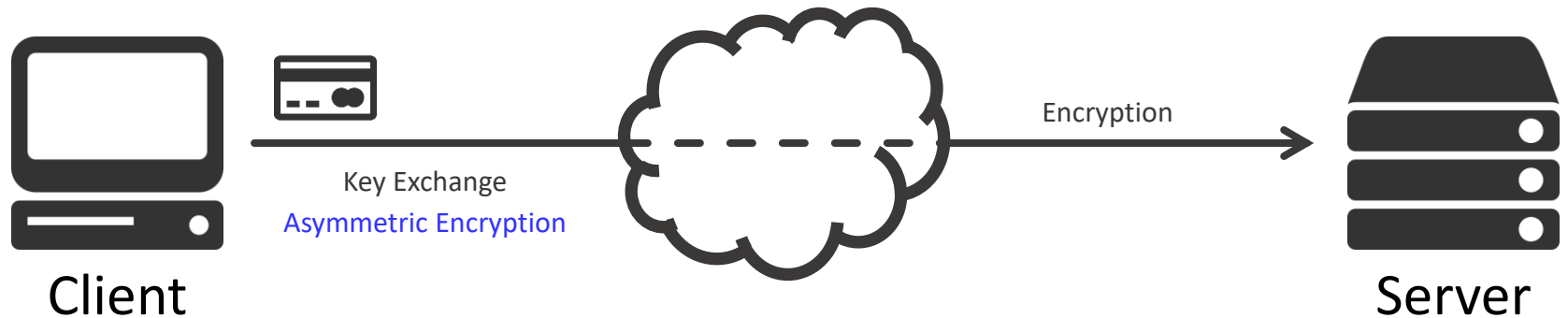


Attack Vectors

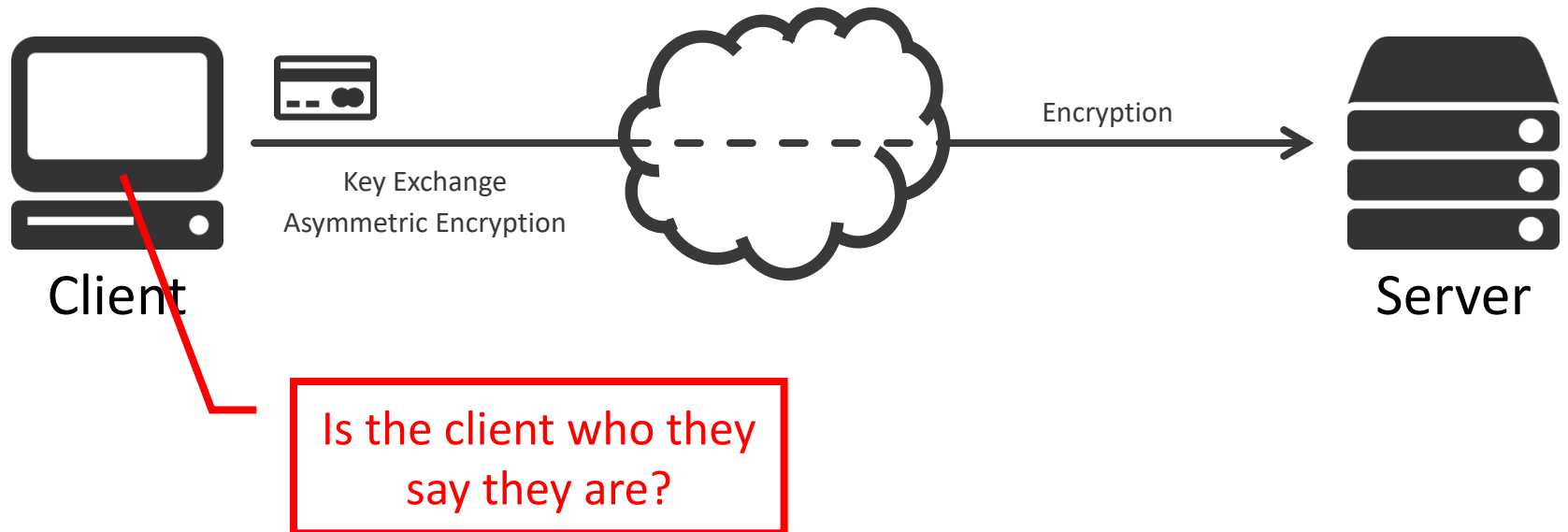


Can a man-in-the-middle
hijack this session?

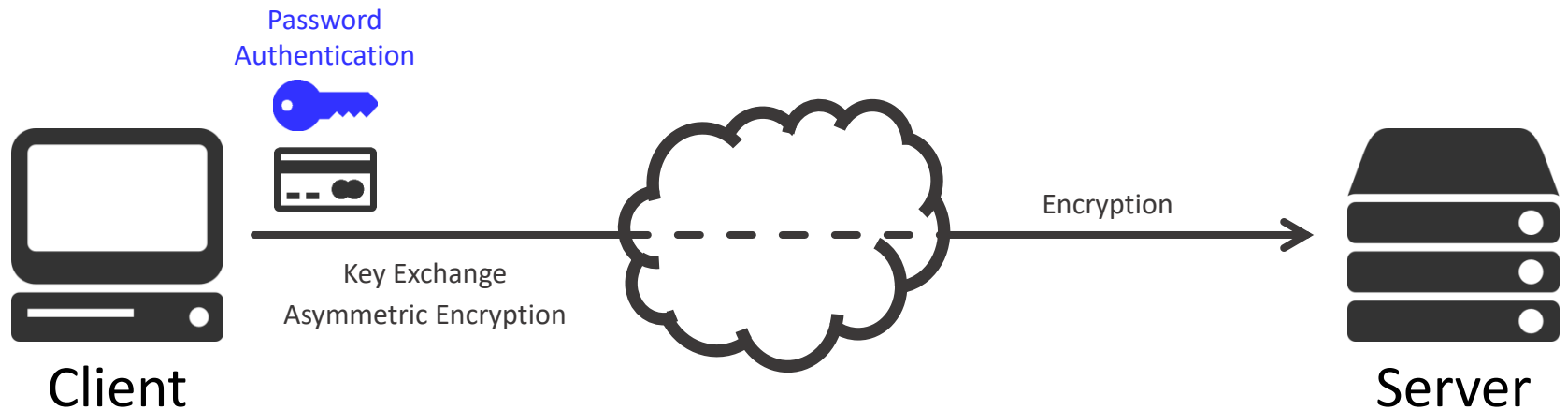
Public-key Encryption



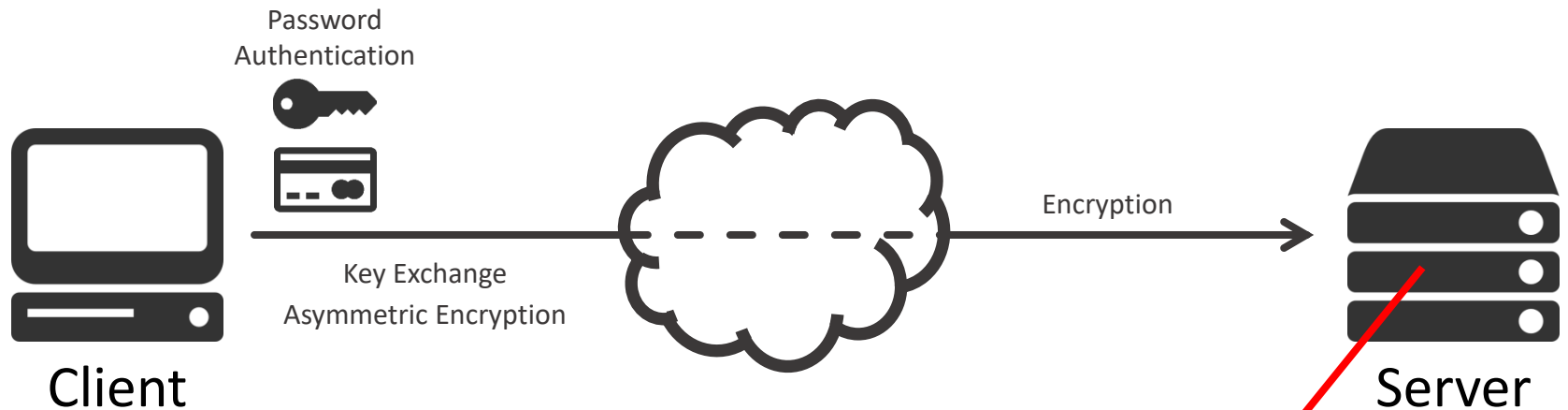
User Authentication



User Authentication

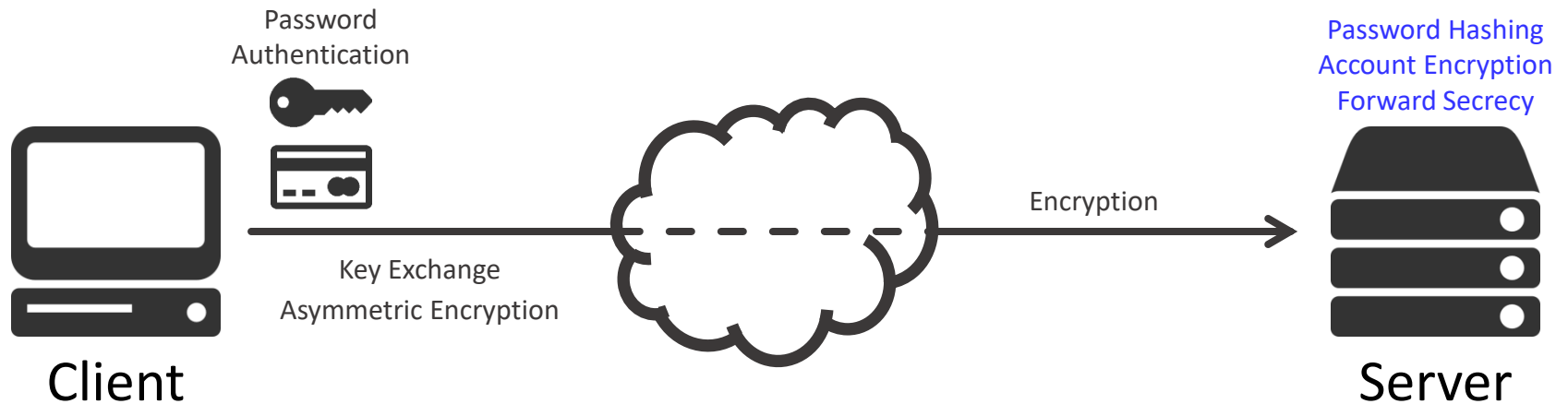


Confidentiality

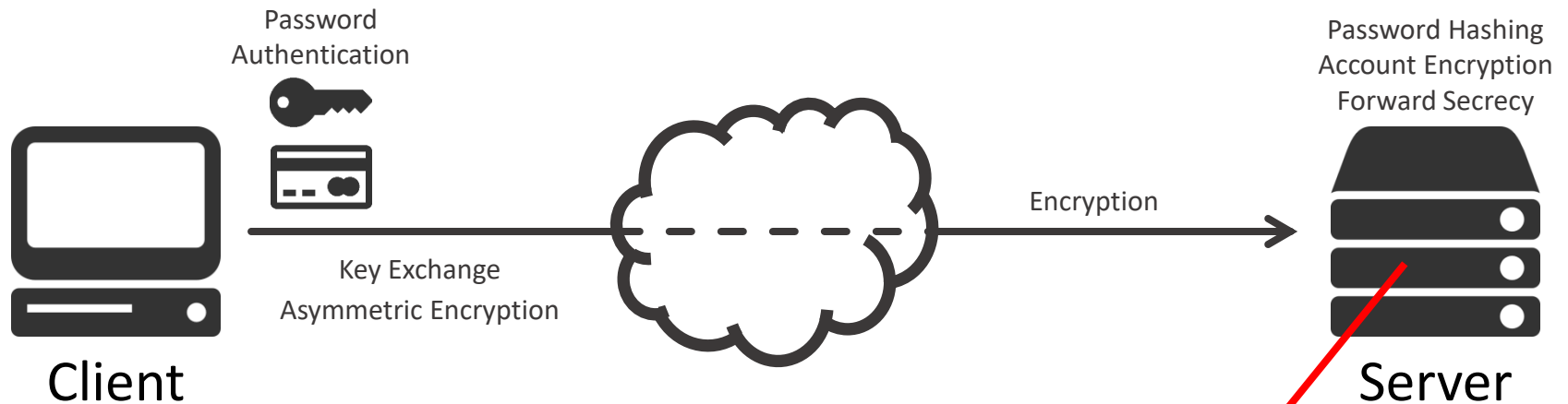


What if the server gets hacked?

Hash Functions

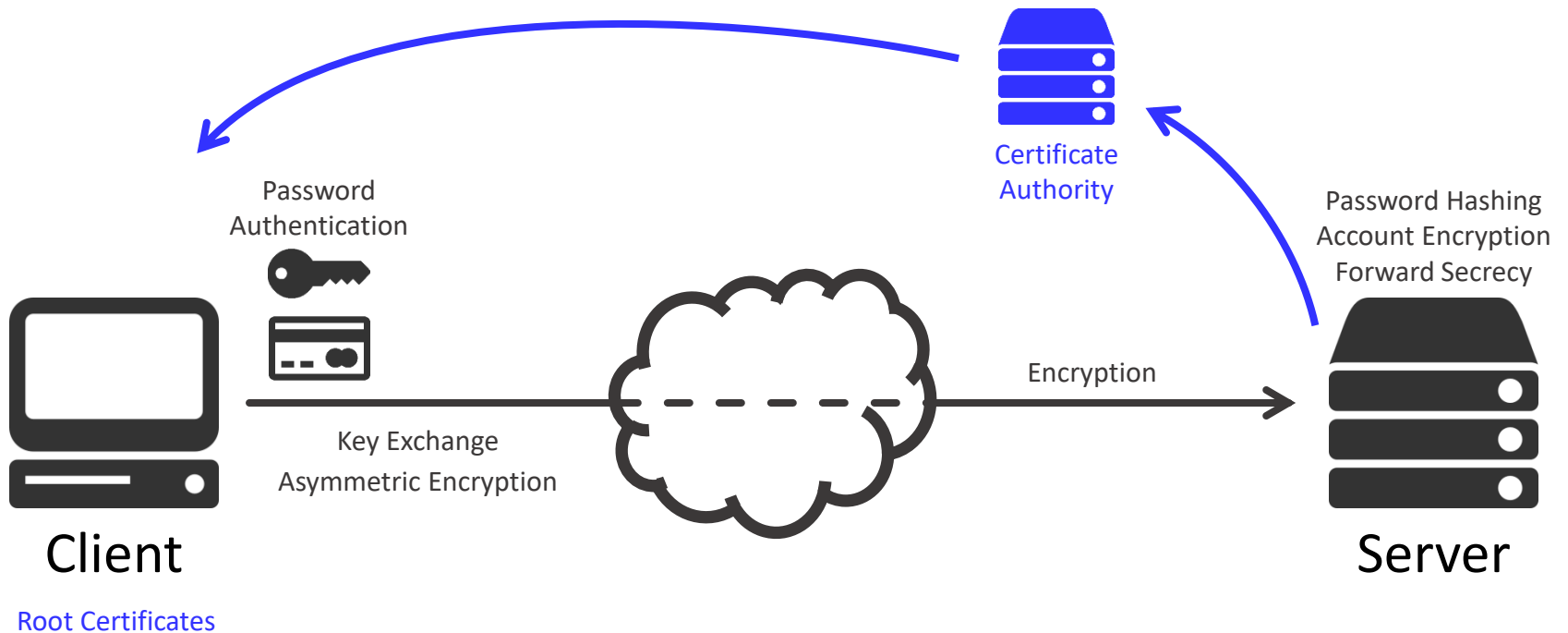


Server Authentication

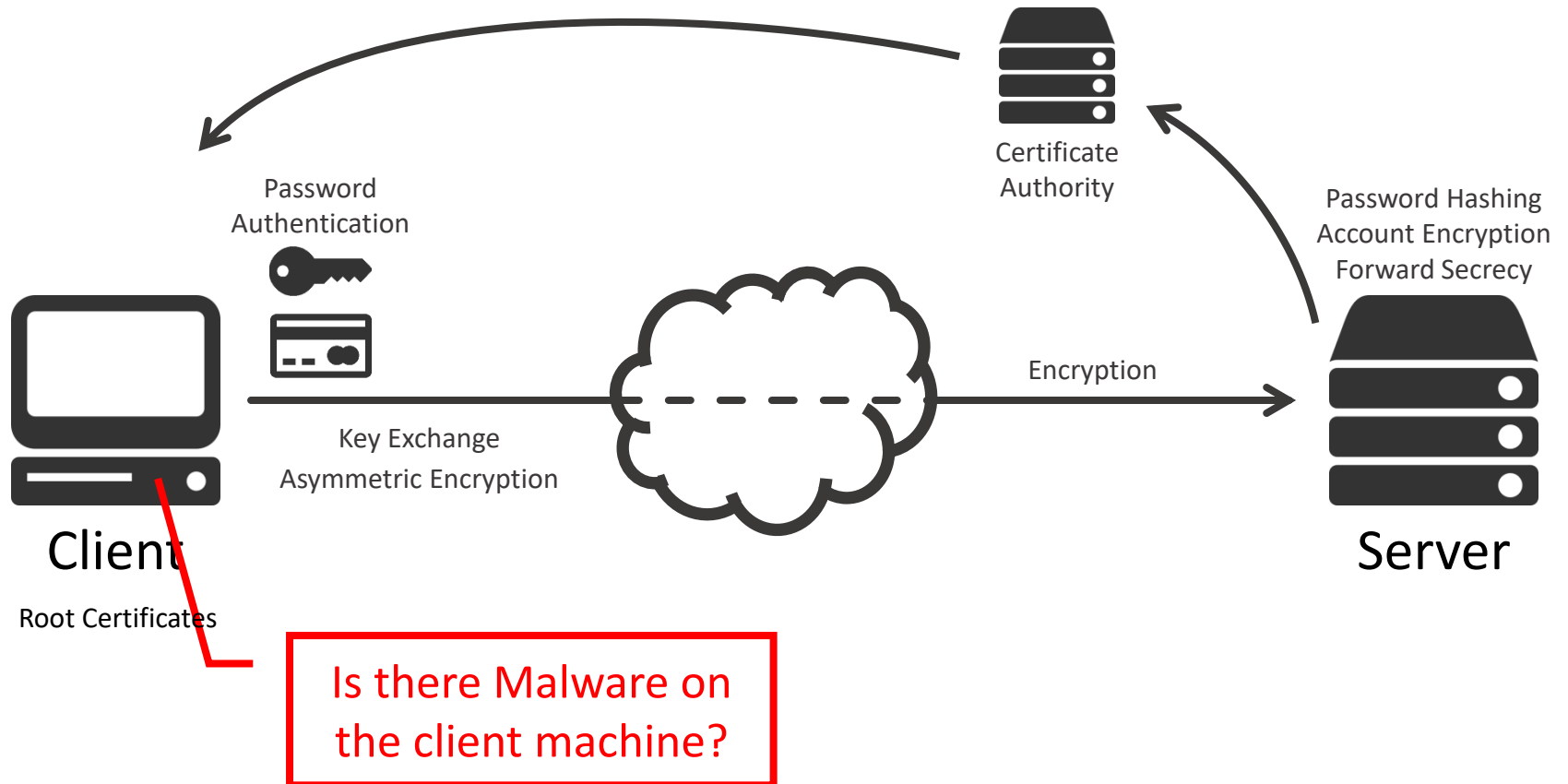


Is the server who they say
they are?

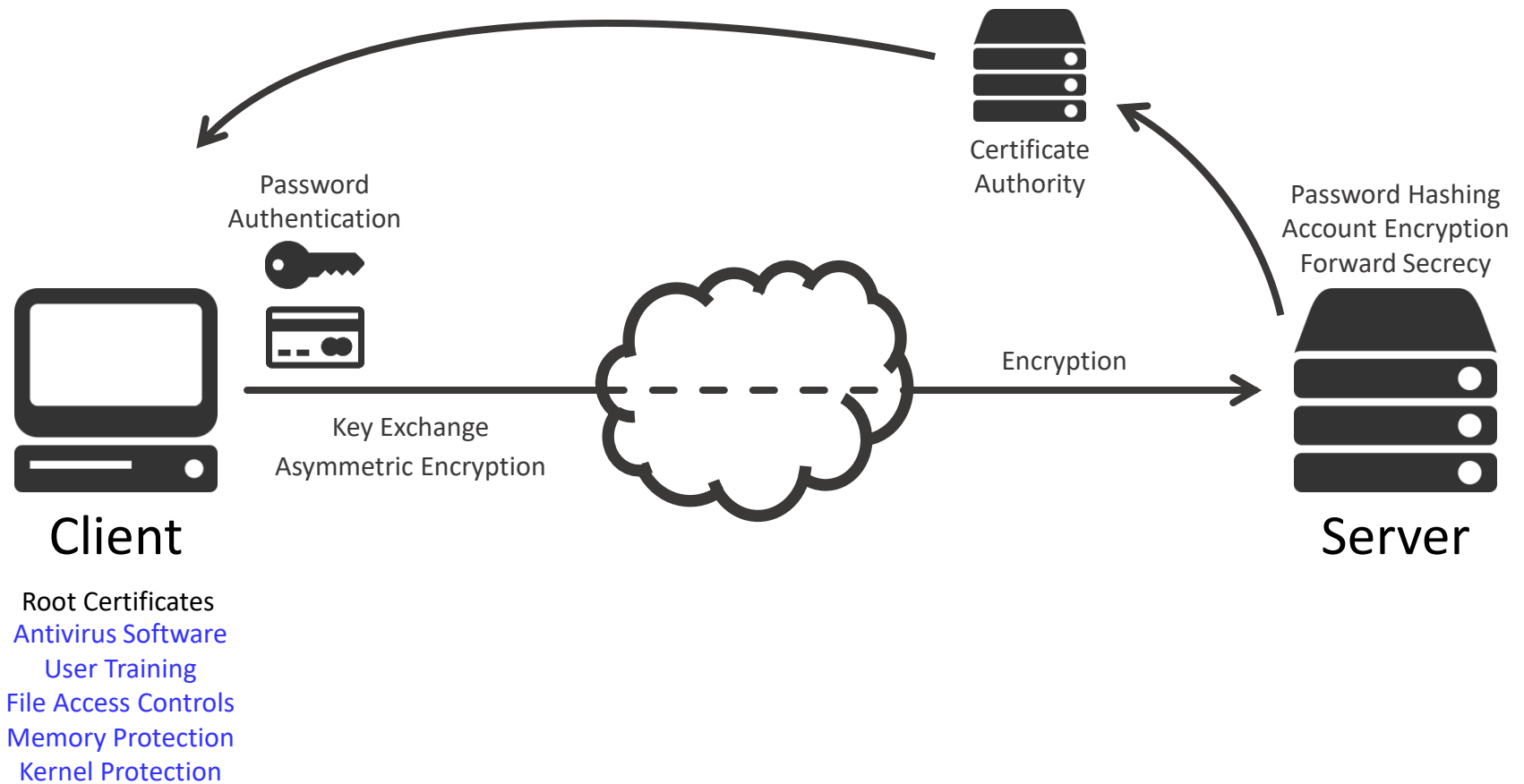
Digital Certificates



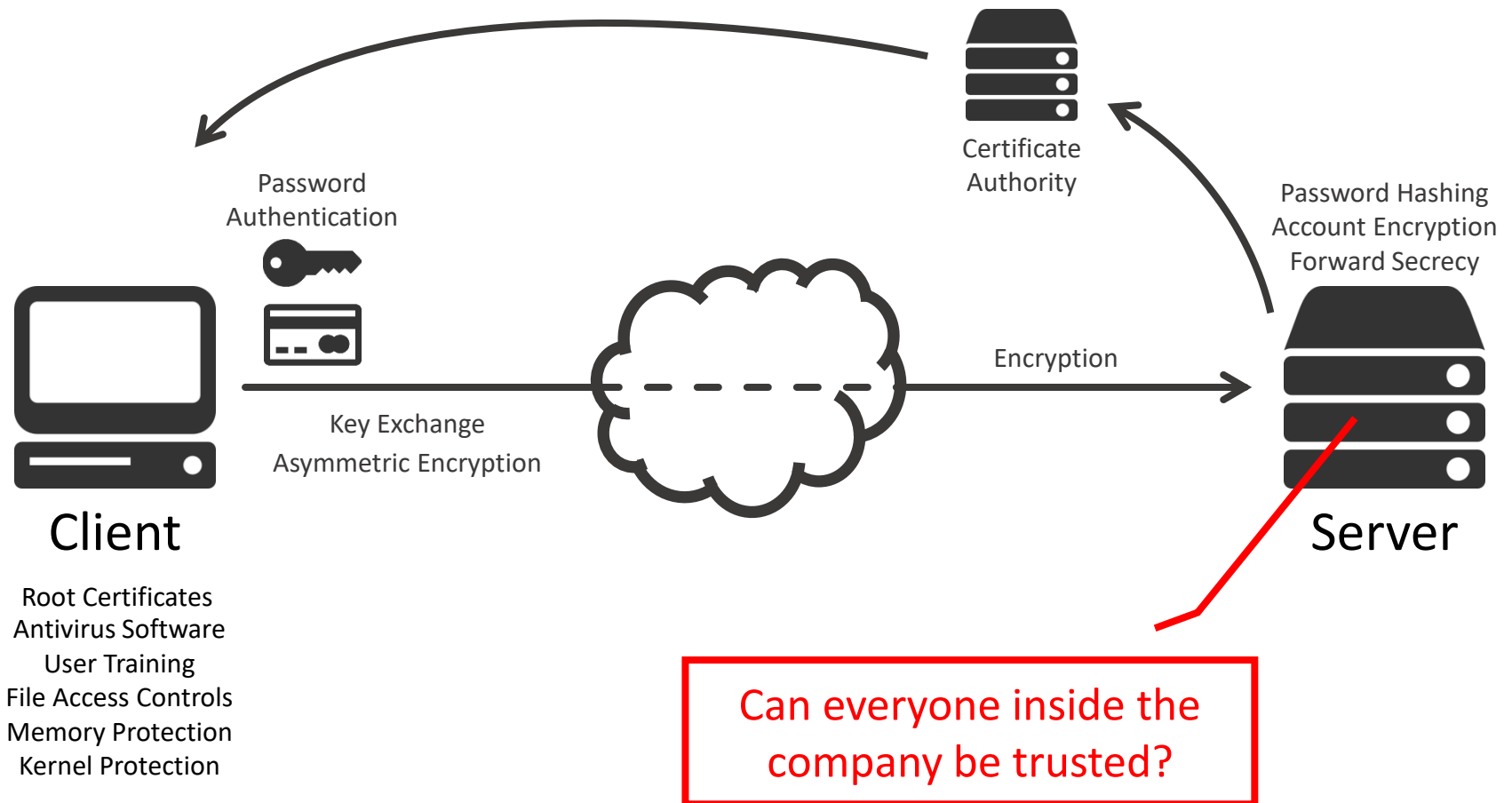
Malware



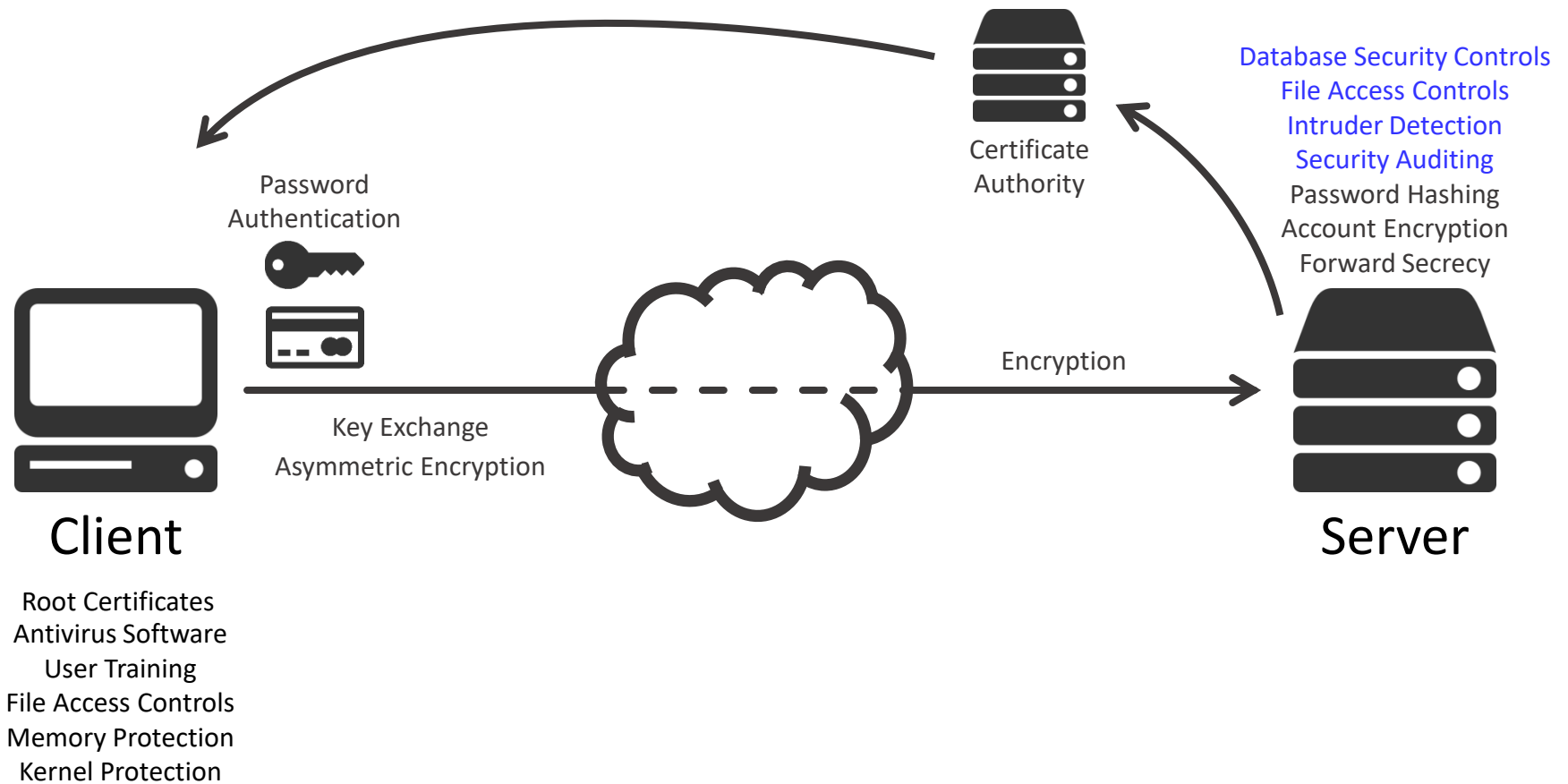
Protection and Avoidance



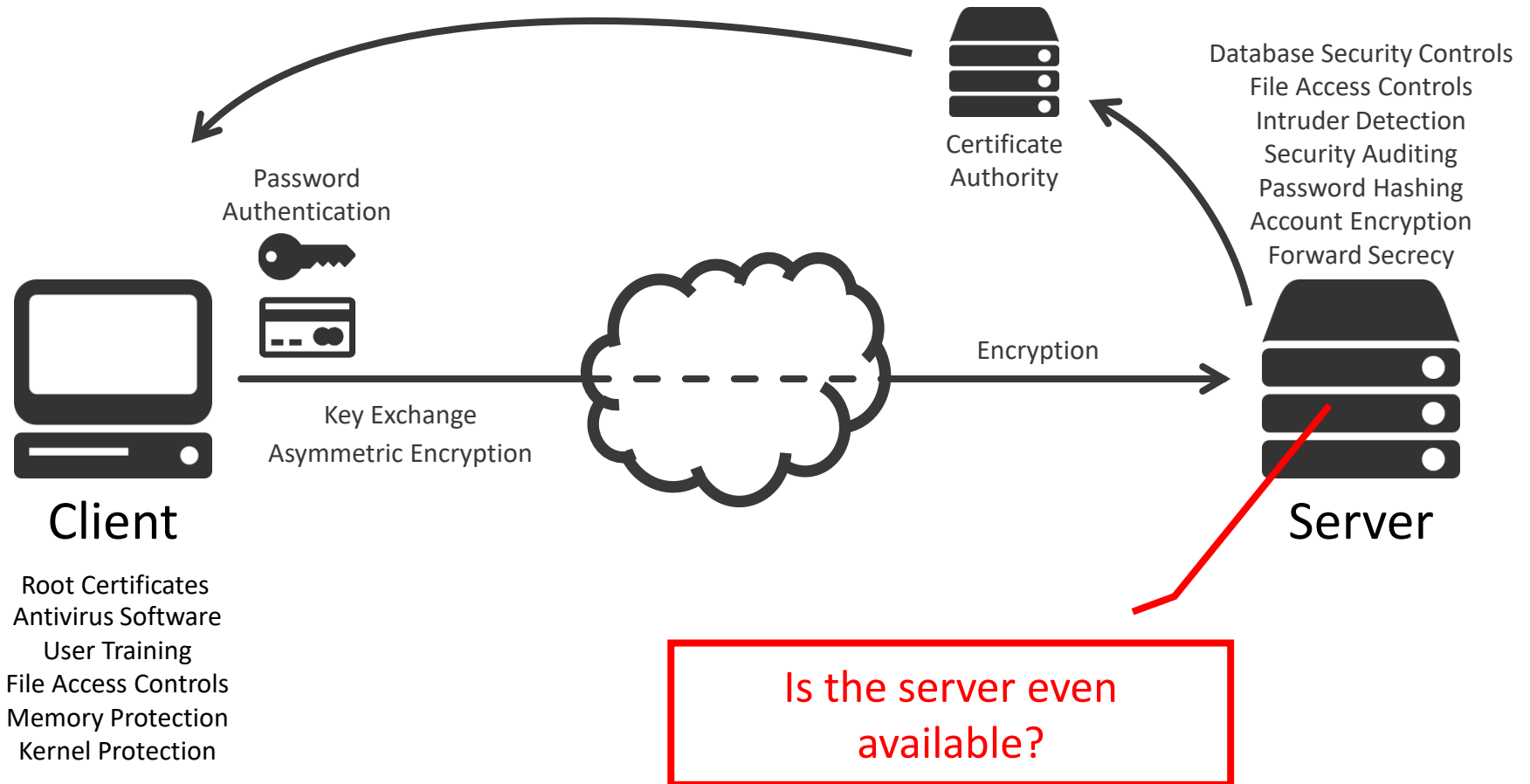
Insider Attacks



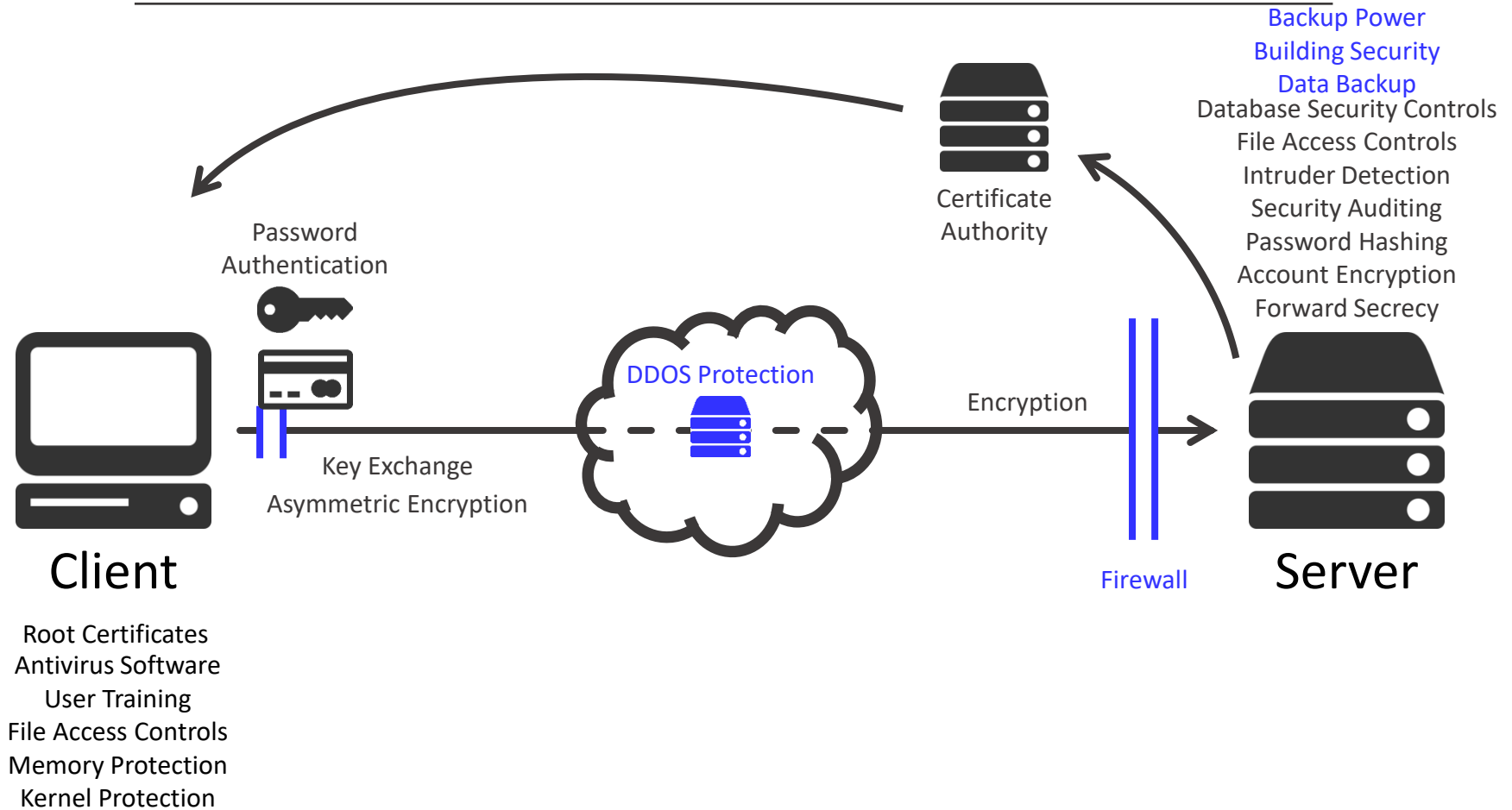
Access Controls



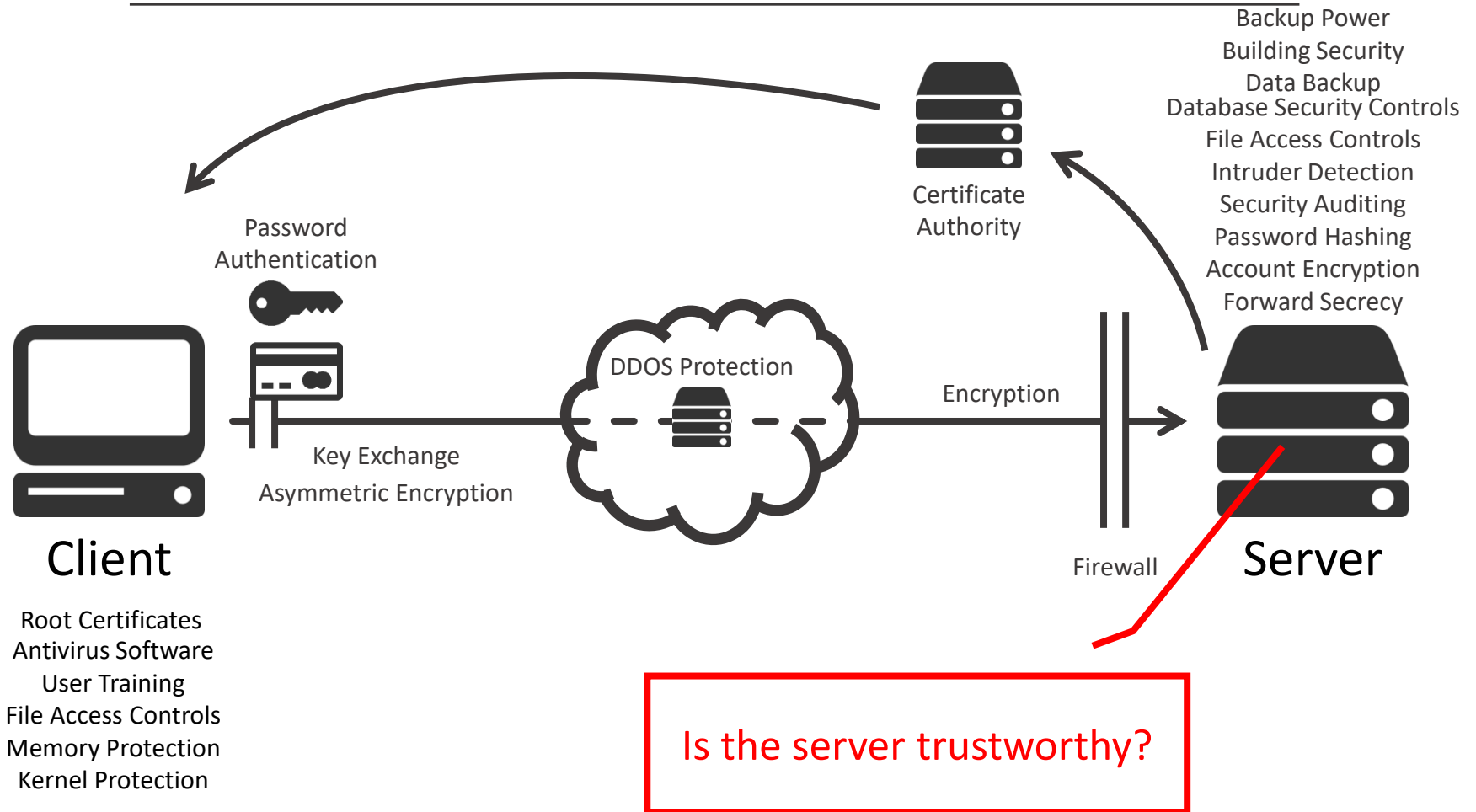
Availability



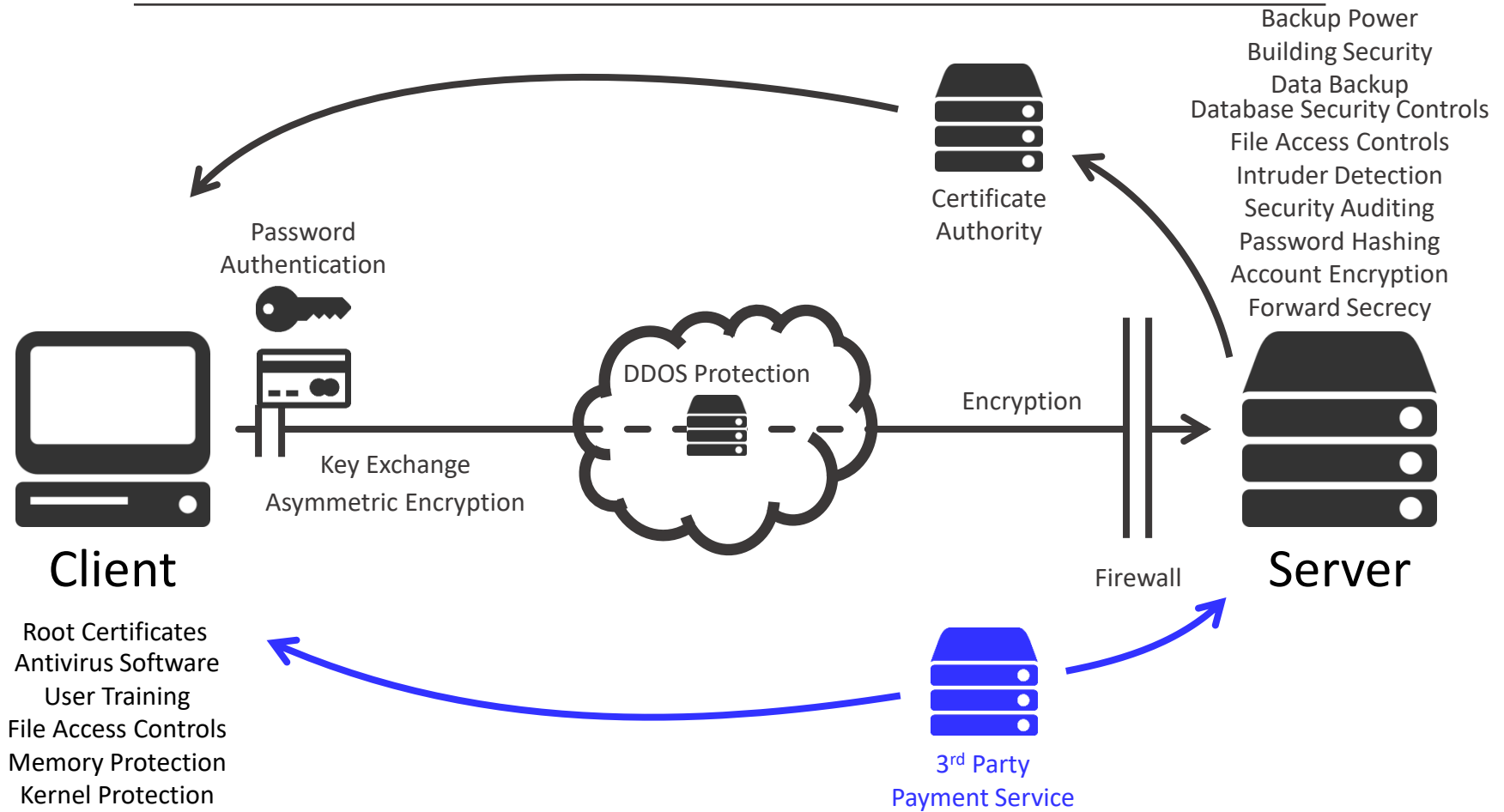
Denial of Service



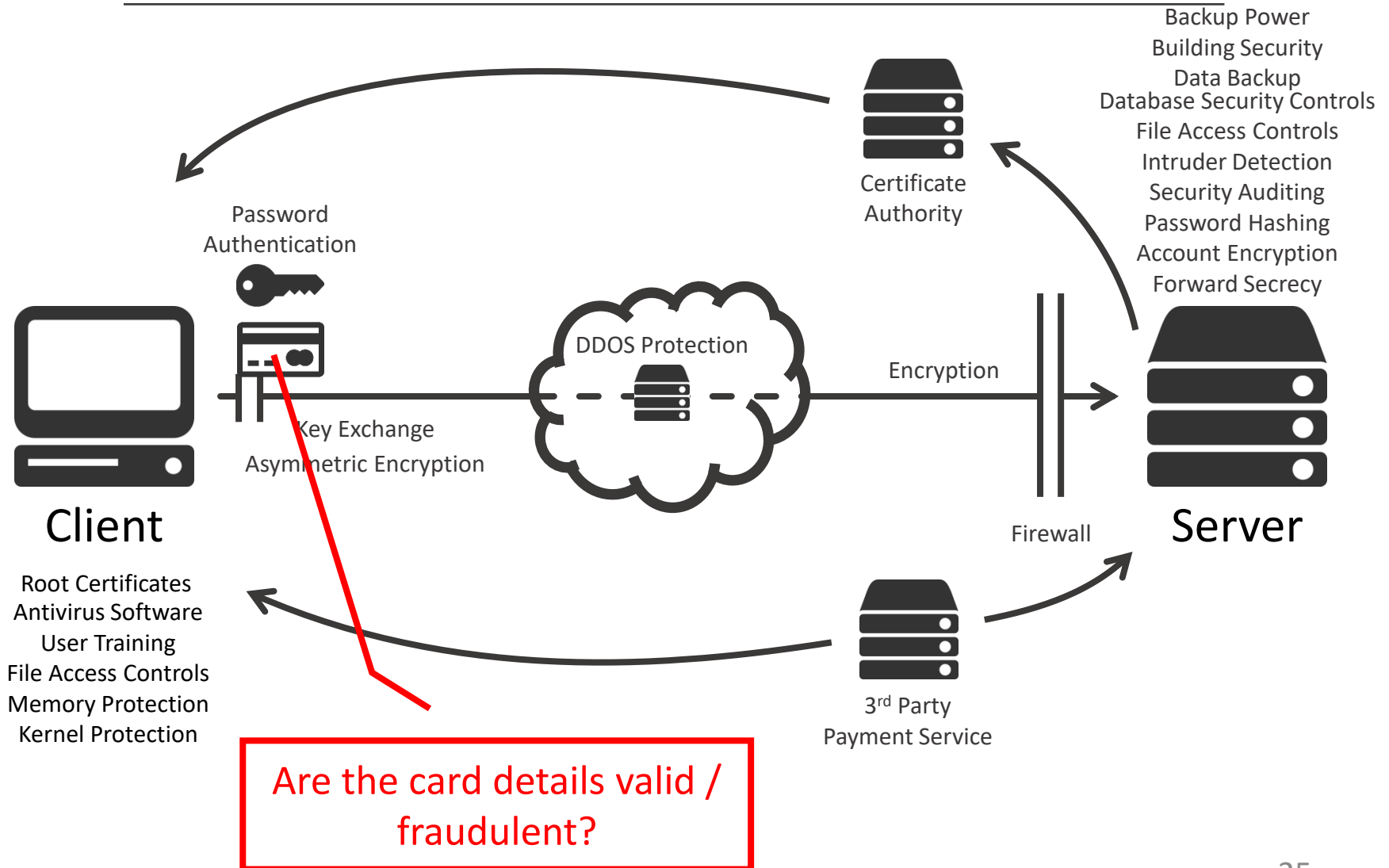
Trust



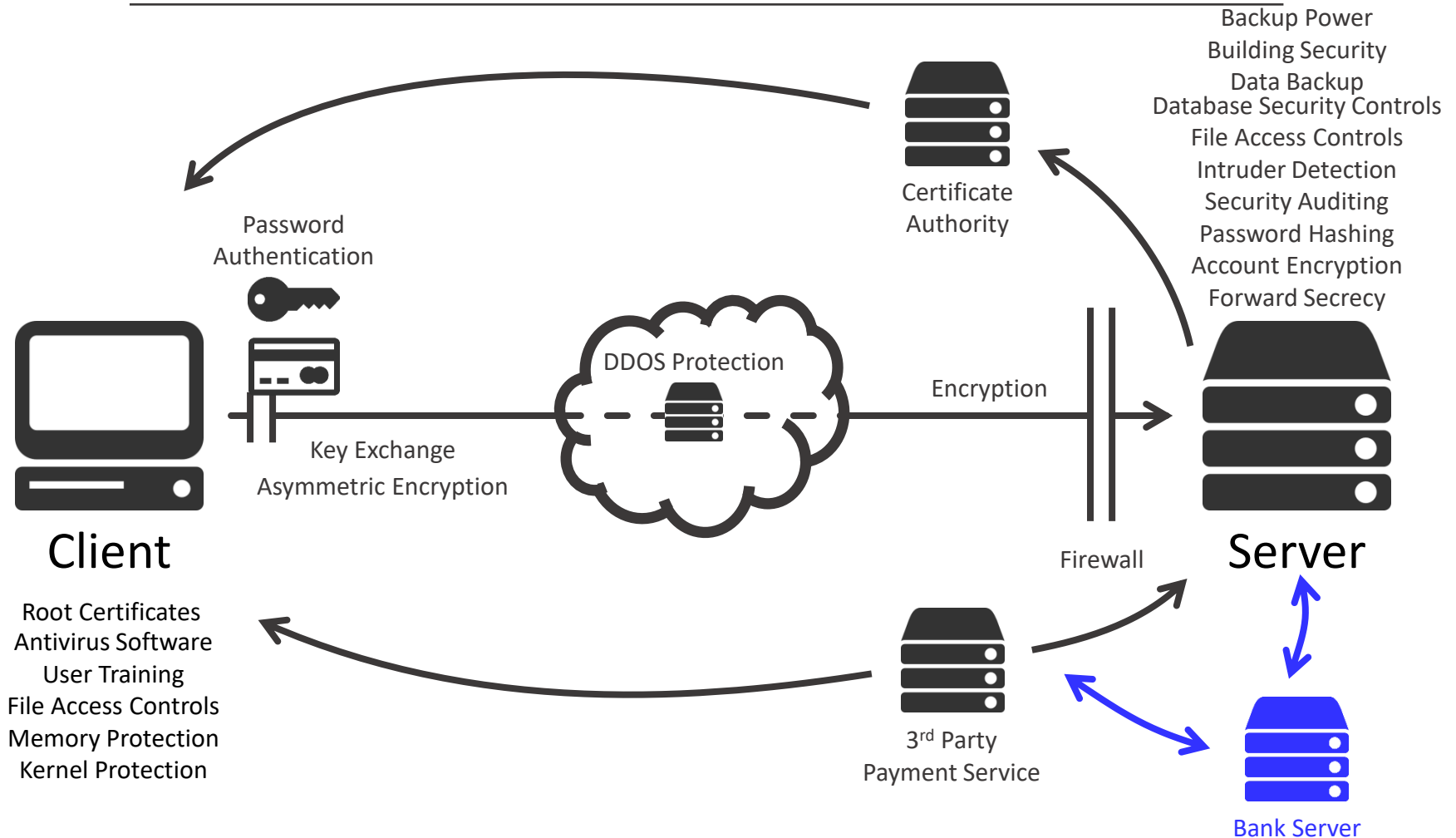
Third Parties



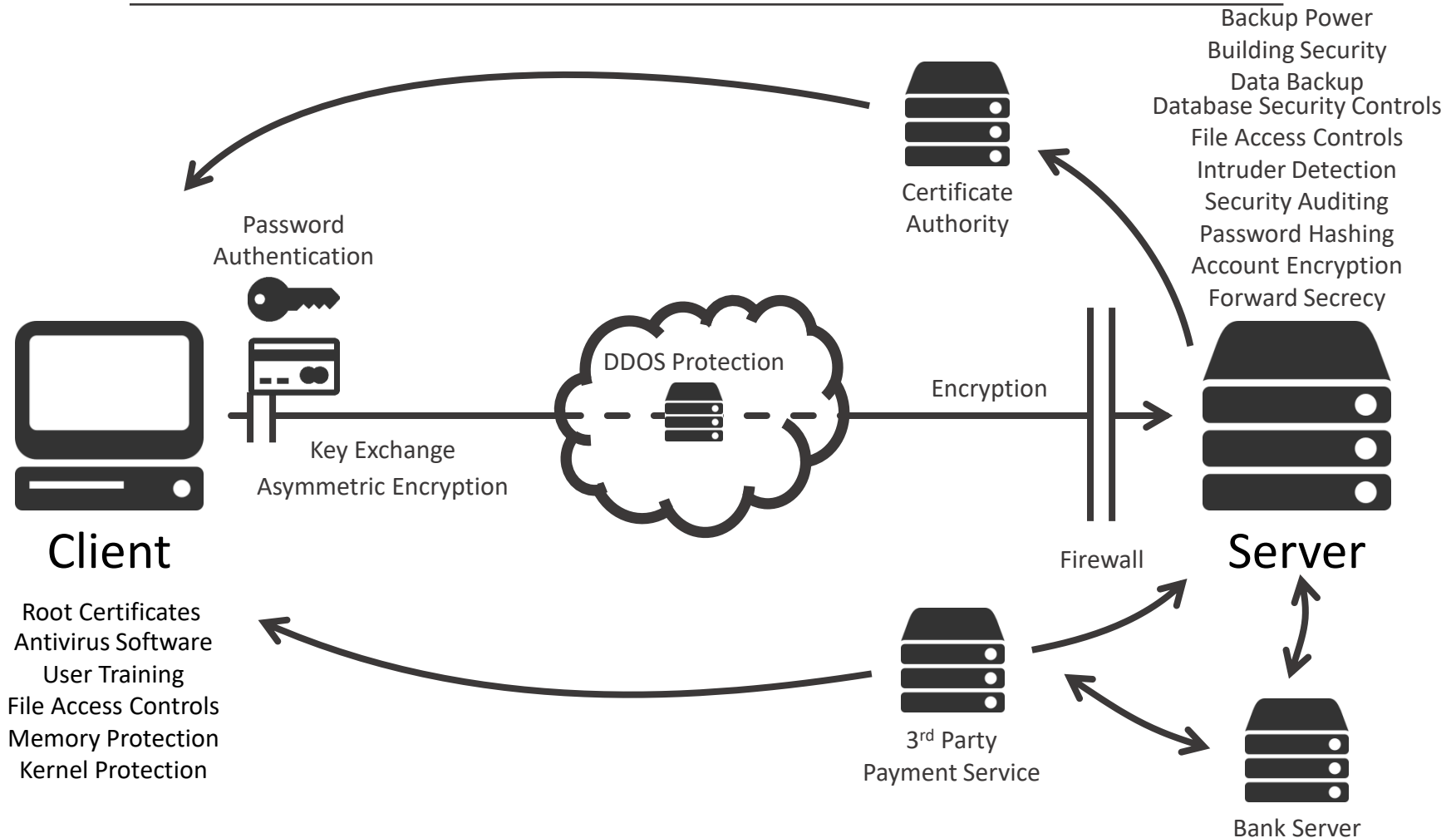
Financial Security



Financial Security



Security Affects Everything



Motivation

- This module will cover the core aspects of computer security
 - but of course we can't cover everything
- Security affects every aspect of modern computer science
- A brief look into common vulnerabilities and countermeasures in distributed systems