16-124-836
Marcel Matti ZAUDER

6.1 Question 1

6.1.A List the three main forms of authentication. Which one can be the most secure? Why?

6.1.B An old website is storing its user's passwords in plain text. You are hired to enhance its security. How would you store and use the passwords (and why)?What type of password attacks are there? What would your counter-measures for them be?

6.1.C A website is using one common salt for all user's passwords, along with server-side hashing. Would using a different salt per user improve the security (and why)? Does a longer salt provide better security (and why)? Would you recommend (or not) to store the salts in an encrypted form (and why)? Assuming no salt was used, would client-side hashing (instead of server-side hashing) decrease the security (and why)?

6.1.D A website is sending "plaintext" passwords over HTTPS. Would the website be safer if these passwords were encrypted (and why)?