

Quiz 3: Security
CS162, November 19, 2012

Your Name:

SID AND 162 Login:

1. A digital certificate is an encrypted binding between the user's identity and user's public key using a certification authority's (e.g., Verisign) *public key*.

TRUE

FALSE

(Note: digital certificate is encrypted using cert. authority's private not public key)

2. "Delay checking" of the password is an effective way to make it harder to crack a password, assuming the attacker doesn't have access to `/etc/passwd`

TRUE

FALSE

3. Checking the size of every argument before copying it in the buffer can avoid buffer overflow attacks.

TRUE

FALSE

4. Typically, the number of hosts infected by a worm increases linearly.

TRUE

FALSE

(Note: typically, the number of infected hosts increases exponentially not linearly)