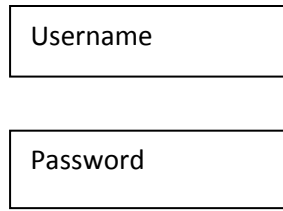


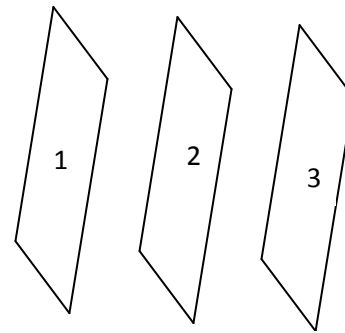


Traditional Topology



VS

VPCMSL™



1. Credentials Presented Together and one or both unmasked.
2. Credential names are well known.
3. User name publically known.
4. User logon location known publically.
5. Uses common publically known character sets
6. Uses well known underlying number system.
7. Lockouts from hacking attempts also lockout user.
8. Vulnerable to malware attacks on client computer giving access to network.
9. Simple passwords degrade security and complex passwords are hard to remember.
10. Open to privilege escalation abuse that facilitates internal fraud.
11. Keyboard Layout Known to Everyone.
12. Facilitates duplicate passwords without differentiation that places user & network at greater risk.
13. Facilitates Credentials sharing that puts networks and copyright at risk.
14. Vulnerable to password guessing attacks.
15. Vulnerable to keyboard logging attack.
16. Vulnerable to phishing attacks.
17. Vulnerable to telephone scams.
18. Vulnerable to man in middle attack
19. Vulnerable to Denial of Service Attacks
20. Poorly maintained client device puts network at risk.
21. Once access has been gained attacker can often change password to prevent user access.
22. Credentials can be stored by user in browser and are available to attacker if client device is compromised.

1. Credentials Presented Separately and all credentials are masked.
2. Credential names can be set to proprietary names not in public domain and can be set for subsets of users down to individual user level if required.
3. User name known only to network administrator and user.
4. User logon location known only to administrator and user.
5. Character set contains proprietary characters know only to the Administrator and user.
6. Number System is Proprietary at minimum of enterprise level and can be tailored to be proprietary down to user level.
7. Hacking attempt lockouts do not result in user lockout.
8. Malware attacks on client computer will not give access to network.
9. Inclusion of picture graphic keys assist users in creating memorable passwords without sacrificing security.
10. Separate access privileges database restricts opportunities for internal fraud.
11. Keyboard Layout Known Only to Administrator & User Group or User.
12. Passwords can by familiar to assist with memorising but are unique to prevent password duplication.
13. Deters Credential sharing.
14. Prevents password guessing attacks.
15. Prevents keyboard logging attack.
16. Prevents user revealing network access credentials to a phishing attack.
17. Prevents user being tricked into revealing credentials.
18. Man in middle attack will not reveal network access credentials.
19. Denial of Service Attacks can be prevented.
20. Operates independent of client device.
21. Change of user codes can only be executed by user who created them.
22. Credentials cannot be stored in browser for attacker to utilise.