

Top Ten Bad Conclusions from *Attacks on Additive Encryption*

10. UDP is more secure than TCP (less redundancy).
9. Token Ring is more secure than Ethernet (packets larger).
8. Ethernet is more secure than Serial/PPP (packets larger).
7. NAT and DHCP increase security (IP Addresses unpredictable).
6. Port-hopping protocols (e.g., H.323) more secure (Ports unpredictable).
5. Setting TTL to high value improves security.
4. Randomly setting DF bit improves security.
3. Randomly setting Checksum values improves security.
2. Low-entropy key generation is more secure.
1. It's most secure to never change your keys.