From “Why Cryptosystems Fail,” it shows that most cryptosystems are vulnerable because the designers of the system used a wrong threat model during design. Designers usually assumes that their system will be implemented by some expertise who is skilful in building security system or with the help from some consultant. However, due to the lack of motivation on the company’s side, unskilled personnel may be selected to implement the system. As a result, frauds are mostly committed by implementation errors and management failures instead of cryptanalysis or technical attacks. Since crypto community seldom researches and learns from the mistakes found in the system, it blocks any feedback usable by the cryptosystem designers when reviewing the threat model for a new design, leading to another failed cryptosystem design. Although there are standards helping companies to choose the security infrastructure their company need, those standards were not considering human errors either, allowing human mistakes to break these cryptosystems easily even if the system has been certified some ultimate level security. Because of irrelevance between the target research force of computer security and the real needs, a paradigm shift is required so the new goals in computer security encompass software engineering ideas, so human error during the operation of the system can be considered in the threat model and incremental improvement can be made in the progression of cryptosystem.

From “Intercepting Mobile Communications: The Insecurity of 802.11,” the article shows that WEP protocol fails to deliver its security goals in confidentiality, access control, and data integrity, and that the security the protocol relies on can be defeated either due to short key length (40-bit for the initial version), or exploitable WEP design model. WEP attacks are feasible to mount because it does not safeguard against resourceful attackers who may have the computational power to brute-force WEP, and the hardware equipment to monitor and inject Wi-Fi traffic is readily available in market. With the widely available equipment, the attacker can tap into any 2.4GHz wireless communication and search for keystream reuses, especially some low-valued initial vector keys as some devices zeroed the initial vector offset whenever it is unplugged. With 2 encrypted packets with same IV, they are XORed to reveal the XORed value of the plaintext of the 2 packets. Since some fields of IP traffic is predictable, once plaintext of either packet is decrypted, then both packets’ plaintext can be decrypted. With multiple ciphertext matching their corresponding secret key, the attacker can build a full decryption dictionary, completely busting the WEP protocol open. Since the plaintext is consist of original message and CRC checksum, and CRC checksum is not cryptographically secure, attacker can modify the sender’s message, or even inject his own message in the sender’s behalf while tapping the traffic between the sender and the receiver through IP redirection attack or reaction attack. To counteract, network administrator can place the wireless network outside the firewall and employ VPN to access the internal network, or improve the key management such that every host has its own dynamic encryption key that frequently changes. The failure of WEP shows that one should reuse past design and make incremental improvement base on the previous design when crafting a new design, then let the public to review such a design so that the design is fully tested against flaws.