Homework 02

Md Moniruzzaman Monir, # 50291708

September 25, 2018

Problem 01

Solution:

- **CFB Mode:**
  - Encryption Formula :

    $C_1 = P_1 \oplus \delta_r[E(k, IV)]$

    $C_i = P_i \oplus \delta_r[E(k, LSB_{b-s} \parallel C_{i-1})] \qquad [i \neq 1]$
  - Decryption Formula :

    $P_1 = C_1 \oplus \delta_r[E(k, IV)]$

    $P_i = C_i \oplus \delta_r[E(k, LSB_{b-s} \parallel C_{i-1})] \qquad [i \neq 1]$

  Here, IV → Initialization Vector, $LSB_{b-s} \rightarrow$ Least significant (b-s) bits of shift register, $\delta_r(a) \rightarrow$ Most significant r bits of a , $a \parallel b \rightarrow$ b appended to the end of a.

- **OFB Mode:**
  - Encryption Formula :

    $C_1 = P_1 \oplus \delta_r[E(k, IV)]$

    $C_i = P_i \oplus \delta_r[E(k, LSB_{b-s} \parallel (P_{i-1} \oplus C_{i-1})] \qquad [i \neq 1]$
  - Decryption Formula :

    $P_1 = C_1 \oplus \delta_r[E(k, IV)]$

    $P_i = C_i \oplus \delta_r[E(k, LSB_{b-s} \parallel (P_{i-1} \oplus C_{i-1})] \qquad [i \neq 1]$

Problem 02

Solution:

a) **Yes** the digest published in the newspaper can be used as a proof that the algorithm was discovered 15 years ago. Here I am assuming that the hashing function used for getting the cryptographic hash was an ideal hash function having **Strong Collision Resistance**. This means it is difficult to find any two messages that

hash to the same value. It is hard to find m_1 and m_2 such that $H(m_1) = H(m_2)$.
So, there is only one m (document containing the algorithm) which will produced the cryptographic hash published in a newspaper 15 years ago.

b) My answer would not change if a cryptographic signature of the document was published instead of the hash. Because ”hash-and-sign” paradigm is used for digital signature. The hash value of the document was encrypted using a private key. While hash value ensure the uniqueness of the document, the private key proves the authenticity. A crytographic signature ensures non-repudiation (unique sender) which is not achieved by crytographic hash. So here it is more evident that the algorithm was discovered 15 years ago by Alice.

Problem 03

Solution:

a) Let’s assume the public keys of Alice and Bob are (e_a, n_a) and (e_b, n_b) which are stored in a file on a server. In order to forge messages from either side Eve will alter the the file with two new key pairs. For this purpose Eve first create two new key pairs (e_{ae}, n_{ae}) and (e_{be}, n_{be}) and register this for Alice and Bob. Here I am assuming that Eve has full access of the communication channel between Alice and Bob. So Eve can intercept every message. Now Eve will alter the communication between Alice and Bob but they will believe that they are directly communicating with each other when in fact the entire conversation is controlled by Eve. After intercepting all messages between Alice and Bob, Eve can undo their computation and replace it with a signature using her version of the key. **e.g.** Alice sends a message **m** to Bob by using Bob’s public key [(e_{be}, n_{be})] which is actually stored by Eve. So Eve would intercept it, decrypt it using her version of Bob’s private key, and now send it to Bob after encrypting it using Bob’s original public key [(e_b, n_b)]. Bob will receive the message and think that it is from Alice. But it was actually sent by Eve. Thus Eve can forge messages from either Alice or Bob, change the messages if she wants.

b) If Eve fails to intercept a message then the decryption will be failed in receiver’s side as the message was encrypted by the sender using the fake public key which was put in the server by Eve. The message destined to Alice and Bob will not correctly decrypted since they will use their real private keys to decrypt rather than Eve’s fake private key.
Alice and bob should periodically verify that the public key they have posted on server is correct. Also they can take help from a trusted third party that can verify (for Bob) that the key he received is Alice’s public key. (This is what TLS does.)

Problem 04

Solution:

a) The article **‘Why Cryptosystems Fail’** describes a misconception about **security of computer systems** by analyzing the failure models of the retail banking system. Unlike other engineering systems e.g airline industry, designers of cryptographic systems get no feedback on their systems. There was no learning mechanism, and the same mistakes was made over and over again. This lack of feedback has led to a false threat model being accepted. Designers and government evaluators have both concentrated on what could possibly happen rather than on what was likely to happen. Initial threat model presumed that attacks would be technically sophisticated, either cryptanalysis or via eavesdropping. But the attacks which actually happened were made possible because the banks didn’t use the available products properly; due to lack of expertise; basic error in system design, application programming and administration. Ross Anderson, author of this article, found that for ATM-related fraud, only two cases out of hundreds involved technical attacks. The main two reasons behind false threat model was :

- Expected criminals with a high level of technical expertise and blindly followed conventional military wisdom which stressed secrecy
- Human Factors

Poor implementation and lack of total quality management are root causes of security failures. So a change is needed in security of computer systems. By adopting new security paradigms the field of security is always evolving. To be effective, the change must bring about a change of focus and need to make a systematic study of what is likely to. The core security business will shift from building and selling 'evaluated' products to an engineering discipline concerned with quality control processes within the client organization. When a paradigm shift occurs, it is quite common for a research model to be imported from some other discipline. Safety critical systems is the new metaphor for the evolution. There are also two competing philosophies from two different models - one is railway signalling system which is reductionist and the other is aviation paradigm which is holistic. The author suggests to follow the aviation industry's paradigm: a properly trained crew is the first line of defense. Also, security systems should be studied by looking at the environment where it will be used.

b) **Building and Operating Secure systems :** The paper explains why the initial threat model was wrong and finds out the problems with secure systems. Some problems are listed below :

- Misguided focus towards building cryptosecurity products without addressing how to incorporate them in real systems. A lot of failures occur at the implementation level.
- Poor certification process
- Threat model assumes only one thing goes wrong at a time.

So we need to focus on Robustness which means security systems should be resilient against minor errors in design and operation, and provide redundancy against component failure. Explicitness should be the organizing principle for security robustness. To achieve the desired security in computer system the paper mentions four very basic points for building and operating secure systems.

□ The specification should list all possible failure modes of the system.

□ It should explain what strategy has been adopted to prevent each of these failure modes or at least make them acceptably unlikely.

□ It should then spell out how these strategies are implemented, including the consequences when each single component fails.

□ The certification program must include a review by independent expert and test whether the system can be operated by people with the stated level of skills and experience.

c) **Main proposal of the paper :** The paper includes many interesting examples from the banking industry and the analogy between secure systems and safety critical systems such as avionics. The author uses automated teller machines (ATMs) as a driving example through the paper. He explains how ATMs work, and how various attackers have or could have managed to defraud banks by attacking ATMs. These attacks are allowed due to human error, negligence, lack of quality control, lack of a feedback loop, incomplete standards. Mainly, it is not due to the weaknesses usually studied formally in universities or companies such as cryptanalysis. Some attacks are listed below :

- Observing customers entering PINs and pick up discarded receipts. Copy account number (on receipts!) to blank cards to loot customers.
- Entering telephone cards. One british banks ATM believed that the previous card was entered again.
- Jackpotting (replay attack)
- Postal interception
- Issued extra cards

- Fit ATMs with devices recording PINs entered

The author mentions that security systems should be treated similar to safety critical systems. Security systems should have certification levels that take a whole security system into account from the cryptography at its lowest levels to the training of employees to the treatment of a wide array of threats. A number of recent threads point towards a fusion of security with software engineering or at the very least to an influx o software engineering ideas.

d) The situation with the banking industry has improved a lot compares with the scenario what is described in the paper. At that time researchers were concerned only about the technical aspects but now they includes human factors into their consideration. The wrong threat model is eliminated. Now every bank has a separate security team consisting of security experts. Security is taken as a holistic approach and is blend with software engineering. Policy makers have changed their policy for the benefits of the bank users.

Protection Mechanisms I encountered in my banking experience : Now almost every bank has their online portal and mobile apps to check all the activities and transactions in real time. After every transaction there is an email and a message in phone. There is also 'Two Factor Authentication' (**2FA**) with One-Time Passwords (**OTP**). OTP systems provide a mechanism for logging onto a network or service by using a unique password that cannot be reused for each transaction. This increases protection for online bank account management. Also, in some bank they call the user if a transaction exceeds a certain amount for confirming that it is not a fraud transaction.

e) In other industries computer security is also very important. And some industries are more targeted by the hackers than banking sector. **Healthcare sector** tops the list of the most cyber-attacked industries, according to the recently released '2016 IBM X-Force Cyber Security Intelligence Index'. This reports more than 100 million healthcare records were breached. This happened due to the nature of customer information they handle, and the relative lack of knowledge on the industrys end in terms of security awareness. Security in healthcare sector is very weak if I compare with security in banking sector. IBM reported that cybercriminals are more likely to steal data from hospitals databases because their security systems are usually outdated, despite the fact that the data they handle are vulnerable (e.g., email addresses, social security system numbers, address and contact details). According to the PwC Health Research Institute, the consequences of healthcare security breaches may cost up to $200 per patient record.

Manufacturing sector, which includes automotive, electronics, and pharmaceutical companies, have always been a vulnerable industry when it comes to cybercrime and security breaches. This is because many cyber attackers are financially motivated and therefore are more likely to hack corporations where they can demand a higher amount of money, as well as sell information to competitors. This sector has not been held to a high standard when it comes to security compliance and risk management as compared to banking sector, which renders it more vulnerable to cyber hacking and malware.
The other vulnerable industries are Government sector and Transportation sector.