Evaluation of physical security in three scenarios in TV series “24”

Irfan Ullah
Email: irful667@student.liu.se
Supervisor: Juha Takkinen, {juha.takkinen@liu.se}
Project Report for Information Security Second Course
Linköpings university, Sweden

Abstract

We analyze three different scenarios for security in TV series “24” and compare these scenarios with respect to physical security. We apply “security engineering” to analyze these scenarios and find that these scenes are farfetched from reality.

1. Introduction

The TV series 24 was first aired on 6th November 2001 by Fox Corporation in United States. The main character Jack Bauer is working for Counter Terrorism Unit (CTU) which goal is to protect US from terrorist, and to disrupt the terrorist cells [14].

The increased communications means have posed many serious threats. Film makers are making movies about security issues. We will differentiate physical issue depicted in movie and in real word.

Security has become a very important aspect including physical security, business security, and business continuity planning.

We have chosen TV series 24 because it is popular and it has many examples of security issues to be examined.

According to the definition, physical security [6] is protection of personal, data, hardware, and network from physical circumstances and events which could cause of serious loss or damage to an enterprise or institution. This also includes protection from fire, natural disaster, theft, and terrorism.

In other words, physical security [6] is that part of security that is concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, material, installations, and documents, and to safeguard them against espionage, sabotage, theft and damage.

The physical security has following security components: locks, barriers, alarms, lights and cameras, and inventory controls.

2. Problems and aims

There are different and farfetched physical security problems in TV series 24, we will identify three of them, and discuss them for physical security issue. The security problems could be caused by human behaviors, deliberate act of theft, sabotage, software attacks etc. or the act of human error, mistakes.

There is need to illustrate the physical security of people, facility, and information [2].

Our main issue is to stress the difference between physical security depicted in movies and in reality. The security issues in TV series 24 seem to be farfetched, because it lacks the features in reality, and therefore does not give the true feeling of security to audience. There are many examples of security breaches in TV series 24. For example, a security analyst finds a backdoor in cryptographic algorithm “Blowfish” in minutes.

We will examine three scenarios from TV series 24, and discuss on physical security feature [8].

In TV series 24, we will mainly focus on season 7, we will focus on following three scenes, first, Breaking blowfish algorithm for opening door, second, a room which could be opened only from inside, and third, getting unauthorized access to office, facility and information, by stealing identity and deactivation of alarms and CCTV [3].

3. Methods

We will use “security engineering method” [11] to identify the threats and eliminate them. We will use fundamental concepts for security for illustration.

Security engineering is specialized field of engineering which focuses on security aspects in the design of system.

It covers physical security, information security and economics of security. Secure systems have to resist not only technical attacks, but also fraud cases.

The security engineering is understanding of typical threats, and usual risk of property and people, incentives created by threats and counter measures. It is also understanding of risk and threat analysis methodology [2].

The security engineering method [4] has following phases:

1. Requirement phase: we identify trust requirements and mission requirements.
2. Design phase: we discuss design guidance and regulations.
3. Integration phase: We discuss issue from multi level security and determination.
4. In closing we discuss aspects of certification and accreditation and establish how to establish certification and accreditation program.

While considering a security policy, physical security [6] should not be overlooked. An attack is possible via physical way or via software means. If we have a well-protected computer system, there is a possibility that an attacker may use physical means to access the computer system. While designing security architecture, the skill level of attacker must be considered.

Diminishing the risk, cost and making decision on economic basis is also involved in analysis.

We will examine scenarios after applying security engineering to eliminate threats. We will discuss that how these scenarios are farfetched in TV series 24.

4. Analysis

We will analyze three scenarios, and find how these scenarios are farfetched; we will also evaluate them by comparing the Security engineering method [11].

It is possible that we give a mistaken analysis of a scenario because physical security is a very broad subject and we can deviate from our primary subject [7].

We will begin from physical security and then prevention mechanism.

We will limit our analysis physical security attacks concerned with these three scenarios only.

4.1 Scenario 1: Breaking blowfish algorithm for opening door

In first scenario, a back door is found in cryptographic algorithm “Blowfish” for opening the door. A security analyst O Brian finds it in matter of minutes working on computer just knowing the ordinary information (name, address, 32 bit word length, and native data points) [1].

Blowfish is a symmetric block cipher that can be used for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use [10].

Many cryptographers have examined Blowfish, although there are few published results. The weak keys is also examined in Blowfish, concluding that there is a class of keys that can be detected, although not broken, in Blowfish variants of 14 rounds or less.

The problem is that the scenario is that how it was guessed by analyst in just 30 seconds.

4.1.1 Security engineering (for blowfish algorithm):

Requirement phase:

This phase includes the determination of applicable security policy. It include information asserts, damage to those asserts, and measure of protection of asserts [7].

In our case, there is need to for such blowfish algorithm which can take at least 14 rounds for weak keys. Blowfish has 448 bits encryption strength, which requires a 32 character password, but allows 8 character passwords. The rule of thumb is length = strength [10].

The credential information of a person should also be protected.

Design phase:

The design guideline represents the set of practices that can be employed to reduce risk of vulnerabilities.

In passwords we should remember three issues to remember:

1. Dictionary words can easily crack.
2. The longer and mixed character (numbers and characters) are harder to break.
3. Not to forget password. Because there is no way to decrypt and re-open encrypted note.

(See table 4 and 5)

While designing an implementation of algorithm, like blowfish for opening doors, the passwords and information should be kept most secret, so that nobody can access them and decrypt the password [16].

Integration phase:

There should be no way for decrypting the password even in case of forgetting password. There should be a trusted third party which manages all passwords.

In TV series 24, we suppose that there was 8 character password was set, which was broken in just 30 seconds, this scenario seems farfetched because we have some data about guessing the 8 character password of blowfish [16].

Password complexity: Single case letters only [16]

Your password uses all lower case (or all upper case) characters, but not both.
For example: matrixse or MATRIXSE

Password length	**Brute-force time to find password** (at 1 billion guesses per second*)*
8	104 seconds

Table: 1

Password complexity: Mixed case letters. [16] Your password uses lower and upper case characters. For example: mAtriXse

Password length	**Brute-force time to find password** (at 1 billion guesses per second*)*
8	7 hours

Table: 2

Password complexity: Mixed case letters and numbers [16]. Your password uses numbers, lower case and upper case characters. For example: mAtri7Xs

Password length	**Brute-force time to find password** (at 1 billion guesses per second*)*
8	29 hours

Table: 3

Password complexity: Mixed case letters, numbers and punctuation [16]. Your password uses numbers, lower case characters, upper case characters and punctuation. For example: m@triX7s

Password length	**Brute-force time to find password** (at 1 billion guesses per second*)*
8	37 days

Table: 4

Password complexity: All ASCII Character set groups in use [16]. Your password uses all available characters in the standard ASCII characters set. For example: m@t7**î**X**š**e

Password length	**Brute-force time to find password** / 2 (at 1 billion guesses per second*)*
8	37 days

Table: 5

According to data tables [16] above, the least time to break simplest password is 104 seconds with bruit force (for 1 billion guesses per second ratio), but the analyst breaks it in just 30 seconds which is impossible.

There are three weaknesses are found in blowfish algorithm [10].

First, a sign extension bug in one publication of c code identified. Sign extension is an operation in computer arithmetic of increasing number of bits of binary number while preserving the positive or negative sign, and the value.

Second, Serge Vaueday [12] (a member of the laboratory of Security and Cryptography) in year 1996, found a plain text attack that 2^{8r+1} known plain text is needed to break algorithm, a class of weak keys could be detected and broken by the same attack with only 2^{4r+1} known plaintexts

Third, Vincet Rijmen [13] (a co-designer of the WHIRLPOOL cryptographic hash function) found second order differential attack that can break algorithm in four rounds,

The name, address, 32bit word, and native data point knowledge enable the analyst to find a backdoor in blowfish algorithm which is an exaggerated approach.

If the analyst has fiestel network software installed on computer, then he may apply bruit force methods, by guessing the combinations, which is very much difficult in 30 seconds. (See table 1) [16]

4.2 Scenario 2: A room only opened from inside

In second scenario, there is a room in which an ex prime minister and his wife is kept, and the room could only be opened from inside. The location of prime minister is kept secret for security reasons. There are thick layers of room and door of safe room is very strong and could be opened only from inside.

To forcing the prime minister to open door from inside, Jack Bauer, fill the toxic material in ventilation system, and the room is filled with gas, as a result, the prime minister wife opens the door from inside.

There are problems in first scenario that toxic gas was made by bleach, and could not be dangerous as “mustard gas” and was bearable to smell. There was no sign of surveillance camera is shown and making access to ventilation system was very easy.

4.2.1 Security engineering (for safe room):

Requirement phase:

The ventilation system of any safe room and perimeter of such kind of facility should be heavily guarded.

Design phase:

The design of a true safe room should protect the room from any unwanted access from outside and inside.

Integration phase:

A true safe room protects its occupants from inhaling harmful or deadly airborne toxins. [5] (See Figure 1)

Figure 1: A duct tape and plastic [5]

The duct tape and plastic provide protection from low level toxin and chemical agents. The system will not allow airborne toxin from migrating into breath air (see figure 1)

In this scenario, there is no barbwire, cameras and alarms are placed in outer perimeter of the room. There are no CCTV cameras to observe the strange activity outside the room. Due to highly sensitive nature of room, there should be less trees and bushes outside.

There should be alarm system which could be activated in a strange activity. There is a problem that alarm system could be shut down by denial of service attack.

The safe room has thick walls, and a strong door, and can only be opened from inside.

First the prime minister is threatened to kill the guards, and afterwards, Jack finds ventilation grid and fills it with a mixture, which fills the room with gas, forcing prime minister to open door.

4.3 Scenario 3: Stealing identity by artificial fingerprints, and by stealing card

In third scenario, the attorney of a prisoner is sprayed with an unknown substance, and her identification card is picked. Her fingerprints are also got, and gummy fingerprints are made used a jelly substance.

The fake attorney passes all the tests using gummy fingerprints, and stolen identity card to visit prisoner.

The fake attorney visits the prisoner and gives him death pills; threaten him about his family, eventually the prisoner suicides.

In this scenario, the problem is use of thin transparent layer for fake fingerprint, and passing the authentication process is slightly exaggerated. The fingerprint reader provides some kind of protection against use of synthetic fingerprints.

4.3.1 Security engineering (for artificial fingerprints and stolen identity card):

Requirement phase:

The smart cards should have the secret key, and the fingerprint scanner should be ultraviolet, because they can detect the live ness of fingerprints better than common scanners.

Design phase:

The design phase of authentication a person should include effective biometrics and design structures which resist the hostile actions.

Integration phase:

”Token” is normally used for any authentication device with processing capacity. Smart cards are a variant, differing only in input and output channels [9].

Token contain a key which could be revealed by different ways, observing electromagnetic emissions, power variations and time to perform operation.

For safety of key, calculation should not be optimized, random steps should be inserted, providing sufficient shielding and avoiding sending sensitive data on internal buses.

Sir Francis Galton proved in the late 19th century that fingerprints do not change over lifetime and that no two fingerprints are exactly alike [17].

In fingerprints are papillary lines (i.e. ridges and valleys), Pattern types (i.e. arches, loops, and whorls), core and delta points and minutiae points [9]. There are three types of fingerprint scanners optical scanner, solid state scanner containing capacitive sensors, and ultrasound scanner.

Fingerprint scanners have good accuracy; can be used for both identification and verification. They have low cost and problem with dirt, or when skin is too dry or too wet.

Fingerprints have medium universality, collectability, acceptability, and high uniqueness, permanence, performance and circumvention proof.

The gummy fingers [9] could be made by residual fingerprints, (enhancing, photographing, and image processing) fingerprint image (printing), mask (exposing, developing) and etching. [9]. (See Figure 2: gummy fingers)

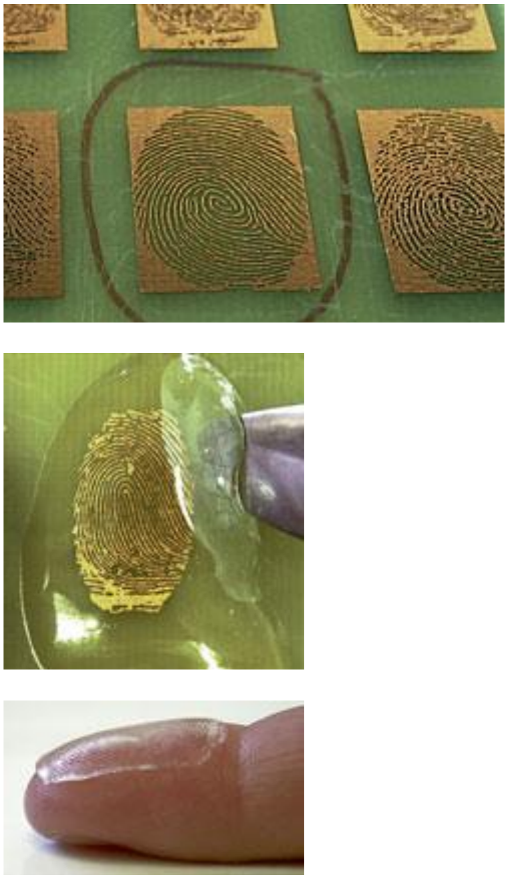

Figure 2: gummy fingers [9]

In TV series 24, key of stolen card is not filmed; we cannot see that how attacker got the key for card.

In making artificial fingerprints, image processing, enhancing, exposing and developing steps are not filmed.

In security engineering methods, there are two stances, default deny and default permit. Default deny means everything not explicitly permitted is forbidden. Default permit means everything, not explicitly forbidden is permitted [11].

According to the security engineering method, we can conclude two ways for protecting these steps: a card must have strong key, and latest fingerprint scanners should be installed which can differ the original and artificial fingerprints.

5. Results

After applying security engineering, we are able to cover the false scenarios with real life problems logic.

We selected three scenarios because they provide more fundamental concepts of security engineering as compared with rest of scenarios. Our main focus was to identify the physical security issues in these scenarios and cover it with security engineering.

The first step in security engineering is to determine objectives. A security policy should address information assets of organization, the damage that can occur to assets and the measure of protection to these assets. A security policy also specifies how to manage, protect, and distribute sensitive and critical information [4].

There are three phases in security engineering: requirement phase, design phase and integration phase.

In requirement phase we identify the trust requirements user and mission requirements and security concept of operation.

In design phase we apply design guidance and regulation. It has a separate set of guidance governing the design and development of trusted systems.

In integration phase we discuss the need of multilevel security policy and the multi-level security integration policy [4].

In secnario1 (breaking blowfish algorithm), requirement phase is to protect the credential, design phase is to choose secure password, and integration phase is that there should be a trusted third party which manages all password.

In secnario2 (a room could be opened from inside), requirement phase is well-guarded ventilation system, design phase is protection of unwanted access from inside and outside, and integration phase is that there should be protection system against inhaling toxins (See Figure 1).

In secnario3 (artificial fingerprints and stolen identity card), requirement phase is that smart card must have a private key, design phase is to implement more effective authentication system, and integration phase is that latest fingerprint scanners should be installed.

6. Discussion

The current situation in three movie scenarios is not satisfactory. The physical security issues could be covered by applying the security engineering method. The main advantage of this method that it covers security aspect in almost an ideal situation.

The physical security of a true safe room must contain safe ventilation system and should have duct and plastic system for prevention of any toxic gas in the ventilation system. (See Figure 1)

There are some environmental constraints and user acceptance for every method for implementation. For complete security engineering, deception of people by emotional methods, skill level of attacker and backup mechanism should also be considered. Complete security engineering also covers risk management, business continuity planning, and data protection along with physical security. The biometric methods can be implemented in parallel to other security methods.

In fact, the 24 is TV series with entertainment purpose, sometime with exaggerating way.

Guessing password in 30 seconds and breaking blowfish algorithm for opening, making toxin gas with ordinary household bleach, and making artificial fingerprints without image processing, enhancing and etching and developing steps are exaggerated scenarios and probability of such events are quite low in real life.

7. Conclusions

We evaluated that in real life how the probability of discussed scenarios is low and our theoretical point of view, regarding physical security is different from scenarios presented in TV series 24.

In case of breaking blowfish algorithm (scenario 1), a safe password must contain alphabets, numbers and special characters, so that password should not be guessed easily by bruit force. (See Table: 4 and Table: 5). There is also need to protect credential, so that no one could retrieve password by using them.

In case of safe room (scenario 2), the ventilation system, and other ways to access the room should be guarded, and a system that prevents harmful inhaling of toxin, should be installed (See Figure 1).

In case of artificial fingerprints and stealing identity card (scenario 3), every biometric methods used for authentication has some advantages and disadvantages. There is need to apply more effective biometric-based solutions should be applied like, iris, face recognition, DNA, and retina scan. There is need for implementation of more authentication methods with suggestion of experts.

The security engineering covers physical security, information security and economics of security.

References

[1] Bruce Schneier, Schneier on Security, “Blowfish on 24, Again” accessed on Mar 22, 2011 http://www.schneier.com/blog/archives/2009/03/blowfish_on_24_1.html

[2]C.ThomasJohnson“ProtectingYourWalls” accessed on April 13, 2011 http://www.rmmag.com/MGTemplate.cfm?Section=MagArchive&NavMenuID=304&template=/Magazine/DisplayMagazines.cfm&Archive=1&IssueID=320&AID=3653&Volume=55&ShowArticle=1

[3] Jon Sandys, Movie mistakes “24 (2001) - 152 mistakes in entire show:” accessed on March 22, 2011 http://www.moviemistakes.com/tv3007

[4] Marshall D. Abrams, Harold J. Podell, and Daniel W. Gambel”Security engineering” accessed on March 27, 2011 http://www.acsac.org/secshelf/book001/14.pdf

[5] Tom Sciacca “Safe room – Filter ventilation system “accessed on April 3, 2011 http://www.campingsurvival.com/hoandapsaro.html

[6] SearchSecurity.com Definitions “Physical security”, accessed on March 29, 2011

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1150976,00.html

[7] J.D. Meier, Alex Mackman, Blaine Wastell, Prashant Bansode, Jason Taylor, Rudolph Araujo “Security Engineering Explained - Chapter 3 - Security Design Guidelines” accessed on April 13, 2011 http://www.guidanceshare.com/wiki/Security_Engineering_Explained_-_Chapter_3_-_Security_Design_Guidelines

[8] The Internet movie database” 24 TV Series 2001–2010”, accessed on March 2, 2011 http://www.imdb.com/title/tt0285331/

[9] Viiveke Fåk, “Biometric User Authentication” accessed on April 1, 2011 http://www.ida.liu.se/~TDDD17/lectures/slides/tddd17_lec03_bio2.pdf

[10] Wikipedia, the free encyclopaedia”Blowfish (cipher)” accessed on March 22, 2011 http://en.wikipedia.org/wiki/Blowfish_%28cipher%29

[11] Wikipedia, the free encyclopaedia”Security engineering:” accessed on March 22, 2011 http://en.wikipedia.org/wiki/Security_engineering

[12] Wikipedia, the free encyclopedia “Serge Vaudenay” accessed on April 13, 2011

http://en.wikipedia.org/wiki/Serge_Vaudenay

[13] Wikipedia, the free encyclopedia “Vincent_Rijmen” accessed on April 13, 2011

http://en.wikipedia.org/wiki/Vincent_Rijmen

[14] Wikipedia, the free encyclopedia, “24 (TV series)” accessed on March 22, 2011 http://en.wikipedia.org/wiki/TV_series_24

[15] Wiley, “Software evolution and feedback theory and practice”, accessed on March 22, 2011 Chapter in Book

[16] “448-bit Blowfish encryption” accessed on April 3, 2011
http://www.mobystar.com/_what_is_blowfish.htm

[17] Wikipedia, the free encyclopedia “Francis Galton” accessed on April 30, 2011

http://en.wikipedia.org/wiki/Galton