# Evaluation of physical security in a Movie

Rhys Moyne – Pierre-Emmanuel Galisson

Email: {rhymo632, piega786}@student.liu.se

Project supervisor Juha Takkinen, juhta@ida.liu.se

Project Report for Information Security Course, Vt. 2009

*Linköpings universitet, Sweden*

## Abstract

*This paper focuses on evaluating three physical security scenarios in the TV series "24". We elaborate on a theoretical scenario, then analyse and compare the three selected scenarios that illustrate some of the fundamental concepts in physical security by using the* Deter-Detect-Alarm-Delay-Respond *method. After completing this evaluation, we find that "24"is often unrealistic from a security point of view. This is mainly due to the fact that the scenarios we used had a lack of coherence and were often too far-fetched compared to reality.*

## 1. Introduction

The last decade has shown a growing concern for security, whether it be on the domestic, governmental or corporate level. Indeed, the development of the Internet as well as the rate of progress in technology has made our systems, appliances and organisations more complex, and as a result, there are more flaws inside it. Since the attempts on the World Trade Centre on September 11, 2001, the western civilisation is becoming aware of the new threats they can face, and are developing countermeasures, risk analysis plans or continuity plans. These have not been developed in order to deter these kinds of attacks but to minimise the damage caused and the recovery time necessary. Security has become an important part of every organisation, and covers so many areas: data protection, risk management, business continuity planning, physical security, etc. that it is sometimes hard to cover the whole subject.

Moreover, our communication means have been increasing, leading to a "digitalized civilisation" in the western countries, and this poses a serious threat in many ways: If a skilled attacker can penetrate into a company network, a healthcare system, or even in the power distribution network, the consequences might be really devastating.

And of course, where there is money to be made, Hollywood is not far behind. Filmmakers have shot endless movies about technology and security issues. The first good one was (apart from the movie *Wargames*, which although a little bit far-fetched, showed the early attacks on computer networks[1]) *The Net*, released in 1995 where a software engineer is facing a compete identity theft [2]. Since then, many examples of what we call "security breaches" can be found in many movies but also in TV shows, like *Chuck* or *24*. They are often far-fetched, because security is not appealing or entertaining and you can't make money out of a product which doesn't have these features. That's the basics of marketing for entertainment.

In this project, our main problem is therefore to stress the differences between physical security depicted in these movies and the reality of this area, to show that somehow the filmmakers are calling for the sense, the feeling of security from the audience, or as Bruce Schneier states: the "Security Theatre", an array of countermeasures whose sole purpose are mainly to reassure people [3]. For instance, the TSA no-liquids policy at airports is less efficient on the long run than armouring cockpits doors. As examples are flourishing, we will mainly focus on the TV show *24*.

Basically, *24* is an American TV show, aired for

the first time in 2001, which portrays an event in real time. Each season consists of 24 episodes, in which an episode represents a time period of an hour. *24* focuses on an agency called the Counter Terrorist Unit (CTU) describing their efforts to protect threats in cooperation with the US government, through its main character Jack Bauer.[4]

The series has been famous after the main actor, Kiefer Sutherland, won a Golden globe for his performance in the first 10 episodes, and has in the meantime been also famous for the plot tools it uses to go on in the course of the season. Indeed, the frequent use of torture during the seasons has made a little scandal in the US, leading to season 7 being more focused on the moral aspects of torture [5](in the current season, Jack Bauer is under a subpoena from the US senate commission on CTU, and is always facing ethical questions regarding whether or not torture should be used to extract information from alleged villains). [6]

We decided on the TV series *24* for two main reasons. Firstly, the series is popular and familiar to us, making it easier to relate to. Secondly, as seven seasons have been aired from now (season 7 is currently being broadcasted in America) the series provides many examples of security scenarios that we can examine. Moreover, the complexity of the scenario provides us with many features useful for study, whether it is from a physical security standpoint or from a security engineer as a whole. The latest example of this is the use of Schneier's cryptographic algorithm, *Blowfish*, where a security analysts states that a "backdoor" is embedded in the code, and cracks it, revealing the data encoded in a matter of minutes [7].

Also, as the series has aired many episodes, we will narrow our project down to a handful of scenarios using an empirical method as outlined below.

Three specific scenarios will be examined which illustrate physical security of people, facilities and data. We first will provide a theoretical foundation of the concepts of physical security, using a lateral-thinking approach and Andersson's method called *Deter-Detect-Alarm-Delay-Respond* [8]. Then, we will describe the three scenarios. Each scenario will be described as shown in the 24 TV series' episodes. Then, details of what would actually occur in real situations will be described. Finally, a comparison will be made illustrating the main differences and similarities. After describing all three scenarios a conclusion will be made using concepts such as security theatre to explain the results. We will mainly use examples taken from the latest season 7, and deal for instance with scenarios such as a terrorist attack on a chemical power plant, or on a funnier level, the abduction of a Prime Minister from a foreign country.

Although at first glance this appears easy, we are expecting to face some risks and problems: First, we are not experts in the field and we might lack some theoretical knowledge. Secondly, as our method is mainly empirical and based on images, it is possible that we give a mistaken analysis of a scenario. Third, physical security is a very broad subject, so it might happen that we sometimes deviate from our primary subject.

## 2. Theory: current concepts, overview of 24

### 2.1. From alarms to social engineering, useful concepts for physical security evaluation

Physical security is an important part of the security of an organisation as physical features are part of the overall protection that is required [8]. This suggests that when considering a security policy for an organisation, physical protection should not be overlooked. An attack is possible to occur via physical means or via software means, so good protection of both is essential. Simply having adequate software protection of a computer system does not prevent the possibility of an attacker making use of physical means in order to access the system. However, physical security does not mean protection of only computer systems, it refers to the protection of any important asset as identified by an organisation. Whatever is being protected, the security concepts still apply, as physical security focuses on actual physical protection of the asset.

It is often the case that security solutions spend most of their effort on preserving the confidentiality and integrity features of a given item, even though availability is normally the key issue for a business. [8] As availability is normally the key focus of physical protection, it means that when considering security solutions, this goal should always be in mind. By doing this, an organisation will achieve protection that focuses on the correct issue, resulting in more effective results if an attack were to occur.

Despite their differences, physical security protection and software protection solutions should be designed in the same way using a model such as "deter-detect-alarm-delay-respond" for the various components of the solution. [8]. Generally the main parts are features that prevent an attack from occurring at all which could include things such as walls and doors, and features that detect an attack that has occurred such as alarms.

**Skill level.**

When the protection design is being considered, it is important that the attacker's skill level is considered [8]. The design should select a skill level that must be protected against, and then the features

that are decided upon can be based on the general capabilities of an attacker at this level. This basically means to design a solution based on the importance and expected attacks that occur as the resources available for a security solution are always limited. There is no point in designing a highly protected security solution for protecting something that has a very low value, the costs would outweigh the protection value. The opposite is also true.

**Deter**.

Features that are used to deter intruders can include choosing a particular location, appearance and restricting knowledge of where the critical area is [8]. A location can be chosen that is viewed as intimidating to potential intruders, thereby deterring the attack from occurring. A location that appears well-protected provides another factor that can deter attacks. Finally, if knowledge of where the protected area exists is restricted, it can be more difficult for a potential attacker to find where the area is. These features can be exploited by a physical protection design so that an attack is less likely to happen.

Barriers and walls are another deterrent feature. There should be consideration of what is to be protected as well as the attacker's skill level when selecting the location and type of barrier or wall [8]. Locks are also another common feature for prevention of an attack. However, the use of locks should be carefully considered with other elements of the protection design. Usually locks in a household are not very important as there are nearly always other ways of entering [8]. Also, locks are not perfect, there are ways of attacking locks such as bumping and master keys and they have revocation problems [8]. So again, the skill level of the attacker provides a reasonable way of deciding how much resources should be used for locks. It is now possible to make use of electronic locks which provide benefits such as live status updates, revocation, or location tracking but this also suffers from a key drawback : determining how to connect the locks together [8]. Deciding on what to use requires consideration of the protection requirements.

**Alarm**.

Alarms are used to provide notification so that a response can be made after an attack has been executed. An alarm is a key part of the protection, but needs to be considered with the rest of the design [8]. There is no use in having an alarm that successfully goes off when an attack occurs but there is a too large delay in the response. The alarm has then effectively become useless. So, an alarm may be a useful component, but it must work well together with the rest of the protection features.

When deciding on the alarm system set-up, there exists a trade-off decision. There needs to be a balance between the number of false detections and accuracy [8]. This trade-off is most important when considering the outer perimeter security as this is where there can be variations. One suggestion to help protect against false alarms is to have a security design in separate layers so that they can be prevented [8]. The different layers can then have differing amounts of security protection which increases closer to the critical core. This prevents less skilled attackers disturbing alarms at the critical core.

An attacker can subvert an alarm system in a number of ways. These issues should be considered in order to choose a design that helps protect against this. An attacker could use the alarm as a distraction or destroy the communication lines [8]. An attacker can prevent the alarm working by exploiting the people behind the system. The alarm system resources could be overloaded by the attacker thus stopping the system from working [8]. These are all issues to consider in the design of an alarm system.

**Social Engineering**.

Social engineering is a security issue that should not be overlooked, however it often is. It is quite straightforward for an attacker to fake things on a computer system and they can exploit the fact that there are always people behind a solution who can be manipulated [8]. Attacking systems through the use of people has been used for quite some time [8]. The attacks through social engineering methods exploit people factors and so therefore require different ways of protection than other issues. The social engineer can use emotional techniques in order to deceive people that they are someone else, allowing the attacker to gain the information they desire [9].

Even if the security of a system is of the highest grade, there is still the possibility of an attacker going around the problem by focusing on the human factors [9]. This means that in deciding on a security solution, social engineering attacks must be considered. The method of social engineering by an attacker uses quite simple tools but can become very powerful.

Using social engineering requires the attacker to make use of people skills so that they can deceive people into divulging information [9]. Usually, people will gladly help someone that needs it, so the attacker exploits this trait. Normally, the attacker requests information that appears to be useless or common knowledge [9]. This means that people do not consider the broad implications of revealing the information and so don't even realise that an attack has taken place. The social engineer uses persuasion when talking, making use of non-threatening

questions [9]. This makes the victim feel at ease and not to question the information that they give out.

As mentioned, the social engineers' main skills are quite basic. They communicate with the victim using persuasion by appearing friendly and innocent. In order not to appear out of place, the attackers normally learn the language of the company so that they sound as if they are genuine [9]. This suggests that companies need to carefully consider whether they are communicating with genuine sources.

In order to help counteract social engineering, it is recommended that there is a security policy that considers the confidentiality of information in a company and how it can be divulged [9]. This means that information that could be used by an attacker should be identified so that it is possible to train staff about incidents that could occur [9]. Training staff means educating them about the risks of social engineering and to ensure that when requests are made, they are verified. Verification of requests is an important method of ensuring that information is not disclosed to potential attackers [9]. This may prevent an attacker from using common knowledge in order to deceive and obtain the information that they desire. The main issue to consider is to educate people [8]. The attackers attempt to appeal to people's emotions [8]. They can use this to make people willingly give out the information that they want. When people are educated about what is possible with an attack, they will be better prepared to resist one.

Social engineering is often viewed as an unlikely event by many organisations. But, as displayed by the many fictional, but likely, stories in Mitnick and Simon [9], it is a real possibility that should be considered. A company's information may appear to be not all that important. However, this information may be the most important part; it provides a large leverage for the attacker to use to their benefit.

With these issues in mind, we can see that security does not simply refer to the common view of software protection. There are also physical factors that should be considered to protect the actual physical assets of the organisation. Additionally, there is also the human element of security. Through so called social engineering, an attack exploits psychological issues to gain what he wants. These two security issues must also play a role in protecting an organisation.

**Security Theatre.**

In addition to this, another concept has to be highlighted in this report, because it is highly related to the subject: the "security theatre" concept. When implementing security policies, governments and corporations often choose to favour visible controls over effective ones. For instance, TSA Airport use screening methods and tough control on everyday passengers, which is beginning to become highly controversial in the US, costing billions of dollars, while reinforcing cockpit doors would diminish the risk and cost less [10]. As Schneier states it, security is a trade-off [11]. You make decisions based on economic reasons, called risk analysis, but also on the feeling of security, i.e. the countermeasures to whatever threat that is going to make you feel safer. This is security theatre.

## 2.2. Overview of the 24 TV show

The TV show 24 is an action and drama TV series. It is currently broadcast by the Fox Corporation in the US, and has a worldwide distribution. First aired on November 6th, 2001, it depicts the work of a fictional character, Jack Bauer, who is working with the government in order to prevent a series of terrorist attacks or domestic threats [6].

24 is presented in real time, i.e. that all the events occurring during one season are supposed to take place in a 24 hour timeframe. Even though the first season was supposed to have only 13 episodes, the success met by the series have led to another batch of episodes to fill the first season. After that, six more seasons have followed, making 24 one of the longest running espionage series. There are currently 168 episodes, representing a total sum of roughly 118 hours of watching. Each episode is 42 minutes long, one hour with commercial breaks. Another feature has been released as well, called *Redemption*. This 2-hour movie takes place between seasons 6 and 7, and aims at reducing the time-lapse between these two seasons. [4]

In this show, the main character, Jack Bauer, is working for an inter-governmental agency called CTU (Counter-Terrorism Unit), a fictional counter-terrorism agency supposed to having been created by Bill Clinton in 1993 in response to the World Trade Centre bombing. Jack Bauer is most similar to a Paramilitary Operations Officer in the CIAs Special Activities Division. CTUs headquarters are in Washington, D.C., with satellite operations in major cities where threats are likely. CTUs primary mission is to disrupt and foil foreign and domestic terror cells hostile to the US, as well as protect it from terrorist attacks. [6]

In season 7, a group of corporate terrorists are working with soldiers from a fictional and remote African dictatorship, Sangala, ruled by a general named Juma. This dictatorship has been attacked by US soldiers following some massacres in the country, and these terrorists want to repel the

invasion. Therefore, they have kidnapped an American engineer and forced him to build for them what they call a CIP device, a tool enabling them to breach into any governmental or non-governmental American network, and to take control of facilities such as the ATC (Air Traffic Control) system, a chemical power plant, and so on. No information is given on the meaning of the acronym CIP, however our guess is that it stands for Critical Infrastructure Protection [12]. Moreover, the former prime minister of Sangala, M. Matobo, is in exile in the US and is meeting with the American President, Mrs Taylor, in order to discuss the future of Matobo's country after the intervention of US troops.

Jack Bauer, under a subpoena issued by the American Senate, is asked to collaborate with the FBI in order to repel the series of threats, through direct consequences of the CIP device. Having discovered that a huge conspiracy is running, in which the terrorists play a small role, he goes undercover with his partner and friend Tony Almeida and is enrolled into Emerson's team. Emerson is a former SAS (Special Air Service, the British Special Forces) agent who has become a mercenary [10].

## 3. Deeper evaluation of 24

In order to theoretically build a scenario of each of the 3 examples below, we will use the *Deter-Detect-Alarm-Delay-Respond* method [8]. For each part, we will describe the most efficient means used, and the theoretical problems raised by them.

### 3.1. Scenario 1: Abduction of a prime minister in a safe room: 24 season 7 episodes 4 and 5

We chose at first glance to evaluate this abduction scenario, because it reflects a concept shared by many security analysts, familiarly known as the "Nasrudin's tomb" [13].[1] This is all but a legend, yet this illustrates the concept that whatever state-of-the-art security tool you have for one aspect of the system, you have to consider security as a whole and not focus all your concerns on one single part of it, otherwise your countermeasures or policies are useless.

In this scenario in *24*, still part of Emerson's crew, Jack Bauer and the team have to abduct the former Prime Minister, M. Matobo, who is kept under heavy guard in a Secret Service's house, a location that is supposed to be secured.

Let us try to figure out how to succeed in this mission, and therefore make a coherent and realistic scenario. First, we have to point out the high importance of the target: a Prime Minister, whose country is currently on the verge of being invaded by troops belonging to the country in which he is in exile. This means that the prime minister is supposed to have large protection. Then, we have to evaluate the attackers: according to the 24 scenarios, Jack Bauer and Tony Almeida are former operatives from CTU, both were before that enrolled in Special Forces and in many operations. Moreover, Emerson and the rest of his crew are former SAS agents, so the level of knowledge and training of the attackers is high.

**Deter:**

Here, the most efficient deterring methods will, in our opinion, not work, mainly because the attackers are highly trained, have huge resources, and therefore will not be impeded by barbed wire, fences, CCTV cameras or guards. Moreover, the location of the Prime Minister is supposed to be kept secret, so any deterrence means might jeopardize the secrecy – it is obvious that there is a high-value target in a facility where heavily armed guards are patrolling.

**Detect:**

The first idea is to set up CCTV cameras in the outer perimeter, i.e. in the neighbourhood, to check any strange traffic activity, and hide them as much as possible.

In the garden, it is preferable to put as less trees, bushes or ornaments as possible, to detect more efficiently any activity. Infrared or laser motion sensors should also be set up there, hidden as small ornaments (i.e. alley lights, automatic hoses,…). Moreover, CCTV cameras in close-circuit should be put on the walls and cover every part of the perimeter, to detect the attacker's point of entry in the house.

In the house, one should avoid electronic locks, which are easier to exploit by DoS (Denial of Service) or avoidance attacks. In the case of an attack or escape, having one key to open every lock might be useful either to close doors as a delaying means, or to have an easier escape route. Having double, triple-glassed windows or even bulletproof ones can also be a means to avoid eavesdropping or to reduce casualties. Moreover, the guards must be

1 Nasrudin is a character from the Persian and Arabic folklore, and is the subject of many jokes, in which he often appears as a fool. Legend says that he wanted to be buried in a tomb where his remains and ornaments would be safe. So, he tried to find the most skilled carpenters, locksmiths and craftsmen in order to have the most unbreakable door at this time. After a while, the door was made, and set up in front of Nasrudin's tomb. Yet, even though the door was unbreakable, the walls of his tomb were nonexistent and shortly after he died his tomb was looted.

completely aware and well-trained so that they can detect any abnormal disturbance.

**Alarm:**

The alarm will mainly depend on the guards training: the higher the level of training and awareness, the lower the detection and alarm time. In this scenario, the guards must be a group of trusted and loyal soldiers applying a strict set of protocols: in the case of any small disturbance, they set off the alarm and put the asset into a secure location. Moreover, as the attackers are highly skilled, an alarm must be connected to the FBI or any governmental agency that can send a backup team as soon as possible.

The problem is that a DoS attack can easily shut down this alarm system.

**Delay:**

Here, any possible means for delaying the attackers will be necessary. In addition to the heavy doors and locks, the size of the house can be an advantage by delaying the time required to abduct the target. Lots of furniture can also be an asset as it can provide cover for the defending people –but also for the attackers as well.

As a last resort solution, a safe room can be used to protect the target. A safe room is a lockdown room with thick concrete walls, roof and floor, a heavy and "unblastable" door that can only be opened from the inside once it is closed. This can be used to repel coercion or manipulation from one surviving soldier. This room should be well aerated so that the people inside can breathe normally while waiting to be rescued.

**Respond:**

The response part is due to the level of training and the equipment of soldiers: the more they are trained, and the more they are acquainted with the facility, the easier it is for them to get rid of the attackers. Yet, bear in mind that they are highly skilled, as they are former Special Forces.

Moreover, the response time from the "task force" sent by any external agency, and the training of their units is also important: these units will have to arrive on scene as fast as possible, and they will also have to be able to counter the firepower of the attackers.

**Problems:**

The first problem with this scenario, and the most important one, is that it does not take into account the "insider" case: someone of the Prime Minister's guard might be manipulated, blackmailed or paid to let Emerson's team in the building without being seen, thus making the abduction faster and easier.

Denial of service is also problematic here, especially in the "detection and alarm" part: for instance, if the guards are called because the alarm went off due to an animal crossing the detectors, they will rely less on the system and not respond accordingly when facing a real threat.

Moreover, the training of the response unit could be a problem as well. If for example in the procedure, the agency in charge of rescuing the target has to send a normal police car every time the alarm goes off, the "average cop" might not be able to face a threat of this magnitude.

As a result, in this scenario the best strategy is to adopt the "brute-force attack": Go in there as fast as possible, kill everyone except your target, and leave the scene before the cops come. Having an insider would be a bonus, but the timeframe is too short here.

Now let's have a look at the "real scenario" from 24. Emerson and his team have at first some intelligence regarding the schematics of the house, provided maybe by the mole inside FBI. So before they move in, they are acquainted with where the Prime Minister should be. Yet, in the meantime and probably to make the action more theatrical, a FBI agent, Renee Walker, finds out about the abduction by interrogating a suspect apprehended a few hours before. So she calls her boss, who warns the minister's guards about the imminent threat.

While the guards scramble to lock down the prime minister, a mercenary switches off the alarm, allowing Jack Bauer and the others to attack the house. They encounter little resistance, i.e. 4 guards armed only with handguns and apparently without vests, which should lead to an easy capture. Yet, one of the guards has time to lock down the minister in a safe room, which can only be opened from the inside. According to the clock, the attack took less than one minute.

Now that the prime minister and his wife are locked down, Emerson tries to question one of the remaining guards, who after some torture tells them that the door can only be opened from the inside. Therefore, Emerson's team is trying to find a way to bypass the problem of the door. They first try threatening the prime minister that they will kill the guard if he does not open the door from the inside of the safe room, but this threat fails. Then, Jack finds access to the ventilation grid, and pours in a mixture of household products, creating a toxic gas which slowly fills the safe room.

After a short while, the prime minister's wife, who is unable to withstand it any longer, opens the

door and both are abducted by Emerson's team. The SWAT team, who left FBI a few minutes after the attack was performed, was too late, and the whole abduction, according to the series' clock, took less than 20 minutes to be completed. [14]

Is this scenario realistic? First, our theoretical evaluation suggested that the brute-force attack was the best option possible and that is what happened. Yet, it is quite astonishing that 4 guards armed only with handguns were there to defend the prime minister, and that none of them were checking the garden (all of them were in the same room when the FBI call arrived). Moreover, there is no sign at all of CCTV surveillance of the house, either inside or outside it. We can see for a few seconds the prime minister checking the cameras from the "safe" room, but that is all.

We can also notice that one of the mercenaries is shutting down all communications and alarms, from a panel apparently located in the garage. If so, how was he able to come inside without being detected? And why is this panel not better protected or located in a better place?

During the attack, three guards are killed or seriously injured. Two of them were standing next to huge windows, while the third one was shot in the garden. Were they dumb enough not to shoot from a covered area? From this and the fact that none of them were carrying automatic weapons or bulletproof vests, we can assume that their training was not sufficient, or that they were completely unwary.

In order to open the door to the safe room, the team first attempts coercion, by threatening the minister to kill the guard if he does not open the door. This is actually plausible, and is one aspect of social engineering.

Then, as this fails, they find a flaw in the "safe room": the ventilation system is easily accessible, so, in the scenario, Emerson's team releases a household-made toxic gas into the ventilation system of the safe room. We are not professional chemists, but our guess is that this might be plausible as well, as household products such as bleach can contain chlorine, which is one of the basic components of the first combat gases used during WWI, called Phosgene [15]. The most known one, Yperite or "mustard gas" was used later on, for the first time in Ypres in 1917, and is not likely to be made from household products [15].

Indeed, one of our friends, who is a chemist, told us that this is plausible because of bleach, which is widely used in houses [2] [16].

We can also point out the inefficiency of the response team: they went in a van, from an office located far from the scene. Knowing the importance of the target, they could have used a helicopter instead of a van in order to avoid traffic and be there in time. This is another flaw of the scenario: by not using the fastest means of transportation, it gave time for Emerson's team to escape.

Finally, as the attackers are leaving the house, they put the prime minister in a yellow van, located in the courtyard behind the house. This raises suspicion: how could the van be driven to the backyard without being detected, either on CCTV or by the guards that are located inside the house?

As a result, we can assess that even though this first scenario is technically plausible, many discrepancies and security flaws are discrediting the plausibility of this scenario.

### 3.2. Scenario 2: Stealing information/identity theft: Season 7 episode 19 (2:00am – 3:00am)

We choose to evaluate this scenario because this is a good example of identity theft linked to physical security.

In this scenario, Jonas Hodges, who is one of the conspirators that aided development of a biological weapon, is arrested for an unknown reason. Upon being arrested, his attorney, Patricia Earnes, is notified about this development and told that she should see her client as soon as possible. As Patricia prepares to leave her house, she is suddenly sprayed with an unknown substance, knocking her to the floor. The attackers then sedate her by injecting some kind of substance using a syringe [14].

The sedated attorney's purse is then searched for her identification cards which the attackers steal. The attackers also take a sample of her fingerprint and place this onto what appears to be a transparent jelly surface. Among the attackers is a woman looking similar to Patricia Earnes. She takes the identification cards and places the jelly surface onto her index finger. The attack took just a few minutes,

---

2 Bleach is originally a solid NaClO, and when put in a solution creates ions $ClO^-$ and then becomes HClO ions in an acid solution (using chlorhydric acid which one finds in houses). These ions react like this:

$$HClO + H^+ + Cl^- = Cl_2 + H_2O$$

$Cl_2$ is a highly toxic gas, and when exposed over a certain level, it is deadly.

maybe no more than ten, for both the break-in and the ID theft, which means that in this timeframe there could be no response at all.

After this attack, the “fake” attorney enters the Secret Service building in which Jonas Hodges has been placed under custody. Upon entering, she presents the stolen identification cards to the administration which validate without a problem. Her fingerprint is also checked, passing authentication due to the use of the synthetic fingerprint placed above her finger. These are the only checks that are made of the attorney's identity.

The “fake” attorney, who is known by Jonas Hodges, is then able to speak with him. Jonas originally believes that she will aid him in escaping from prison. However, instead Jonas is threatened due to his erratic behaviour and unauthorized use of the biological weapon. His co-conspirators are afraid of their identity being revealed. The “fake” attorney gives Jonas a red pill and threatens that his family will only be safe if he takes it, therefore killing himself [14].

In order to evaluate this scenario, we firstly consider the experience level of the attackers. The attackers are part of a group of accomplices that are in some way connected with the development of a biological weapon. Therefore, their skill level and amount of resources available is extremely sophisticated. The attackers are likely to have some kind of advanced training and due to their connections, they have a large amount of money for obtaining any resources that may be required.

The resources used by the attackers are relatively minimal. Firstly, some kind of spray is used in order to render the victim unconscious. Then, a drug is injected into the victim so that she is sedated. Finally, the attackers have some specialised type of computer. This computer reads the fingerprint data stored on the identification card of the victim and then creates a thin transparent layer where the fingerprint is drawn onto it. These are the only special tools that are used by the attackers. The spray and drug could quite easily be obtained by attackers of this level of skill. The same is true of the specialised computer. It is quite plausible that this machine was developed for them based on their requirements. However, the ability to create the transparent layer in real time may be slightly exaggerated. Regarding whether the tools used are actually possible, it would seem that it is so. The spray and drug seem both possible with current medical knowledge. Similarly, making use of synthetic fingerprints is a known attack against fingerprint readers which is described by authors such as Schneier [17].

Below we consider the possibilities of protecting against such an attack, using the same method as the one for the first scenario.

**Deter:**

In the case of deterrents, the attackers had a lot of knowledge of their victim. They knew when the victim was going to leave the house, thus providing a good opportunity for this attack. As the skill level of the attackers was very high, most deterrents implemented within the vicinity of the victim’s house are likely to be subverted. In this case, it seems that the skill level of the attackers is too high for most deterrents. However, as mentioned below, the specific checks performed to verify the identity of the attorney can be an additional deterrent.

**Detect:**

Detecting an attack such as this can be via monitoring of the victim. In the case of this attack, the attackers exploited the fact that the victim was not considered someone that requires constant protection. Therefore, detection of such an attack will likely take some time.

Methods to aid detection include providing monitored surveillance, personal guards, and living with others. Surveillance of the outside perimeter of the house may also provide a means of detection. Another method of detecting the attack could occur during the time that the synthetic fingerprint is checked.

It is possible to make use of fingerprint readers that provide some kind of protection against use of these synthetic fingerprints [18]. ”Sweeping” readers, such as the ones on some professional laptops or USB sticks are somehow more efficient than touch sensors, due to the latent prints [19]. Here, because the facility where Jonas Hodges is located belongs to the secret service, biometric readers should be more precise and able to detect either by ultrasound techniques or by other means the “liveness” of the fingerprint. If one of these fingerprint readers were used, the synthetic fingerprint may not pass validation and therefore the attack could be detected. Furthermore, there could be additional identification checks introduced when checking the identity of the attorney. By implementing more checks, it may make the attack more difficult for the attackers to perform the attack, and thus this may even be considered a deterrent.

**Alarm:**

An alarm notification of an attack such as this depends heavily on the methods of detection. This particular attack is quite simple for skilled attackers such as these without causing any disturbance. Once the attack has been detected, there should be a way that the victim can disable use of their stolen

identification cards and fingerprints. In this case of the identification cards, revocation can be possible relatively easily. Revocation of biometric identifiers is more difficult as they are permanent features of someone [18].

**Delay:**

After detection and notification of the attack, it can be delayed through a number of means. Use of secure doors and locks and other entrance points may help delay the attacker from gaining access to the victim. The house layout can also help, with places where the victim is able to hide from the attackers. Identification checks involving communication with humans may also delay the attack process.

**Respond:**

When it is time to respond to an attack, due to the high level of experience of the attackers, there needs to be a highly trained response to the attack. The skill level of the response team must be capable of counteracting the attackers. Additionally, the response time needs to be within a reasonable period before any delaying attempts outlive their usefulness. Yet, as the target is of no high value, this could look like a normal robbery and therefore the response may not be appropriate. Moreover, the timeframe of the attack is too short to trigger any response.

As can be seen from this scenario, the main issue is the skill level of the attackers. When the skill level of an attacker is extremely high, it becomes relatively easy for them to perform an attack on a victim that is not considered of high importance. The attackers are able to make use of the false assumption that an attorney is not a valuable asset that should be protected. The protection resources of the victim are unable to prevent against attackers with a high skill level. Additionally, the limitations of identification checks need to be considered as it is quite possible for this to be exploited.

### 3.3. Scenario 3: Entertainment takes over reality, Attack on a chemical power plant: Season 7 episode 7

This episode was chosen because, as you will see below, this is a perfect example of how entertainment is taking over security. Here, it is the least probable and so it is the most astonishing scenario that has been chosen.

In this scenario, the conspirators are targeting a chemical power plant in order to create a terrorist attack by releasing toxic gas on nearby cities.

First of all, we have to make a theoretical evaluation of this type of attack, in order to have some insights of how this could be prevented. We will again use the Deter-Detect-Alarm-Delay-Respond method described by Ross Anderson [8]. We will also only consider highly-skilled attackers, in order not to widen too much the span of our study.

A chemical power plant is not like any other company or facility, therefore the protection and security level vary due to the components stored. Moreover, employees are provided with special training in order to quickly react in case of disaster. In some countries, such sites are under strict regulation, like for instance the SEVESO directive, set up by the European Union following the Seveso chemical disaster in 1982 [20].

**Deter:**

Fences and barbed wire should be the least protection used in order to deter passers-by and regular thieves. In addition to that, private security companies are often on site, providing guards, and sometimes tough controls at entry points. CCTV cameras can also be an efficient tool for deterring people, yet highly skilled attackers, such as in this case, are not likely to be intimidated by this.

**Detect:**

Like the previous scenario, guards and CCTV cameras are the most effective, both in terms of security and costs, in order to detect any physical breach in the perimeter. Motion sensors would be quite costly for a huge facility like this, therefore these should be reserved only for highly sensitive areas. In case of breach into the network, (provided that the facility is networked) an Intrusion Detection System should be set up. As such, facilities are often monitored 24/7, where any abnormal change in pressure, temperature or any other parameter can be detected.

**Alarm:**

In case of perimeter breach, i.e. intruders in the facility, regular alarms should go off. Moreover, security guards should be able to quickly react when they detect any disturbance, but the time between the moment they detect something strange and the moment they set off the alarm will vary depending on their training and awareness. If the system still works, any sudden change in the gas parameters will automatically trigger an alarm.

**Delay:**

If the attackers are skilled, it may be quite difficult to delay an attack. Indeed, security guards from private companies, if we exclude contractor ones such as Xe, the former Blackwater company, are often not trained to counter attacks from highly trained mercenaries [21]. Moreover, only nuclear power plants are protected by a military force, and only in case of special events or high alert level [22], so guards might not have enough firepower to delay and respond to a brute-force attack.

In case of system breach, i.e. attackers taking control of the system, measures could be taken, like for instance

flowing the gas into an empty tank if the first one is leaking, or shutting down some valves.

**Respond:**

If the alarms are properly configured, and if the managers or guards know enough about the threat they are facing, they can either try to defend themselves, or send all the information they have obtained to the police so that the latter can set up an appropriate response. The main parameters here will be the time for the policeman/woman in charge of the call to alert the chain of command, the time for the people in charge to set up a team, and the time for the team to arrive on scene. Here, the attackers are skilled, and so, as stated previously, the security guards might not have enough training and firepower to repel them.

Hence, many types of attacks are possible: one can for example try the brute-force attack, where one enters the compound heavily armed after having cut the alarm, quickly puts some explosive or triggers some valves before the manager or the person in the control room has time to respond, and blows off the tank, releasing the toxic gas in the air. The attacker can also try to have some insider to make the attack easier, either by letting the attacker in or by making the insider do what the attacker wants to do.

In the scenario, Dubaku has a plan to attack the Boyd Chemical Plant by making use of the CIP device. The plan is to take control of the plant so that toxic chemicals can be released, potentially killing up to 17,000 people. Dubaku hopes that the impact of this attack will force the president to respond to his requests [14].

Janis Gold, FBI analyst, notices a potential breach of the CIP firewall by seeing some kind of code fragment that is being generated. This is an indication of the attack taking place by Dubaku. After noticing this signal again, combined with the location of the signal, a colleague of Janis' wonders what is located close by to the signal source. Janis and her colleague examine a map and find out that there is a nearby chemical plant, the one under attack by Dubaku [14].

Upon discovering that the chemical plant may be under attack, Janis contacts the manager of the plant, John Brunner. She finds out from John that the plant has been experiencing problems with the main tank. After hearing this, it confirms her suspicions of the terrorist attack and so she immediately informs John about this, asking him to shut down the plant. John Brunner attempts to shut down the plant using the computer system but finds out that they have lost control over the system. Therefore, John Brunner decides to release some valves manually in order to give some more time before the attack has an impact [14].

As this occurs, a group including Jack Bauer has been going after Dubaku. They manage to infiltrate his defences causing him to panic. He stops the attack on the plant and escapes, leaving behind the destroyed CIP device. The attack on the chemical plant was unsuccessful [14].

Firstly, we examine how the attack was possible. Dubaku made use of the CIP device in order to penetrate the CIP firewall so that Dubaku's attackers could access the computer systems of the chemical plant. The CIP firewall is supposedly some kind of system meant to prevent outsiders from accessing critical systems that should be protected. The CIP device is able to penetrate the system of the chemical plant and thereby gain access to the protected systems behind the CIP firewall. This attack is not physical and so the physical protection features of the plant are irrelevant for this case.

A first consideration should be whether the systems of the chemical plant should be accessible from the outside world at all. It may be the case that some systems need to be accessed remotely but the critical functions should be separated from the global network. This would make a breach of the systems remotely quite difficult unless there is an unidentified link available to a remote location.

Penetration of the CIP firewall with the CIP device could be possible. It is impossible to have a fully perfect security solution and so it is possible there is some way of bypassing the CIP firewall. However, the CIP firewall is used to protect many critical services and so it is expected that it would be quite difficult to bypass.

Assuming that it is possible to gain access through the CIP firewall, it is questionable if it would be possible to use the system to release the toxic gases. The system is surely going to have systems that monitor the amount of gases released and provide protection against undesirable emissions. If large changes have been made, the system should prevent these changes from occurring and provide some kind of notification so that the attack can be identified. Also, once some kind of an attack has been identified a chemical plant would have well defined procedures to prevent any major problems occurring. It is likely that the system would shut down and alarms would notify the appropriate personnel.

In the episode, the chemical plant loses control of the computer system and cannot shut down the plant using the system. This seems implausible as the people in the plant have physical access to the system meaning that there should be some kind of way of manually shutting down the system when things go wrong. It should not be possible for an external attacker to have greater control over a system than the personnel with physical access.

We can see that this third scenario, as portrayed in the TV series *24*, seems quite unrealistic. The main issues are how it was possible to access the system at all, how it was possible to perform the attack without detection and how it was not possible for the personnel within the plant to stop the attack.

## 4. Conclusion

We examined three scenarios from the TV series *24*, and compared them with our theoretical viewpoint on physical security. From our evaluation, we found that almost every time, the scenarios from the series are far-fetched, and that even though some of them might be realistic, there are always some aspects which discredit them. The attack on the prime minister in the first scenario shows for instance a huge syndrome of the "Nasrudin's tomb", by focusing only on the door of the "safe" room, and not on all the outer security aspects. The ID theft in the second scenario, even though plausible, is not doable in the timeframe described in the episode, and surely not with the devices used. Finally, to add fuel to the fire, the attack on the chemical plant in the third scenario is quite unrealistic even though the latest news has shown some breaches in American governmental networks [23].In addition to that, we ought not to forget that *24* is a TV show, and so its main purpose is to entertain, which means that sometimes the writers need to exaggerate things to keep the audience watching. Moreover, our evaluation focused only on the type of attackers with the same level of skill as Jack Bauer and other protagonists, and therefore the probability of such events is quite low in real life.

## References


[1] "Wargames", *The Internet Movie Database*, accessed May 22, 2009, http://www.imdb.com/title/tt0086567/

[2] "The Net", *The Internet Movie Database*, accessed May 27, 2009, http://www.imdb.com/title/tt0113957/

[3] Schneier, B, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, Copernicus Books, 2003

[4] "24", *The Internet Movie Database*, accessed May 17, 2009, http://www.imdb.com/title/tt0285331/

[5] Clive James, "The clock's ticking on torture", *BBC News*, March 30th, 2007, accessed May 27, 2009, http://news.bbc.co.uk/1/hi/magazine/6510593.stm

[6] *24 (TV Series) Seasons 1-7*, Fox Broadcasting company, 2009.

[7] Schneier, B. "Blowfish on 24, Again", *Schneier on Security*, March 19, 2009, accessed April 12, 2009, http://www.schneier.com/blog/archives/2009/03/blowfish_on_24_1.html

[8] Anderson, R., *Security Engineering* 2nd edition, Wiley, 2008

[9] Mitnick, K. and Simon, W. *The art of deception: controlling the human element of security*, Wiley, 2002.

[10] Zack, P. "*FEATURES Security Theater*", 2007 http://www.govexec.com/features/0807-01/0807-01s3.htm.

[11] Schneier, B. "The Feeling and Reality of Security", *Schneier on Security*, 2008, accessed April 29, 2009 http://www.schneier.com/blog/archives/2008/04/the_feeling_and_1.html

[12] "What is CIP and why is it important?" *US Fire Administration*, accessed May 27, 2009, http://www.usfa.dhs.gov/fireservice/subjects/emr-isac/what_is.shtm.

[13] Shah, I., *The pleasantries of the incredible mullah* Nasrudin, The Octagon Press, 1995.

[14] *24 (TV Series) Season 7*, episodes, 4, 5,7,19, Fox Broadcasting company, 2009

[15] Karlsson, L, *Chemical weapons: threat, effects and protection*, L K Engman et al. Swedish Defence Research Agency (FOI) Briefing Book, ON, 2002.

[16] Personal communication, April 23, 2009, mail, friend of Pierre Galisson and engieer in *génie chimique*.

[17] Schneier, B *Crypto-Gram Newsletter May 15th, 2002*, accessed April 25, 2009, http://www.schneier.com/crypto-gram-0205.html.

[18] Blommé J. "Evaluation of biometric security systems against artificial fingers", *Institutionen för systemteknik*, Linköping Uiversity, 2003.

[19] Maltoni, D. et.al. *Handbook of Fingerprint Recognition*, Springer Verlag,2003.

[20] *Chemical Accidents (Seveso II) - Prevention, Preparedness and Response*, last accessed April 20,2009 http://ec.europa.eu/environment/seveso/index.htm

[21] *XE's corporate website*, accessed May 27, 2009 http://xecompany.com/

[22] Lamm, V. *La protection des installations nucléaires civiles dans les conflits armés*, 2002, accessed May 27, 2009 http://www.nea.fr/html/law/nlbfr/nlb-72/029-040.pdf (in French)

[23] Markoff, J. "Vast Spy System Loots Computers in 103 Countries",*The New York Times*, March 28, 2009, accessed April 27, 2009 http://www.nytimes.com/2009/03/29/technology/29spy.html?_r=1