Training Method : Awareness to Computer Security for a Neophyte Audience v0.2

Tiphaine Romand-Latapie

06/05/2015

Résumé

The document describes how to train a neophyte audience to the basic principles of Computer Security. This method is based on a role playing game, invented by the author. The reader will find in this document the information needed to carry out the training.

1 Copyright

Contact :

`tiphaine.romand@orange.com`

`tiphaineRL@gmail.com`

The concept of this methodology is born from the need to train an operational and neophyte audience to the computer security stakes. According to the author experience, standard training focused on the technical context (what is a password is, how does a computer work etc.) tends to bore or scare a neophyte audience. An alternative would rather be to concentrate on the generic principles of InfoSec :

— The decision whether or not to trust an entity/a person

— The notion of in-depth defense

— The attacker's motivations

— The attacker : stereotype versus reality (he is not necessarily a "genius hacker")

— The necessary trade-off between operationnal constraint and security

— The goals of the security team (forecast the attacker's behaviour, prevent or detect the attack).

The concept of the training stems from the fact that basics principles, in particular the followings, are the same for physical or computer security :

— In every day life, we have to decide who we trust.

— In physical security, we always work on the worst-case scenario and we handle the cases where the basic security measure is deactivated/ineffective.

— Attackers' motivation are money, ideology etc.

— The most common attacker is a not crime genius.

Physical security brings constraints too (lock the door, carry a badge, perform security check at the airport etc.). These constraints serve the same goal : forecast the attacker's behaviour, prevent it or detect it.

Yet, a neophyte audience is more familiar with physical security than with computer security, in their everyday life or professional life. We lock the door before going out, we don't let anybody enter our home, we've all already gone through security checks etc.

The core idea of this training is therefore to make neophyte people realize that they already know security best practices. They only have to learn how to apply them to computer security : they do so in a fun way, while playing the game.

2 The role playing game

The training is developped around a role playing game consisting in attacking and defending a building.

2.1 Rules

The game is led by a Game Master (GM) and involves an attack team and a defense team.

2.2 General description

— The action takes place in an office building located in a dense urban area, with an underground parking lot and an helicopter landing strip. A highly valuable object (fitting in a backpack), used by employees during the day, is stored somewhere in the building.

— At the beginning of the game, the building is not secured at all.

— The attackers propose an attack, the defenders a mitigation, in an iterative way.

2.2.1 Attack team's rules and goals

— Goals : steal the object without being caught.

— Rules : unlimited budget, limited number of human attackers in the game (no more than ten person). Physics rules apply (gravity, etc).

2.2.2 Defense team's rules and goals

— Goals : prevent the theft or retrieve data allowing to catch the attackers.

— Rules : unlimited budget, unlimited staff. Physics rules apply, the law must be respected, employees must be able to work in the building during office hour.

2.2.3 End of a scenario

— I recommend to stop the current exchange (called "scenario" in the following) when teams get to a blocking point (everybody is dead, the object is destroyed, the police has arrived ...).

— It is then possible to move on a new try of the attack team. The defenders are keeping all the security measure already deployed.

— If the players want to, or if the GM wants to revive the game, it is possible to switch the team : the attackers become the defenders and vice versa.

2.2.4 End of the game

— There is neither winner nor loser !

— I recommend to do multiple scenarii during one game. The duration of the session is a choice of the GM, (forty to sixty minutes is a good duration for a 6 player game).

— The session is followed by a debriefing by the trainer, allowing him or her to highlight the concepts (see the "Debriefing" section).

2.3 Behind the rules

2.3.1 The playing environment

The playing environment (building, dense area etc.) was chosen to maximize the playful side of the game and facilitate its application to the training :

— The fact that the building must be usable by employee during the day allows the trainer to work on security versus constraint compromises and offer a familiar environment for the players.

  — It can be a good idea to personalize the details of the game using the players' professional environment : company's building, its key product, etc. This allows a faster immersion and involvement from the players.

— The choice of a dense area, as well as the helicopter landing strip and the underground parking lot, reinforce the fun part (the attackers can think of helicopter landing on the roof, can jump from a building to another etc.) and guides the players. Furthermore, it helps diversify the scenarii.

— The choice not to further detail the environment has been made to let the players' imagination run wild and to simplify the rules of the game.

— The usability of the object during office hour allow us to stay clear of non constructive mitigation, like “we cast the object in concrete”.

— The location of the object within the building is let free, it can change during the game if the defenders wish so.

— Beginning with a non-secured building is important :

  — It allows the trainer to work on the security measure stacking and on the principle according to which the attacker always seeks the easier way in.

  — Sometimes, the attackers consider that there is basic security in the building (locked door, CCTV etc.) . In this case, it’s not essential for the GM to recenter the frame. It is, however, interesting to make the players think about it during the debriefing.

— Fast exchange allow a living and fun game.

2.3.2 Attackers’ rules and goals

— A simple goal, sending back the players to Blockbusters, easy to translate in computer security goal (going in and out without leaving trace).

— The unlimited budget simplifies the game, futhermore, it is always possible to discuss financial aspects during the debriefing.

— The small number of human being authorized for the attack team during the game allows us to stay clear of non realistic scenario like “laying siege with a tree hundred people army”.

— Respecting the laws of physics allow us, once again, to stay clear of non realistic scenario or unsporting behavior.

2.3.3 Defenders’ rules and goals :

— A simple goal, sending back the players to Blockbusters, easy to translate in computer security goal (controlling the ways in/out, slowing down the attackers etc.).

— The unlimited budget simplifies the game, futhermore, it is always possible to discuss financial aspects during the debriefing.

— The unlimited staff is here to compensate a little the need to respect the law, while allowing the trainees to experience that sometimes expensive security measures can be uneffective.

— Respecting the laws of physics allow us, once again, to stay clear of non realistic scenario or unsporting behavior.

— Respecting the laws of the country reminds the trainees that IT security engineers have to do the same.

2.3.4 Losing and Winning

There is neither loser nor winner, even if the teams usually want to name one. Rules to define winners/losers would made the game more complex with no reason. The rules aim at stimulating fun exchanges between players while bringing out the idea needed by the GM to achieve the training.

2.4 The facilitation of the game

The trainer, also named Game Master (GM), facilitates the game. It is essential to forme small teams. I recommend two to three defenders and the same for attackers. beyond this number, it is very difficult for the trainer to follow the game.

The trainer begins the session by explaining the aim of the game, and its rules :

2.4.1 Aim of the game

Make the trainee realize that they already know security best practices. The training is here to give them the keys to apply them to computer security.

2.4.2 Game rules

It is essential to highlight the physical aspect of the game. In a few cases the trainees, aware that they attend a computer security training, seek straight away to "hack" information systems. The double goal (prevent or detect for the defender, theft without being caught for the attackers) must be highlighted during the rules presentation, in order to make the impersonation or traces concept emerge. Finally, do not hesitate to insist on legal aspects : the attackers do not respect the rules, which is not the case of the defenders.

2.4.3 Playing the game

As soon as the game begins, the GM must write down the exchange on a medium visible by all players (see the example supplied in this document). As the Game Master, the trainer is responsible for the respect of the rules and has the right to impose limits to one or the other team.

He must make the players precise their action when necessary :

— if something is locked, we must now what type of lock is used (biometry - eye or finger, entry pass, pin code, physical key, etc.) and who exactly owne the means to open the lock.

— in case of generator fall back for example, the players must precise which security measure are supplied by the generator. The GM can limit the time during which the generator is working. Typically if the generator supplies all the security features, it cannot work more than a few hours.

— If CCTV are used, the players must specify if they are watched in real time, by who and by how many people.

The need to precise one action is decided by the GM, according to the teachings he wants to highlight during the debriefing. However, I strongly recommend to make players precise the above mentionned actions.

Everything that is not explicitly said by one team can be interpreted/hijacked by the other team : if the defenders do not precise that the windows are closed, the attackers can consider them opened. If the the attackers do not precise that they are masked, one must consider that their face is caught on CCTV.

The game master can guide one or the other team if he thinks the game is not going in the right direction, or to revive it. He can, for example, bring back the rules at the appropriate time, like saying to a shy attack team "I remind you that you do not need to follow the law, you can blow up this doors or kill this guard". The GM's goals is to bring up in the game (or look for) the ideas allowing him to illustrate the basic principles of computer security during the debriefing.

No analogy with computer security must be done during the game. The link is brought up during the debriefing only.

2.4.4 Game over

It is recommended to close the ongoing scenario if :

— The attackers keep going in the same unsuccessful course of action ;

— The ongoing scenario becomes too complex ;

— The ongoing scenario becomes too unrealistic ;

— The trainer wish to switch teams ;

— The players start to lose motivation (it is then possible to either stop the game or switch teams) ;

— The trainer already has the material he needs for the debriefing.

2.5 Exchange/scenario example

This exchange was observed during a training. At this time, the game was on for 10 minutes.

Table 1 – Scenario example

Attackers	Defenders	Game Master
Corrupt a subcontractor's employee and make him carry out the theft		

Table 1 – Scenario example

Attackers	Defenders	Game Master
	When used, the object stay visible to the user at all time. As soon as the user has finished, the object is put in a safe locked up by a physical key. Three person have a copy of the key : the user himself, his manager and the company's head of security. The actions of the keys owner are tracked.	Who have the key of the safe ?
Find the name of the company's head of security, watch his schedule. Violent theft of the key witch is then given to the subcontractor.		
	The safe is not easily found	Uneffective measure : the maintenance staff can find it easily
	CCTV on multiple surveillance screens. One guard is behind the screens 24/7, the video streams are recorded. Another guard is in the lobby.	Warning : to many cameras implies it is difficult to watch them in real time
A cleaning lady distracts the CCTV guard while another one perpetrates the theft		

Table 1 – Scenario example

Attackers	Defenders	Game Master
	The guards were trained by the special forces, there is a background check on all subcontractors.	There is always a way to find a weakness to exploit to blackmail a personn. Futhermore, the guards could need to go to the bathroom, or can be sick. But the attackers loose : the cleaning lady's face is caught on CCTV.
The cleaning lady hides in the bathroom to dress up, the person distraying the CCTV guards uses a device that can destroy the video data on hard drive (magnet)		
	There is a CCTV camera on the corridor leading to the bathroom, the server room is protected against tampering (in the center of the building, in a faraday cage)	The CCTV camera has been put in front of the bathroom instead of inside it because of a GM remark, french law does not allow CCTV in bathrooms.
Unplug the CCTV in front of the bathroom		
	Audio and visio warning in the guard lodge as soon as the camera is unplugged or malfunctionning	The Game Master forces the end of the scenario, to make attackers move on.

3 The game's debrief

3.1 Learning the common basic good practices

As explained in the introduction, neophyte people already know security good practices that can be apply to physical security as well as to computer security. I recommand to present these good practices just after the game, in order to link them to the scenarii come up during the game. You can find below a non-exhaustive list of good practices needed to be hightlighted by the trainer :

— Do not trust by default ;
— Check IDs ;
— Don't give your home key/alarm pin/password to anybody ;
— Case of the emergency services : would you give them your home key "in the event of" ?
— Call the police/security team when you suspect malicious activity ;
— Aask ourself :
— Could someone be interested in attacking my building ? To which extent ?
— Could this information/badge/key be of value to someone ?
— What do I do in case of malfunction ?

3.2 Scenarii decoding keys

It's easy to make a connection between the physical element used by the trainee during the game and computer security elements. The debrief idea is to have the trainer making this connection, according to the key points he wants to highlight. The table 1 presents a non-exaustive list of decoding keys of wildly appearing elements in the game :

3.3 Similarities and divergences

The similarities between physical and computer security have already been presented multiple times in this document. We now get over them one more time to highlight key examples that illustrate these principles and come up in the role playing game.

3.3.1 The "trusting someone" problem

Very quick in the game, gamers are exposed to the access control principle. You'll see appear quickly the concept of badges, ID verification in the lobby or disguised or lying attackers. It's important to use this key points to make the trainee think about the concepts of trust, identity and authentication. The use of a false ID card is, for instance, very interresting : what can we use to trust someone when he states his identity ? This notion is at the center of every security system. The trainer can also take advantage of this discussion to talk about the different authentication methods :

Physical security	Computer security
Key / Badge	Password, smartcard
Safe, reinforced door	technical measure of protection
CCTV	Supervision/logs/anti-virus
CCTV redcords destruction	Logs destruction or tampering
Blackout / arson	Denial of Services
Guards, surveillance employee	Security Operationnals
Disguise/false ID card	Impersonnation of IP adresses or identity
Observation, get some top manager's name, get info ...	Social Engineering
Emergency procedure, generator etc.	Failure resistance, in-depth security, after sale
ID card	Certificate
Specific technology use (jammer, explosive, drone ..)	Use of exploits, command and control center etc.

FIGURE 1 – Decoding keys

— Biometry

— PIN code or passwords

— Key (whitch can be lost, stolen, copied etc.)

— ID cars, whitch sends back to the concept of trusting a third party (the government in physical security, the Certification Autority in Infosec)

Finally, in most game sessions, the attackers were fast using lies or identity impersonation. For example, in one of the session, the attackers were geting the name of a top managers, and were insisting on the urgent nature of a delivery at the reception. This type of scenario is very usefull to illustrate the concepts of phishing, scam and social engineering. It's also the moment to make the trainee think about a great principles in security "the human is the weakest part".

3.3.2 In depth security

The in depth secuoity idea, which consist in piling up security measures and handling the possible failure of one of them, appears easily in the game. For example the trainee consistensly proposed an access control in the lobby and a different one for the room where the object is stored. Often, they even added an access control near the object itself.

The trainer must highlight this behaviour, and make the trainee notice that the same applies to computer security. It's the moment to talk with them about multiple security measures, and to make them aware of their convenience. We often hear, as security engineers, sentences like "But it's in the LAN, ther is no risk" or "but the user has already enter another password, why do we need a new one ?" etc.

The multiplication of technologies (physical key, badge, biometry etx-c.) is also a way to make trainee think about the security best practice (one password per usage etc.). Finally, the attackers' different attemps allow us to illustrate the fact that the security level of a system depends on the security level of its weakest element.

3.3.3 The attackers' motivation

The differents scenarii allow the trainer to illustrate the important notion of the attackers' (or defenders') motivations. When the attack itself cost millions and months of preparation, we can ask ourselves : is the object worth it ? The same question may be asked to the defenders.

It is also an opportunity to discuss the security level versus the attackers level, and to think about the question at the earth of all security systems : what do we protect, and against who ?

3.4 Demistify the attackers (who is not a computer genius)

One of the idea the least understood by a neophyte audience is the diversity of the attackers profiles. The collective imagination depicts them as a genius hackers, in an undergournd cave, yet, as in physical security, there is a variety of attackers : if your door is not locked, every delinquent can enter your building. When the scenario becomes complex, we face very well organized and motivated attackers.

The blackmarket idea is also not well understood

- In physical security, the objects are resold or ordered prior the theft. It is the same in computer security, and the trainee must be aware of this.
- As a physical attackers will buy specific tools (explosives, jammers, false ID, ...), and computer attacker will do the same. Which means an economy has developped ourond the discovery of tools (vulnerabilities, exploit etc.) and their trade. Make the trainee aware of these different profiles : anybody can push a button on a jammer, but you need specific skills to design one.

3.4.1 The constraint versus security compromise

To illustrate this idea, the trainer must focus on the security measures deployed by the defenders, and the contraints they imply for the company's employees or the company itself. The link is then easily made with computer security contraints.

One interesting element to work on is the presence of emergency services (police, army, firefighters, etc.) whether they are legitimate or not. Ask the trainees : do they give the emergency teams full access to the building, just in case ? Do they check if they are legitimate ? In one of the game sessions, the attackers posed as a medical team who evacuate victims via helicoper (they, in fact, were evacuating the stolen object). This is the time to discuss the privilege accesses of teams like after sales, IT support etc. and the need to store cleartext passwords "in the case of the client needs it".

3.4.2 The security teams' goals (predict the attacker behavior, prevent or detect it)

In the game, the work for the defenders team is easier than in the real world : the attackers announce their intention and their goal is known. The trainer can pinpoint, during the debrief, the difficulties of the security teams' work, they have to imagine the attackers' behavior and evaluate their possible motivations. The trainer can also make the trainees think about supervision or tracing tools.

3.4.3 Divergences

Of course, the whole physical security isn't transposable into infosec (and vice versa). But the differences, as essential as they may be, are not that many :

- The time factor differs greatly :
  - In example : testing a password is a lot faster than testing a physical key on a door.
- The geographic factor nearly no longer exists :
  - The attacker does not need to be physically present to conduct the attack. The physical distance does not matter anymore.
  - There is, of course, exceptions to this rule :
    - The laws depend on the physical location of the stolen or tampered data ;
    - When attacking via compromising signals, radio flux or hardware element, the physical distance can come up again as a critical issue.
- These two scale changes result in mass attacks costing less and put them within anybody's reach ;
- The exact and easily collected evidences only relate to the machines, less easily to the human beings ;
  - It can be very difficult to find the actual perpetrator ;
  - The attackers can hide themself behind innocent third parties ;
- The theft is virtually impossible to detect (electronic copy) ;
  - Some evidences of the theft can be found is the system is correctly configured ;
- Too often, there is no basic security deployed in IT, where, in the physical world, people would have a working lock on the door, at a minimum.

4 Game session example

This game session has been carried out with five people (three defenders and two attackers), it lasted nearly fifty minutes.

TABLE 2 – Example of a full game session with five player for a duration of nearly fifty minutes (without debrief)

Attackers	Defenders	Comments	IT security parallel
Open the door, collect the object, get out	The door is secured by a badger and is physically locked after 8 PM. If an attempted theft is detected an alarm is trigerred, linked directly to the police station		Unprotected data theft Password based protection, access control, supervision
A woman is sent to seduce an employee, she tells him she has forgotten her badge, the man employee let her pass (theft then exit)			Social engineering

Table 2 – Example of a full game session with five player for a duration of nearly fifty minutes (without debrief)

Attackers	Defenders	Comments	IT security parallel
	The object is locked in a safe, a PIN code is needed to open the safe. The site supervisor is the only one who knows the PIN (people must call him each time they need to use the object). Carrying a visible badge is mandatory within the building, security agent ensure the enforcement of the rule. Futhermore, employees are aware of the risks lying in letting an unknow personn enter the building.	We can notice that the measure is very restrictive for the company (one and only one personn has access to the object)	Password based protection. Non sharing of passwords. Supervision. Awareness training.
Dressing up as a janitor, entering with a stolen badge and a cart containing a blowtorch. Open the safe with the blowtorch, get the object, put it in the cart and exit			Impersonation, brute force attack

TABLE 2 – Example of a full game session with five player for a duration of nearly fifty minutes (without debrief)

Attackers	Defenders	Comments	IT security parallel
	There is a smoke sensor in the room. The entry of the room is protected by a retinal scan.		Attack detection, biometry.
The attackers land a helicopter on the roof of the building and use the air conditionning pipes to gain access to the room. Go down "like in 'Mission : Impossible'" and steal the safe. Exit from the building and then open the safe.			OffLine attack, theft followed by protection workaround.
	The safe is sealed in the wall, futhermore, it is electrified until the retinal scan is OK		Offline attacks banning. Ban all action before authentication check.
Blackout			Denial of Service/failure of the security system
	Generator supplies all the security measure of the room		emergency backup system

TABLE 2 – Example of a full game session with five player for a duration of nearly fifty minutes (without debrief)

Attackers	Defenders	Comments	IT security parallel
The attackers take a member of an employee's family in hostage and blackmail him to commit the theft himself.			Social engineering
	CCTV camera are placed in front of and in the room, the camera feeds are watched in real time 24/7 by employees in the security command center which is not in the same building.		Supervision and logs on dedicated servers
Blowing up the security command center			Detruction, tampering of the logs
	In case of explosion or communication loss with the security command center, teams of guards are sent to the command center and to the building. An alarm is trigered in case of communication loss.		Logs protection, in depths security, monitoring of security measures etc.

TABLE 2 – Example of a full game session with five player for a duration of nearly fifty minutes (without debrief)

Attackers	Defenders	Comments	IT security parallel
Hacking of the CCTV feed to cut the video stream			Attack to destroyed the logs, DoS on the supervision system
	A motion sensor is put on the object, if triggered, the object blows up.	Refused : the object must be usable during the day, and not compliant with french law	In InfoSec, we call this technique “emergency erase”. If an attacked is detected, all sensitive data are erased. Very constraining.
Intrusion by using the CCTV camera blind spots, theft of a badge for entering			
	Enough CCTV camera to have no blind spot at all, there is one watching guards per screen, one screen per camera.	Costfull measure	Increase of the supervision and security operationnals
Cover the camera with a picture of the hallway			
	A guard is in the lobby and control all the entry, patrols with dogs		
Kill the guards and feed the dogs to distract them			
	There is always the retinal scan, a fingerprint scan is added.		Biometry

Table 2 – Example of a full game session with five player for a duration of nearly fifty minutes (without debrief)

Attackers	Defenders	Comments	IT security parallel
An infiltrated employee commit the theft			
	Systematic personn search at each going in/out the building	Very contraining measure (several seconds by person, in rush hour, etc.)	Real time control of everything stored on employees computers (forbidden by french law)
Drone use to get the object out of the building			Data exfiltration
	Personn search at each going in/out the room.	Very constraining measure (several seconds by personn, in rush hour ...)	
Murder of the guard securing the room			
	Antitheft device on the object allows to know when the object leaves the building, in case of detection, the site is lock down.		Data watermarking (less effective)
Trigger an arson to obtain the automatic opening of the doors			Emergency procedure attack
	Geolocalization of the object		
Use of silver foil to avoid detection			
	Army intervene to take down the drone		

TABLE 2 – Example of a full game session with five player for a duration of nearly fifty minutes (without debrief)

Attackers	Defenders	Comments	IT security parallel
Hundreds of drone making diversion			
	Radio jammer to prevent piloting the drones		
Drones autopilot pre programmed			
	jammer for GPS signals to prenvent the autopilot working		
Passing by the underground parking while the drone gets out with a copy of the object, exit on three motocycles, only one has the object			Diversion, overload of the supervision system
	Nails were spread on the exit road as soon as the alarm was triggered. There is a reinforced door at the exit of the parking lot		All expected ideas have been expressed, futhermore, the scenario is becoming to complex. End of the game.