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 needed information to carry out the training himself.

1 Copyright

Contact :

`tiphaine.romand@orange.com`

`tiphaineRL@gmail.com`

The idea behing the training is born from the need to train a operationnal and neophyte audience to the conputer security stakes. Instead of strating from a standard training mecanism, based on technical context learning (what is a password, how does a computer works etc.), which, according to my experience, has a tendency to bore or scared a neophyte audience, I'd rather concentrate on he generic principles of InfoSec :

- The problematic lying in the trusting of a entity/personn ;
- The in-depth defense concept ;
- The attacker motivations ;
- The attacket demystification (who is not necessarily a "genius hacker") ;
- The concept of compromize between operationnal constraint and security ;
- The goals of the security team (forcast the attacker behaviour, preventing it or detecting it).

The concept underlying this training is the following : this basics principles are the same for physical or computer security :

— Everyday, we are explosed to to the problem of trusting somebody ;

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

— Attackers motivation are money, ideology etc. ;

— The most common attackers are not crime genius.

Physical security is also setting constraints (lock the door, carry a badge, security check at the airport etc.). The goals are common : forcast the attacker behaviour, preventing it or detecting it.

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

The core idea of this training is therefore to make people aware that its already prepared, that it has the good reflex and thinking and to train it to apply them to computer security, while play done InfoSec.

2 The role playing game

The training is based on a role playing game bases on attacking and defending a building.

2.1 Rules

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

2.2 General description :

— An office building, in a dense area, with an underground parking lot and a 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, and we do it again.

2.2.1 Attackers team's rules and goals

— Goals : steal the object without being caught.

— Rules : unlimited budget, limited human attacker in the game (no more than ten person), observe physics rules.

2.2.2 Defenders team's rules and goals

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

— Rules : unlimited budget, unlimited staff, observe physics rules and the law, employee 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 arrive to a blocking point (everybody's dead, the object is destroyed, the police has arrived ...) ;

— It is then possible to move on a new try of the attackers team. In this case, 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 no winner nor loser !

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

— The play is followed by a debriefing by the trainer, allowing to highlight the wished concepts (see the "Debriefing" section).

2.3 Behind the rules

2.3.1 The playing environment

The playing environment (building, dense area etc.) has been chose 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 game details using the players professional environment : company's building, key product of the company etc. This allow a faster immersion and involvement from the players.

— The dense area choice, as the helicopter landing strip and the underground parking lot enforce the fun part (the attackers can think of helicopter landing on the roof, jump from a building to another etc.) and lead the players. Furthermore, its allows to force the diversification of the scenario.

— The choice to not precise more the environment has been made to let the players imagination run wild and to simplify the games rules.

— 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.

— The 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 fame. It is, however, interesting to make the player thinks on this subject during the debriefing.

— The 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 simplify the game, futhermore, it is always possible to discuss financial aspects during the debriefing ;

— The small number of human being authorized for the attackers team during the game allows us to stay clear of non realistic scenario like “siege done by a tree hundred people army” ;

— The physics laws respects allow us 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.) ; security goal (going in and out without leaving trace) ;

— The unlimited budget simplify 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 country law, it is also a way to make the trainee work on the compromises price versus security need during the debriefing ;

— The physics laws respects allow us again to stay clear of non realistic scenario or unsporting behavior ;

— The respect of the country law sends the trainees back to the need for IT security engineers to do the same.

2.3.4 Losing and Winning

There is no loser or winner, even if the teams often want to appoint one. Rules allowing to name a winner would made the game more complex with no reason. The rules goal is to stimulate 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 construct little teams of player. 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 begin the session by explaining the aim of the game, and its rules :

2.4.1 Aim of the game

Make the trainee aware of the fact that they already possess the right reflexes in security, the training is here to give them the key for applying them to computer security.

2.4.2 Game rules

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

2.4.3 Playing the game

As soon as the game has begun, 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 of the rules following and has the right to limit one or the other team.

He must make the layers 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 own 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 supply all the security features, it cannot work more than a few hours.

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

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

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 timid attackers 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 watch for) the idea 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 made only during the debriefing.

2.4.4 Game over

It is recommended to close the on going scenario if :

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

— The on going scenario become too complex ;

— The on going scenario become too unrealistic ;

— The trainer wish to switch the teams ;

— the player are losing their motivation ; (it is then possible to either stop the game or switch teams) ;

— The trainer already has the material needed for the debriefing.

2.5 Exchange/scenario example

This exchange has been observed during a training. At this time, the game has begum since 10 minutes.

Table 1 – Scenario example

Attackers	Defenders	Game Master
Corrupt a subcontractor 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 closed by physical key. Three person have each one copy of the key : the user himself, his manager and the company head of security. At each time, the actions of the keys owner are tracked.	Who have the safe key ?
Find the name of the company head of security, watch his schedule. Violent theft of the key witch is then given to the subcontractor.		
	The safe is not easly found	Uneffective measure : mainteners can find it easily
	CCTV on multiple surveillance screen. One guard is behind the screen 24/7, the video streams are recorded. Another guard is in the lobby.	Warning : to much camera implies a difficulty in watching 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 have been trained by the special forces, there is a backgroud 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 who can destroy the video data on hard drive (magnet)		
	There is a CCTV camera on the cooridor 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 Common reflexes learning

As explained in the introduction, neophyte people already have goo security reflexes, which can be apply to physical security as well as to computer security. I recommand to present this reflexes just after the game, making the connection with the scenarios come up during the game. You can find here a non-exhaustive list of good reflexes needed to be hightlighted by the trainer :

— Trust is not a default state ;
— We must check ID ;
— We don't give our home key/alarm pin/password to anybody ;
— Case of the emergency services : would you give them your home key "in the event of" ?
— You call the police/security team when you suspect malicious activty ;
— We ask ourself :
— Could someone be interested in attacking my building ? To which extent ?
— Could this information/badge/key be of value to someone ?
— We do we do in case of malfunction ?

3.2 Scenrios 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 this connection made by the trainer, according to the key point he wants to highlight. The table 1 presents a non-exaustive list of decoding keys of widly apparing elements in the game :

3.3 Common points and divergences

The common points between physical and computer security have already been presented multiple times in this document. We now get over them one more time to indicate key example illustrating this principles and coming up in the role playing game.

3.3.1 The "trusting somone" 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 ideas of trust, identity and authentication. The use of a false ID card is for example very interresting : what can we use to trust someone when he states his identity ? This notion it at the center of every security system. The trainer can also take advantage of this discussion to talk about the differents 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 paswords

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

— ID cars, whitch sends us to the concept of trusting a third party (state in physical sécurity, Certification Autority in Infosec)

Finally, in most game session, 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 lobby. This type of scenrio is very usefull to illustrate the concepts of phishing, scam and social engineering. It's also the time to make the trainee thinks about a great principles in security "the weakest part is the human part".

3.3.2 In depth security

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

The trainer must hightlight this behaviour, and make the trainee notice that the same applies in computer security. It's the moment to talk with them about multiple security measure, and to make them aware of their convenience. We often hear, as security engineers, typical 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 increase of technology type (physical key, badge, biometry etx-c.) is also a way to make trainee think about the security best practice (one passwoard per usage etc.). Finally, the attackers different try allow us to illustrate the fact that the security level of a system depends on the security level of t-its weakest element.

3.3.3 The attackers motivation

The differents scenarios allow the trainer to illustrate the basic notion of the attackers (or defenders) motivation . When the attacks itself cost millions and months of preparation, we can ask ourself the question : is the object worth it ? The same question may be asked to the defenders.

It is also the occasion to discuss the security level versus the attackers level, and to think about the question at the earth of all security system : what do we protect, and againt who ?

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

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

The blackmarket idea is also not understood

— In physical securit, the objects are resold or ordered prior the theft. The same exists in computer security, and the trainee must be awar eof that fact.

— As a physical attackers will buy specific tools (explosives, jammers, false ID, ...), the computer attacker d the same. Which means there is a economy linked to the discovery of the tools (vulnerabilities, exploit etc.) and their selling. It's the moment to make the trainee aware of these different profiles : anybody can push a button on a jammer, but you need specific skill to design one.

3.4.1 The constraint versus security compromize

To illustrate this idea, the trainer must concentrate on the security measures deployed by the defenders, and the contraints they imply on the company's employee or the company itself. The link is then easy made with conputer security contraints.

One interresting part to work on is the emergency services presence (police, army, firefighters etc.) whether they are legitimate or not. Ask the trainee : do they autorize full access of the building, at all time ? Do they check if the emergency services ar legitimate ? In one if the game session, the attackers pose as an medical team evacuating victims via helicoper (they, in fact, were evacuating the stolen object). This is the time to discuss the privilege accesses of team like after sales, IT support etc. and the need to store cleartext passwords "in the case of the client needing it".

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

In the game, the work for the defenders team in more easy than in the real world : the attackers announce their intention and their goal is known. The trainer can pinpoint, during the debrief, the difficulty of the security teams'work, they must immagine the attackers behaviour and evaluate their possible motivation. The trainer can also make the trainee think about supervision or traces tools.

3.4.3 Divergences

All physical security is not transposable in infosec (and vice versa). But the difference, as major as they are, are not that many :

- The time factor differs greatly :
  - In example : testing a passworg is a lot faster than testing a physical key on a actual door.
- The geographic factor nearly no longer exists :
  - The attacker does not need to be physically present to lead the attack. The physical distance does not matter anymore.
  - There is, of course, exception to this rule :
    - The applying law are dependent of the physical location of the stolen or tampered data ;
    - In attacking compromising signals, radio flux or hardware element, the physical distance can come up again as a determining element.
- These two scale changes allow mass attack to cost less and to be accessible to anybody ;
- The exact traces whoch are easily recoverable concern the machines but the human with difficulty.
  - It can be very difficult to find the actual perpetrator ;
  - The attacker can hide itself behinf innocent third party ;
- The theft is virtually impossible to detect (electronic copy)
  - Some traces of the theft can be found is the system is correctly configured
- Too often, ther is no basic security deployed in IT, where, in the physical world, people have at minimum a working lock.

4 Game session example

This game session has been realized with five people (three defenders and to 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 the 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		Non protected 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 the 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 knowing the PIN (he needs to be called everytime the object must be used). Carrying a visible badge is mandatory within the building, security agent monitor the instruction compliance. Futhermore, the employee are aware of the danger residing in letting enter an unknow personn.	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 the debrief)

Attackers	Defenders	Comments	IT security parallel
	There is a smoke sensor in the room. The enter of the room is protected by a retinal scan.		Attack detection, biometry.
The attackers land on helicopter on the building roof, then use the air conditionning pipes to gain access to the room. Going down "like in "Mission : Impossible" " and theft of the safe. Building exit followed by the safe openning.			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 supplying all the security measure of the room		emergency backup system
The attackers take an employee family in hostage and blackmail him to commit the theft himself.			Social engineering

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

Attackers	Defenders	Comments	IT security parallel
	CCTV camera are disposed in front of and in the room, the camera feeds are watched in real time 24/7 by employee in the security command center whitch 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, guards teams 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 measure etc.
Hacking of the CCTV feed to cut the video stream			Attack to destroyed the logs, DoS on the supervision system

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

Attackers	Defenders	Comments	IT security parallel
	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 eraseé. 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 operationnal
Cover the camera with a picture of the hallway			
	A guard is in the lobby and control all the entry, patrol with dogs are done		
Kill the guards and feed the dog to distract them			
	There is always the retinal scan, a fingerprint scan is added.		Biometry
An infiltrated employee commit the theft			

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

Attackers	Defenders	Comments	IT security parallel
	Systematic personn search at each going in/out the buildinf	Very contraining measure (several seconds by personn, in rush hour ...)	Real tim 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 ...)	
Killing of the room guard			
	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
	Geoloation of the object		
Use of silver foil to avoid detection			
	Army intervene to take down the drone		
Hundreds of drone making diversion			

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

Attackers	Defenders	Comments	IT security parallel
Drones autopilot pre programmed	Radio jammer to prevent the drone piloting jammer for GPS signals to prenvent the autopilot working		
Passing by the undergroung parking while the drone get out with a clone of the object, exit on three motocycle, only one has the object			Diversion, overload of the supervision system
	Nails have been put down on the exit road as soon as the alarm was triggered. There is a reinforced door at the exit of the parkin		All the expected idea have been expressed, futhermore, the scenario is becoming to complex. End of the game.