Dungeons, Dragons & Security

Tiphaine Romand-Latapie
Who, why & how

• About me:
  • Currently: Airbus Group Innovations (joined May 2016)
  • Before: Orange Labs as a Project Security Team Leader (job: convince people to do security)

• Why:
  • RPG design for and by myself to train my interlocutors

• How:
  • Design
  • Test on family, friends & coworkers (redesign)
  • Used on ~70 people at Orange: Project manager, Top manager, Retail, Customer Support, Call Center
Neophyte view of InfoSec

• “We do not need to protect ourselves from hardware level attacks. If the user opens his product, he loses the warranty anyway.”

• “We don’t risk a thing: it’s in the LAN”

• “I don’t know why we even bother, we’ve never been hacked!”
Let’s go train them!

• “That’s not an API; an API is the thing we publish on our website.”

• “I do not think that the kernel is essential.”

• “In case of massive network failure, we want to send a message to all customer devices indicating that there is a massive network failure.”
Let’s go train them...

• …without talking about technical aspects…

• “We do not need to protect ourselves from hardware level attacks. If the user opens his product, he loses the warranty anyway.”

• “I don’t know why we even bother, we’ve never been hacked!”

ARE NOT TECHNICAL MISUNDERSTANDING ISSUES
Learning

• When can you decide whether or not to trust an entity/a person? And for what?
• What is in-depth defense?
• Bad attacker, bad!
  • his motivations
  • stereotype versus reality (he is not necessarily a “genius hacker” – sorry)
  • money, money, money
• Who’s the security team (beside obnoxious nerdy people who don’t know real life and prevent people from working)?
Neophytes have good instincts…

… when it comes to physical security:

- They close their doors in the morning
- They have insurance (auto, home, fire, liability, disability, etc.)
- They even hide valuables before leaving home for an extended period of time
- They don’t let just any stranger enter their home
- They are OK with security when they feel it protects / benefits them (home alarm, locks, cameras, etc….)
Core Idea

• Using neophyte knowledge in physical security to teach them about computer / info security

• Requirements:
  • Not another boring mandatory security training session…
  • Make it FUN!
  • No heavy technical aspects
  • Learn the basics
  • We want trainees to learn to think « infosec » by themselves

✓ RPG in physical security
Game & Settings

You need:
- One meeting room and one paperboard / drawing board
- 4 to 8 players
- Energy
- 90 to 120 minutes (more if you’re up to it)
- No Dice / No Dragon

You (The Security something):
- Are the Game Master
- Conduct the game during 30 to 45 minutes
- Then explain the parallel between what happened in the game and the InfoSec world
The Game

- At the beginning of the game, the building is not secure at all
- Two teams:
  - The attackers must steal the object
  - The attackers propose an attack, the defenders a mitigation, in an iterative way
The Rules

Attack team:

Goals: steal the object without being caught (either during or after)

Rules: unlimited budget, limited number of human attackers in the game (no more than 10 people). Laws of physics apply (gravity, no Deadpool, etc.).

Defense team:

Goals: prevent the theft or collect data allowing you to catch the attackers.

Rules: unlimited budget, unlimited staff, laws of physics apply, the law must be respected, employees must be able to work in the building during office hours (and use the object)...
Real session minutes (synthetized)

Get in, steal, get out

Guards at the front door, safe in the object’s room, badge reader at the room entrance. Access to safe key & room: 3 managers of the team needing access to the object.

Kidnap of one of the managers, steal badge and safe key. Enter building through parking lot.
The safe key never leaves the building, CCTV everywhere (except bathrooms!!), CCTV surveillance 24/7 by external company

Hack the CCTV (video loop), enter with the manager’s badge then steal the key of the safe

Badge associated with facial recognition

Hack facial recognition DB before the theft
Real session minutes (synthetized)

- Kill the manager and steal his face (actual face!!)
- Video loop detected by putting analog clocks in front of all camera
- Iris scan to access the floor
- Fire (all doors open), land in fake firemen helicopter
- The object is put back in the safe in case of evacuation
Real session minutes (synthesized)

- Open the safe with blowtorch
- Blackout (no more electricity)
- CCTV guard calls the police
- Backup generator
Real session example

- After all this: drone evacuation of the object, kidnapping of guards’ families, GPS tracker, faraday cages, poison, etc.
- This is actually a “tame” scenario
- Think about: James Bond, Mission: Impossible, Oceans 11 etc.

- That was fun, but… InfoSec anybody?
Debriefing (synthetized)

Get in, steal, get out

- Security operational & technical measures, access control, “least privilege” principle, defense in depth, bad security measure deployment (nothing in the safe)

- Guards at the front door, safe in the object’s room, badge reader at the room entrance
- Access to safe key & room: 3 managers of the team needing access to the object

Kidnap one of the managers, steal badge and safe key. Enter building through parking lot

- Social Engineering, password theft, path of least resistance
Debriefing (synthetized)

- The safe key never leaves the building, CCTV everywhere (except bathrooms!!), CCTV surveillance 24/7 by external company
- Hack the CCTV (video loop), enter with the manager’s badge then steal the key of the safe
- Log tampering, credential theft
- Biometry, multi-factor authentication
- Hack facial recognition DB before the theft
- Hardware security – Supervision, SOC
- ACS attack
- Badge associated with facial recognition
Debriefing (synthetized)

- Video loop detected by putting analog clocks in front of all cameras
- Hack account/computer. Rebound attacks
- Iris scan to access the floor
- Use of customer support/debug access – fail safe/fail secure
- The object is put back in the safe in case of evacuation
- Hardware security
- Biometry
- Watchdogs/Keep alive (!!!!!)
- Kill the manager and steal his face (actual face!!)
- Fire (all doors open), land in fake fire department helicopter
- Debriefing (synthetized)
Debriefing (synthetized)

- Open the safe with blowtorch
- Hardware attacks/ use of exploit
- CCTV guard calls the police
- Blackout (no more electricity)
- DoS on security infra./supervision
- Back up infra.
- Back up generator
- SOC/CERT
Other discussions examples

- Cost of security (attack) VS. the object value
- Constraints on employees (and tradeoffs)
- Social engineering (they all do it!)
- Black Market:
  - Of data
  - Of exploit
  - Of video feeds
  - etc.
Physical Security != InfoSec

- Time & Space:
  - Instantaneous testing (!= testing a key for a lock)
  - Geography (nearly) doesn’t matter
- Copy & Paste:
  - Theft is actually copying
  - Without a trace
Pro Tips

• 6 to 8 players max
  • Too difficult to follow beyond this number

• Ask who wants to attack
  • Defense is “forced” to respond

• Switch teams
  • In case of “timid” attackers

• You are the law
  • Kill all the trolls

• Forget the rules
  • They’re just here to prevent “foul game”

• Have fun
Short term results

- Attackers are bad: “We put the dogs to sleep, then we kill the guards”
- People from Security Teams are fun: “Can we use missiles?”
- And their work is hard: “That’s not fair! It’s too difficult to win if we have to respect the law”
- And they actually help users: “Can you tell me again how to choose a password?”
- Trainers have fun too: “Does a dead eyeball pass an iris scan?”
- Does not work on: YOU
Long term results

• Actually working: “You’ve changed the life of my team, we don’t go to the bathroom with our smartphone anymore”
  • (They’re too afraid of being recorded)

• A lot of contact afterwards
  • To ask for the same training for coworkers
  • To ask for technical trainings
  • To ask for help
  • To report possible incident

• Trainers wants to train more people (!!!)
Thank You

• And thanks to all my guinea pigs and trainees at Orange
• You want to know more? White paper provided “NeoSens: …”
• This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.
• Please, try it and tell me about it:
  • @Flutsunami
  • aska.icoe@gmail.com