

Lifelong learning as a critical success factor for state of the art investigations: the Carabinieri INeS training

Cap. CC RTL Gianluigi Me
Comando Generale (HQ) dell'Arma dei Carabinieri
gme@carabinieri.it

Time to market hardly afflicts ICT causing several problems for security professionals and, consequently, for computer crime investigators. The most relevant effects of this phenomenon are shown, as threat severity, in the matrix attack technique/technology:

Technology/Attack technique	NEW	OLD
NEW		
OLD		

Example are:

- NEW/NEW: New attacks relying on new technologies (e.g. Bluesnarfing on Bluetooth since late 2003) ;
- NEW/OLD: A typical example of New Technology/Old Attack is provided by Voice-over-IP spam, namely “Spit” spam over Internet telephony. Even if VoIP is a technology almost ten years old, in 2004 with more than 24 millions installations, has overcome PSTN installations. This wide market penetration allows hackers to perform attacks with high impact on service level, user confidence with technology and companies image.
- OLD/NEW: Integer overflow, day-zero attacks
- OLD/OLD: Software bugs, giving rise to new vulnerabilities and relative attacks (e.g. buffer overflows);

Computer Crime investigators have to face all these attacks, including the newest one. Furthermore, as stated by existing literature, quality of computer crime professionals hardly affects the whole investigation activity (e.g. computer evidence collection), due to the fact that a computer can be further used as a tool for conducting or planning a “non-digital” crime. In fact,

1. Most criminal payoff functions have a penalty addend like:

$$\alpha_i \cdot r_i$$

Where

- α_i , is the probability to be detected by Law Enforcement (LE);
 - r_i , is the crime related penalty.
2. The virtual community afflicts α_i : in fact, in communication networks, e.g., cryptography and steganography techniques raise the LE attack cost, raising the probability to escape detection (lowering α_i).
 3. The coefficient α_i has 2 components:
 - Pr (Event A): probability to be detected by LE
 - Pr (Event B): probability of strong evidence recovery by LE
 4. The coefficient α_i will assume the form

$$P(A,B) = \alpha_i = P(A) \cdot P(B|A)$$

But $P(B|A)$

- Is strongly afflicted by the competence of the investigators.
- When the crime is strictly related to strong evidences (e.g. paedophilia) with probability ≈ 1

$$P(A,B) = \alpha_i = P(A)$$

This term (upper than the general case) lower the criminal payoff.

For this reason, the foremost action to face computer (or, better, digital) related crimes is education, to improve the investigation quality and to expand the investigation spectrum. In particular, computer related investigations capability can be considered as an additional weapon in the well-established investigative techniques: by this way, the investigator can choose the most effective/efficient one, depending on the single crime investigation context.

Since the previous considerations about the quick obsolescence of ICT knowledge, the Arma dei Carabinieri Law Enforcement adopted the lifelong learning paradigm to train computer crime militaries disseminated in the whole Italian territory. After a 12 days intensive course (named Investigazioni Elettroniche Speciali, InES), they are remotely trained with up-to-date best practices, knowledge repository access and state-of-the-art documents, with on line technical support.

While this is the primary objective to reach, together with high performance in computer related crimes (e.g. computer evidence collection), an immediate return on investment can be expected, with a payback period estimated in less than 1 year.

In fact,

- Cost per student
 - Teaching : 550 €
 - Travel allowance and accomodation: 750 €
- Total cost (roughly) 200 K€

Consider:

- Estimating average consulting activity cost (outsourced): 5 K€
- Estimating 0.5 consulting activities (per year, per Command)

$$\text{ROI (first year)} = \frac{\text{Savings : } 112 \cdot 0.5 \cdot 5 \text{K€}}{\text{Sustained costs : } (200 \text{ k€})} = 1,4$$

These results, to be verified with the First Annual Check, confirm that this action is remunerative in less than 1 year, just by economic side, while we're expecting by the aforementioned FAC the hit ratio of computer related crime investigation.

Many other related spin-offs, typically intangible assets (e.g. popularity), represent further advantages of the action.

REFERENCES

Eoghan Casey, Digital Evidence and computer crime, Academic Press 2001

Harlan Carvey, Windows Forensics and Incident Recovery, Addison Wesley, 2005

Merlin Dresher, The Mathematics of Games of Strategy, Dover, 1981