

Attacks in IT Systems: a Human Factors-Centred Approach.

Denis Besnard
*University of Newcastle upon Tyne,
Department of Computing Science
Newcastle upon Tyne
NE1 7RU
United Kingdom
denis.besnard@ncl.ac.uk*

1. Introduction

The current approaches to security in information technology (IT) systems rely on technical solutions. However, issues such as attackers' motivation and strategies cannot be omitted. Three research directions are proposed (see section 3) in order to link together computing science and human factors.

2. Approaches in the protection of IT systems

In the domain of IT systems security, financial losses are measured in hundreds of millions of dollars per year in the United States alone [1]. As a consequence, the protection of computer-based systems against malicious actions is gaining more and more attention. This becomes imperative as the information technology -in areas such as e-commerce, banking or mobile applications- takes a central role in our society.

The approaches taken to secure IT systems are currently technically focused. For instance, a recent project funded by the European Commission, MAFTIA¹, investigates an attack tolerance paradigm which aims at implementing technical solutions to an attack. Although the technical approach is necessary, it disregards the consideration of human factors involved in malicious actions. Addressing this topic would provide key-elements for understanding the attackers' motivation and the way attacks are performed and adapted to the target. This would be a contribution to systems dependability, especially availability and confidentiality (see [2]).

3. Research directions

Three main directions of research are proposed. They address the issues of motivation of attackers, the

subsequent strategies they implement and the possible counter-measures we may deploy.

3.1. Why do attackers attack systems?

Answering this question will permit understanding of the attackers' motivation and could help establish a classification of the targets. In the case of intrusions, the attack may have two origins [3]:

- It can be performed by an illegal user attempting an unauthorised access to a server. In this external intrusion, the implicit target may be peer recognition gained by hacking a site or performing a successful intrusion.
- Alternatively, the attack can be performed by a legal user who is abusing his rights on the system. In this internal intrusion, the targets may be motivated by to personal interests such as illegal profit or revenge (e.g. financial embezzlement, files corruption or destruction).

Sociology is a potentially fruitful theoretical frame for studying external attacks since phenomenon like peer-recognition are believed to be a major driving force. Nonetheless, sociological considerations will also be needed in order to assess internal attacks as these may be driven by causes originating in the workplace itself where social interactions and tensions are of major concern. Finally, trust relationship in organisations is an issue that cannot be avoided.

The targets may vary according to the motivation of attacks. As a consequence, the strategies implemented during an attack may vary accordingly. The different types of attacks is the issue addressed in the next section.

3.2. How do attackers attack systems?

This section of the paper will briefly review the strategies used by the attackers and some possible interests for research.

¹ <http://www.newcastle.research.ec.org/maftia/>

Some classifications already exist about the types of attacks. For instance, Arlat *et al.* [3] identified intrusions (see section 3.1) and malicious actions as two broad categories of attacks. Malicious actions (logic bombs, trojans, trapdoors; virus, worms, etc.) aim at impairing the functioning of the system (e.g. corruption, destruction) or setting an illegal entry point in a system.

Recently, with the increasing traffic of emails, new forms of attacks have arisen. Of worldwide consequences, the 'Love letter' VISUAL BASIC script has made malicious emails notorious. But less explicit actions such as false virus-alert messages or nuisance petitions allow attackers to saturate servers or reduce the communication bandwidth. These attacks can be directed to an unknown target server.

Last but not least, malicious actions can be performed during the development process of a software product. In that case, a developer can design trapdoors at a very early stage of the lifecycle of a piece of software.

With respect to the strategies implemented, especially in the case of external intrusions, the cognitive models of human activities (e.g. [4]) provide a useful theoretical frame in order to analyse such issues as:

- How is the goal set by the attacker?
- How is the entry point chosen?
- What is the route taken to the target?
- To which extent are the three features mentioned above redefined on-the-fly, during the attack?
- What are the criteria for giving up an attack?

It is assumed that external intruders very seldom have a specific target in mind. Following this assumption, it is strongly believed that the planning of actions performed during an attack is strongly ad hoc [5]. Moreover, there must exist some criteria for abandoning an attack. As a consequence, it is worth discovering how intrusion strategies start, evolve and eventually halt in order to implement counter measures centred on human cognition.

3.3. What kind of protections can we deploy?

The question of the possible protections reveals the interdisciplinary aspect of this paper. It will involve a strong collaboration between skills from the Computing Science and human factors.

Detecting a potential attack in real-time is an attractive vision. In the case of unauthorised intrusions, one possible security approach could be the recognition by the system of a pattern of commands identified as potentially dangerous. As a response, one can imagine the execution of real-time proactive counter-measures.

This would imply extensive field work in order to acquire knowledge of patterns of malicious commands and would need system resources to be allocated to screening only.

This proposal may be ambitious. However, pattern detection has already been adopted by the marketing department of an international airline in order to tailor customer services. Moreover, the design of human-centred protections is related to such high stakes that it is seen here as a mandatory recommendation for effective protections.

4. Conclusion

The computing science has already started research on the protection of IT systems. Integrating human factors in the study of malicious actions will permit the implementation of more efficient, human-centred protections. Such synergy would promote interdisciplinarity in a domain where our increasing dependence on IT systems makes both operational and financial consequences of attacks more and more critical.

5. Acknowledgements

This paper was written within the DIRC project (<http://www.dirc.org.uk>). The author wishes to thank collaborators for useful comments and the EPSRC for funding. Special thanks to the LAAS (Toulouse, France), in particular to David Powell, Corinne Mazet and Jean Arlat who suggested the main directions for this work.

6. References

- [1] Computer Security Institute. *Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar*. http://www.gocsi.com/prelea_000321.htm
- [2] Randell, B. 2000. Facing up to faults. *The Computer Journal*, vol 43, pp. 95-106, 2000.
- [3] Arlat, J., Blanquart, J.-P., Costes, A., Crouzet, Y., Deswarte, Y., Fabre, J.-C., Guillermain, H., Kaaniche, M., Kanoun, K., Laprie, J.-C., Mazet, C., Powell, D., Rabejac, C. and Thevenod, P. *Guide de la sûreté de fonctionnement*. Cepadues, Toulouse, 1996.
- [4] Rasmussen, J. *Information processing and human-machine interaction*. Elsevier Science, North Holland, 1986.
- [5] Hoc, J.-M. *La psychologie cognitive de la planification*. Grenoble, PUG, 1987.