Attacks in IT Systems: a Human Factors-Centred Approach

Denis Besnard

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]. Thus the protection of computer-based systems against malicious actions is gaining a lot of attention. This becomes imperative as the IT, 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, MAFTIA[1], investigates an attack tolerance paradigm that aims at implementing technical solutions in order to protect internet-based applications against potential attacks. This technical approach is necessary but it disregards the consideration of human factors in malicious actions. Addressing this topic would provide key-elements for understanding the attackers' motivation and strategies. 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 unauthorised user attempting an access to a server. In this external intrusion, the implicit target may be peer recognition gained by 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 choice of targets may be motivated by 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 a phenomenon like peer-recognition is believed to be a major driving force. Sociological considerations will also be needed in order to assess internal attacks as these may be driven by causes originating in the workplace where social interactions and tensions are of major concern.

The targets may vary, depending on the motivation of attackers. As a consequence, the strategies they implement during an attack may vary accordingly. As an overview, a brief presentation of the types of attacks is the issue addressed in the next section. Some possible interests for research are also introduced.

3.2. How do attackers attack systems?

Some classifications of different types of attacks already exist. 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 or setting an illegal entry point.

Recently, with the increasing traffic of emails, new forms of attacks have arisen. Of worldwide

[1] http://www.newcastle.research.ec.org/maftia/

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 and reduce the communication bandwidth. 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. Thus 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 interdisciplinary aspects. It requires a combination of skills from the computing science and human factors.

Detecting a potential unauthorized intrusion in real-time is an attractive vision. Even more attractive is the anticipation of the goals of the attacker. To these respects, the cognitive analysis of potentially dangerous patterns of commands can be fruitful: if we can reinterpret these patterns in terms of an intrusion strategy, then we will be able to predict which elements of a system are likely to be the targets of a given attack. As a response from the system, one can imagine the execution of real-time proactive counter-measures.

This interdisciplinary approach would imply sharing the knowledge of patterns developed by the computing science and infer cognitive processes from these patterns.

This proposal for human-centred protections may be seen as too ambitious, even if little consideration is given to internal intrusions. But the design of human-centred protections implies such high stakes that it is seen here as a mandatory recommendation for effective protections.

4. Conclusion

Computing science has already started research on the protection of IT systems against malicious actions. Integrating human factors in the existing technical approaches 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.