Trends in Information Security

Topic Description: Usable Security and the Role of Human Factors in Information Security

Prof. Chris Johnson,
School of Computing, University of Glasgow.
Johnson@dcs.gla.ac.uk
http://www.dcs.gla.ac.uk

Introduction

Human behaviour has a profound impact on the security of any system. Many companies have elaborate security management systems and policies that are worthless because they only exist of paper and have no impact on the everyday working behaviour of employees. In some cases, staff do not know the rules that they should follow. In other situations, individuals will deliberately violate security policies. Rules are ignored because they undermine other objectives - for instance, a doctor might be forced to violate patient confidentiality in order to save a life. Similarly, procedures can be ignored because they are simply too hard to follow – hence there is an area of reserch called 'usable security', looking at questions such as the best ways to provide passwords that are both secure and do not need to be written down! Violations also occur when staff do not understand the reasons behind a particular requirement. Management may also provide implicit support for these violations – for example, when management performance may be assessed by productivity that is increased when security procedures are violated. Underlying all of this is the concern that the violation of security policies does not always coincide with an attack – in other words, staff may feel that they have succeeded when ignoring a security rule because nothing bad happened that time. However, this does not mean that they will always escape without a breach in security in the future.

Different Perspectives

Opinions and perspectives differ radically in this area. Some people believe that humans are a 'weak link' in information security. In this view, automated tools should assume as much responsibility as possible for data input, processing and consequent actions. This approach builds on conventional security practices in restricting access to critical resources. However, increased levels of automation lead to an increasing emphasis on systems configuration and management. Errors by systems administrators can lead to massive vulnerabilities – hence, it is difficult to envisage a future in which human factors can be entirely engineered out of information security.

The retrospective analysis of security incidents is another active area of study. This looks at the root causes of security breaches. As mentioned above, most incidents stem from what can be called 'human error'. However, this is controversial because many would argue that human error cannot be a root cause of an incident. Instead, we must identify the reasons why a policy was ignored or deliberately violated. In this view, human error is a symptom of deeper problems in management or regulation. If companies had provided incentives – through training or closer audits then staff would be more likely to follow appropriate policies.

Those who view humans as the “weakest link” in information security, often rely on the enforcement of rules and procedures to ensure that staff do as they are told. However, the continuing high level of security violations suggests that other support is needed if we are to improve systems security. In particular, it is often important to explain not just the ways in which to comply with a rule but also to explain the justification and motivation for a particular policy.

Open Research Questions

Some of the issues to do with usable security and the human factors of information security are also raised in the topic that deals with cyber exercises – this focuses on issues of training and contingency planning – helping people to prepare for an attack. In addition, the following list provides a partial summary of open questions in this area:

- **Human Error vs Human Resilience**?
  Conventionally there has been a focus on why humans violate security policies. However, there is a growing area of research within resilience engineering that focuses on the reasons why “things go right rather than why things go wrong”. Everyday companies successfully detect or mitigate attacks, by studying these more frequent successes we may learn more than be studying infrequent/catastrophic failrues.

- **How to Achieve Usable Security?**
  As mentioned before, there is a very active community looking at ways to make security mechanisms easier to use. Much of this work focuses on authentication – alternatives to passwords using biometrics such as fingerprints, or graphical passwords of various forms. For many years these approaches had only limited up-take but many have recently been successfully used on mobile devices. Other aspects of usable security research focus more on systems administration tasks – how to easily configure access control mechanisms, how to detect and mitigate attacks without overloading users with false alarms (see the section on situation awareness below).

- **How to Support Cyber-Situation Awareness.**
  Endsley has published widely on the concept of situation awareness in dynamic systems. It has recently attracted a lot of attention within security research. In particular, it has informed the development of systems ‘dashboards’ that are being deployed by service providers so that their staff are alerted to potential anomalous behaviour that might be symptomatic of malware. It is important to present this information in a way that does not overload the operator with too many false alarms, equally if the system filters many potential alerts then users may miss a critical warning of an impending attack.

- **Audits vs Training?**
  There are many different techniques for improving human behaviour in following security policies but at the heart is a question about whether it is better to spend resources on audit and disciplinary action to ensure compliance or to focus more on the promotion of positive behaviours. Complicating factors include the Hawthorne effect,

individuals will act differently when they know that they are observed – this issue is raised in the section on cyber-exercises but it is a general concern for training. Initial compliance with policies and procedures may reduce over time as staff forget the lessons that they learned in the past.

References

Bartsch, S., Sasse, M. A. (2013). How Users Bypass Access Control - And Why: The Impact Of Authorization Problems On Individuals And The Organization. Proceedings of the 21st European Conference on Information Systems. (pp.Paper 53-). Utrecht, Netherland

S. Brostoff and M. A. Sasse, "Are passfaces more usable than passwords? a field trial investigation," in Proc. HCI '00, 2000. Available at: http://www.cs.ucl.ac.uk/staff/S.Brostoff/index files/brostoff sasse hci2000.pdf

C. Colwill, Human factors in information security: The insider threat – Who can you trust these days? Human Factors in Information Security, Volume 14, Issue 4, November 2009, Pages 186–196

Endsley, M.R. (1995b). Toward a theory of situation awareness in dynamic systems. Human Factors 37(1), 32–64.

Karen Renaud. Blaming Noncompliance Is Too Convenient. What Really Causes Information Breaches? IEEE Security & Privacy. May 2012..

K. Renaud_ P. Mayer, M. Volkamer and J. Maguire, Are Graphical Authentication Mechanisms As Strong As Passwords? Proceedings of the 2013 Federated Conference on Computer Science and Information Systems pp. 837–844