This is the published version of:


Copyright:

Copyright the Publisher. Version archived for private and non-commercial use with the permission of the author/s and according to publisher conditions. For further rights please contact the publisher.
Using Simulation for Effective Computer Security Training

WARRICK FONG
CHANG SOO LEE
PAUL A. WATTERS
Department of Computing, Macquarie University

ABSTRACT
User-awareness continues to be a major hurdle to addressing computer security concerns in the business environment. The aim of this project was to develop a simple but effective training facility for computer security awareness, based on a simulation game that explores different ways in which security can be achieved. Security concepts rarely translate easily into virtual representation. However, by identifying appropriate security components, we were able to construct a business scenario that participants could relate to, rather than relying on simple textbook examples. Measuring the real impact of threats continues to be a significant constraint to a realistic simulator. Risk analysis and better metrics would appear to be a solution to this problem – having an interactive game does not guarantee the successful delivery of an educational goal.

Introduction

Computer security continues to be an ever-present issue in the corporate environment. Numerous surveys indicate that security breaches of various kinds associated with viruses and other types of malware have a direct cost of around US$12 billion per year for business (D’Amico, 2000), while consumers directly pay around US$5.2 billion per year to repair or replace crippled home systems (Hart, 2006). Not keeping up with cyber threats can sometimes place business viability at risk. Most security texts (e.g., Abrams et al., 2001) provide good coverage of security principles, although they vary considerably in their emphasis on specific topics. There also exist numerous papers and commentaries directed specifically at solving current computer security issues (e.g., Anderson, 2001; Pfleeger & Pfleeger, 2003). Nevertheless, all are consistent in the recognition that computer security, previously an afterthought, has quickly become an integral part of the core business
model. The plethora of security manuals, guides and gurus has done little to increase general awareness of information security across the organisational spectrum.

What are the information security concepts that users really need to be aware of? Most organisations continually strive to achieve competitive advantage. Having better quality information assists in enhancing such an advantage. Conversely, keeping confidential information secure deters competitors from acquiring what would otherwise be a subjective advantage. Computer security, in the business sense, ultimately becomes the proper management of information resources (Anderson, 2001), and concerns itself with the preservation of the following non-functional requirements (AusCERT, 2004):

- confidentiality – prevention of improper disclosure of information
- integrity – prevention of improper modification of information
- availability – prevention of denial of authorised access.

Barker (2004) refines these further in his six-element security framework:

- availability – usability of information for a specific purpose
- utility – usefulness of information for a specific purpose
- integrity – completeness, wholeness, and readability of information and quality unchanged from a previous state
- authenticity – validity, conformance, and genuineness of information
- confidentiality – limited observation and disclosure of knowledge
- possession – holding, controlling, and having the ability to use information.

Maintaining adequate security comes at a cost and often involves trading off investment in one area against another. There are inherent risks involved with inadequate information security (or perhaps its perceived adequacy). Security can sometimes be interpreted as ‘acceptable risk’, while still maintaining a competitive advantage. It involves decisions made to balance the cost of providing security to business-sensitive information, versus the cost as a result of its potential loss. Workers at all organisational levels can have access to this information, and can be sources of leakage, if they do not have appropriate training. Yet it seems unlikely that many individuals would read an information security textbook out of interest – so how do we change awareness and practices across an organisation to minimise risk?
PROBLEM OVERVIEW

Can computer security be effectively simulated – and if so, how? What are the security objects that should be involved, and how do we represent these? To what detail do we need to capture the nature of these security objects? How do we measure the impact of threats? These continue to be some of the interesting questions when attempting to construct a security game that can be used by people who are not security experts to raise their awareness levels.

From a general perspective, encouraging IT security consciousness is an ongoing problem area, particularly when dealing with business managers who were in the workforce before computer use became widespread. Some do not appreciate the vulnerability of IT systems or leave IT security to security managers who themselves may not be particularly IT literate.

Given the diverse nature of computer security we need to ascertain the purpose of our simulation, and who the audience is. Areas of focus could range from physical device settings, to logical concepts – and anything between the two. Wrapping these extremes are policies which dictate the processes and procedures to ensure that the security principles are adhered to. Would the simulator be in ‘real-time’ – or does this matter?

Impact could be viewed as the subjective costs necessary to reinstate previous functionality (Bond, 2004). Conversely, impact could be seen as the extent of risk exposure that an organisation is willing to undertake, while still maintaining an expected level of competitive advantage. Often, the difficult aspect is the unit of measure, which may not easily translate into monetary terms. This manifests itself in two ways:

- The relative costs of impact varies between organisations, as a particular threat to one organisation may not necessarily have the same effect on others.
- Reporting of security threats is generally not publicly disclosed for fear of negative reputation, and possibly an invitation to further attacks (Gollmann, 1999).

PEDAGOGICAL PERSPECTIVES

The pedagogical tools used by many training organisations – lectures, tutorials and textbook readings – are effective methods of learning in many disciplines, but for many people, learning can be significantly enhanced by hands-on participation (Aldrich, 2005). This can be achieved even if students are learning at a distance, or from their workplace (Watters, 2006). The use of interactive tools encourages participants to apply new skills and reinforce their learning. The question is no longer whether a learning tool will be useful – instead it is more a question of
how best to construct such a tool to facilitate learning.

In the arena of computer security, it is relatively difficult to simulate a fully functional environment. The field is extensive and there are numerous variables to account for. The best environment is the real world – although using such an uncontrolled environment for testing ideas may simply be unsuitable due to the inherent security risks involved. To work around this, we need to canvass issues that affect computer security and identify components that can be modelled. In addition to its suitability for simulation, this selection needs to be aligned with the objectives of the formal classroom agenda. Depending on the security context, varying degrees of emphasis toward specific components needs to be taken into account. There is an inherent limitation to capturing several security principles in a general game, and yet still be sufficiently detailed to provide an educational purpose.

From a game-oriented perspective, there needs to be a purpose and objective to the exercise, mainly to avoid a wane in interest. A scoring mechanism needs to be in place to instil a competitive purpose. Instead of playing against the computer, players can be pitted against each other. This approach allows the game to evolve according to participants’ experiences, and the outcome is the collective result of the choices taken by all participants. As in reality, there is no final winner in such a scenario; it is a case of continued measures of each participant’s attempts to maintain competitive advantage, while not compromising computer security. It is expected that through the game process, participants get to think about security concerns, make decisions, and evaluate the impact of their decisions.

Having the ability to be both a defender and attacker also provides for a more dynamic scenario and moves closer to a realistic scenario. It is not the objective of the simulator to precisely accommodate monetary costing nor quantify the actual impact to an organisation. It is sufficient that the impact is recognised, and its significance apportioned to the necessary resources required to rectify or mitigate it. For this reason, the use of a non-absolute ‘cost-scale’ provides a relative comparison between different security components.

Some examples of a few such simulators are in the form of a game where participants assume the role of an attacker or defender of a computer system. Others are simply in the form of online quizzes (Irvine et al., 2005), in which progression to the next stage is attained by successfully meeting the current set of challenges, or correctly answering the questions. Digital Hazard (Irvine et al., 2005) is a simulator game where the player is a hacker. Apart from snazzy graphics and audio (which do not appear to provide any real functional value), game interaction is primarily achieved through the command line. Essentially, the game teaches hacking skills, with instructions provided along the way.
to guide the player to the next step. It is very much focused towards attacking with insufficient regard to other security concepts.

CyberCIEGE is currently being developed by Rivermind (Irvine et al., 2005) under sponsorship by the US Navy. Irvine and Thompson refer to computer security as “information assurance” (IA) (2003, p. 64). They have broken the complexity of IA into what they see as relevant components of IA and built specific scenarios around this. The scenarios are broken into separate game modules, each concerning itself with specific computer security concepts. Participants must configure and maintain an environment where the assets are protected against certain threats. The game interface includes graphical elements to enhance the realism of the game. The authors have undertaken extensive research and identified specific security components, and assigned arbitrary monetary costs to securing such components.

In this paper, we present the results of a project where we attempt to promote information security awareness by using a game, with a view to its usage as a learning tool. The goal is to provide a realistic simulation environment, developed using the Java programming language, which goes beyond the CyberCIEGE approach of just focusing on how to attack, instead focusing on broader issues in information security. For example, one system risk may be deemed acceptable if it gives rise to an acceptable economic loss, whereas another risk might be deemed critical. Teaching all members of an organisation to understand risk in information security is critical, as it is simply not technically or economically feasible to address all risks. Indeed, all network attacks could be prevented by simply switching off the Internet, but this is clearly not a desirable solution.

In the following sections, we outline the methods used to design the game; describe the basic interaction sequence used during the game; and present our evaluation of whether the simulation is realistic or not.

**Methodology and Design**

To ensure the broadest possible uptake within organisations, users of the game are not assumed to be IT savvy. However, some basic exposure to relevant computer security theories would be useful. Thus, the game should be played in conjunction with an introductory IT security course, pitched at an appropriate level.

The focus of scenarios presented in the game should be on the security of commercially sensitive information, and how its loss could affect business continuity. This may include (although not exhaustively):

- identifying security-sensitive components of a typical business environment
• understanding the common security concerns facing most organisations
• understanding some of the decision-making processes to identifying what ‘acceptable risk’ is
• understanding the implications of information loss as a result of security breaches
• exploring common methods and tools used by hackers to circumventing security, and how to detect and respond to such threats.

The above will be considered in the light of how it will best fit into a simulator with the object of a learning experience. The objective is that the participant needs to make an assessment as to the purpose of the security component, and what the implications are of the components’ configuration.

For the purposes of the game, each participant is responsible for the IT security of a fictitious cosmetic company. Each has a ‘secret formula’ that is not to be disclosed to unauthorised parties.

All participants begin with equal resources and competitive advantage (CA). For simplicity, it is assumed participants could spend on either computer security, or marketing; the latter strongly influencing the profitability of the company. The setup and securing of security-components involves costs, and it is the participant’s decision-making process that will determine how much resource is allocated to secure their organisation – obviously, with a reduction in the marketing budget. Once all participants have completed configuration, a round of the game is played, similar to a round in a card game; each round could reflect a business cycle, or month of the year.

Participants are exposed to threats and environmental elements, for example, hackers, or electrical disruption, amongst other things. Threats could affect one or more security components of each participant, and their security component may/not be compromised, depending on their setting of that component. After each round, each participant is given the opportunity to assess the results from the previous iteration. Changes would be introduced as a result of other participants’ tactics, environmental influences, and marketing profitability. Remember that the overall objective is to maintain competitive advantage, so this will not be achieved without due consideration to the marketing budget. The resulting profitability may be inversely proportionate to the amount of IT spending. Resources available for computer security spending in subsequent rounds is influenced by the marketing outlays apportioned in previous rounds – so, participants simply cannot expend all current resources to fortifying their IT infrastructure, as maintenance of an aggressive security campaign will require significant ongoing expenditure (Kabay, 2002).
USING SIMULATION FOR EFFECTIVE COMPUTER SECURITY TRAINING

The following categories are used to organise security components:

- **Infrastructure Layer** – focuses on the office environment, computer hardware, and the physical network
- **Logical Layer** – describes processes and procedures affecting hardware
- **Application Layer** – describes software, processes and procedures, and access controls
- **Information Pane** – provides useful information on available resources, security components, and results of previous activity
- **Extra-curricular Activities** – players can expend resources to gain competitive advantage. This could be in the form of hacking activities aimed directly against another competitor.

The following processes are used in the game implementation:

- The usage of security components is reflected by the level of setting made by a player. Each security component has an associated cost, and the higher the setting, the more resource will be required. Resources are reduced accordingly, as security components are set.
- Automatic decrement of security component setting occurs after each round. This simulates the cost of ‘maintaining’ the security component. Expenditure is reflected in the marginal cost of reinstating the previous setting, without having to outlay the whole cost of the security component.
- A security threat can affect one or more security components. The effectiveness of a security component in warding off threats depends on the severity of the threat. Conversely, a security component can be affected by more than one threat, and the success of the security component depends on the net outcome of the threat matrices.
- Each turn represents a fictitious business cycle and players’ resources change in response to the ‘changes in the market’. Essentially, revenues resulting from a player’s competitive advantage reflect the proportion of non-IT spending, relative to the other players.
- Changes in security status involve issues resulting from the previous activities, and arising from previous rounds. These will only be evident if the participant selected logging/auditing for the particular set of affected security component(s).
- To provide variation, each participant could expend resources toward ‘extracurricular’ activities against other participants, and to gain competitive advantage. The intent is malicious, with the objective of obtaining the competitor’s ‘secret formula’. ‘Honeypots’ could also be set up to see if another competitor is hacking.
A ‘king-down’ situation occurs when a player’s infrastructure is sufficiently compromised, to the extent where it no longer becomes feasible to continue as an operating concern. A predefined combination of security components has been sufficiently compromised to the point where a threat exposes the organisation’s ‘secret formula’ to unauthorised parties. For the purposes of this simulation, the exposed participant would have lost the game, and in reality, this outcome reflects a worst-case scenario.

Evaluation

This project attempted to encapsulate computer security principles in the form of a game, with a view to its usage as a learning tool. A great challenge has been to develop a realistic context in which to frame an otherwise idealised exercise, with respect to the characterisation of security concepts. Attempting to encapsulate security in a virtual context will invariably result in some deviations from reality, which is acceptable for a limited educational purpose. To that end, it is intended that the game be delivered in the form of a business scenario, the objective of which is to maintain competitive advantage. Along the way, participants would always be encouraged to think about the consequences of their security choices.

Quantifying the impact of security breaches is frequently subjective. This is often due to non-disclosure by affected organisations, and the relative measure of actual impact varies between organisations. Fortunately, this is changing with the publication of statistics through AusCERT (2004) surveys which provide a general picture of how security concerns are evolving.

The project team encountered the greatest difficulty in suitably organising the myriad of computer-related objects into succinct categories. Not only are there interrelated dependencies between components, several can fall into many categories, depending on the context in which it is used. For example, a firewall can be both a physical device, and a software application, for which logical rules are necessary to ensure its effectiveness – how then should such a component best be classified (device or application)?

It appears that distinct learning modules, each dealing with a particular security concern, may be necessary to provide the appropriate level of focus. As an idea, the security game sounds appealing, although quickly loses initial appeal without the allure of ‘bells and whistles’ expected of a typical game experience. Although technically functional, and utilising a graphical interface, further developments will need to be
made in this area to enhance the game’s usability.

What is the real cost of security to an organisation – is it more than the simple cost associated with the replacement or reinstatement of one or more components, or something less tangible (Guzman, 2003)? This conflict appears be the most difficult concept to encapsulate in the game, and continues to be largely unanswered. One of the challenging tasks is to measure a security breach, and its consequential impact on an organisation’s profitability (Plato, 2004). We are left to hypothesise and extrapolate from estimates, as most companies are unwilling to provide this type of raw data. Thus, the identified impact would always be based on a subjective assessment, and this would clearly vary from one organisation to another. Part of the difficulty arises from the lack of information about actual costs, and how these are measured. For example, how much damage to reputation does an organisation incur as a result of website defacement? The impact would appear to be extremely varied, even among organisations within the same industry.

The cliché, “security is a journey and not a destination” captures the essence of the dilemma. If this cliché were true, there should be no theoretical limit to the amount of spending to protect a business. No business activity should be treated as a journey that never ends - indeed, all security initiatives should come to a logical end and then be evaluated for their success (e.g., SANS, 2006). Metrics need to be established relative to security objectives and these assessed to confirm that they are providing real value (Shema & Johnson, 2004). Estimates were used to quantify the amount of resources required to enable components. In addition to the existing game-play logic, quantifying the full impact of a security threat would require further research – this is likely to be answered through further analysis in the area of risk management.

**Discussion**

The simulation currently provides a centralised, single system perspective on security. Future development will focus on implementing a networked configuration. Currently, a single, turn-based game, the provision of a networked interface can provide better dynamics and introduce the real-time concept of urgency. All players can then be constrained by time limits within which reactions to current threats have to be made.

Improving the metrics for measuring the impact of individual decisions is a major challenge – the maturity and sophistication of an organisation’s overall IT framework will determine the type of metrics that can be successfully collected. As processes become institutionalised, the IT program evolves from simply having policies, to implementing
detailed procedures, and finally to integrating policies and procedures into
daily operations. At the highest level, processes can facilitate automated
metric collection, and may be effective in measuring efficiencies of
security controls with respect to the organisation's overall objects. The
impact of computer security decisions to the organisation's overall
objectives can then be determined by data correlation analysis. The
concepts of "defence in depth" and "blended-threats" (Swanson et al.,
2003), and how these translate into the simulator, must be further
explored. The idea of 'one threat, one cure' has become outdated as
threats attempt to achieve more than one single purpose. Security
components could be arranged in complementary configurations thereby
providing a layered defensive mechanism against specific threats. This
could also be a refinement of the 'king-down' situation, where inter-
related components assist in fortifying various layers of an infrastructure.
In addition to cushioning the impact of a threat, layering also provides
checkpoints of alerts where assessment of damage could be measured.
However, given the combinatorial explosion in matching multiple
components of a possible solution to determine an optimal outcome needs
to take place in a realistic, time-pressured environment.

A dedicated hacker role, where a player could assume the role of a
 hacker, with the objective of causing havoc to other players, could add a
dedicated rogue element into the game.

In conclusion, computer security is the attempt to mitigate the method,
motive, and opportunity of attackers. Technically, this may not be
difficult - however, it is the users interacting with these computer systems
who frequently determine the extent of risk exposure, as they are often the
target of socially engineered attacks. The reality is that security policies
are only effective if individuals adhere to them.

More broadly, the gaming approach suggested should work in making
at least some of the private sector workforce more security conscious,
particularly those who already enjoy gaming or who work in IT. They no
doubt would be willing participants. If used for the general workforce, to
raise awareness of security issues, it would have to be relatively
uncomplicated or perhaps have incremental levels of difficulty. Less
sophisticated security gaming than what we are proposing has already
been used in government agencies to raise consciousness of security
levels.

The use of simulation tools is a positive step towards raising
awareness about computer security concerns. Given the wide breadth of
security concepts, constructing a simulator that fully reflects reality is a
non-trivial task. Subtle interdependencies between security components
sometimes cannot be captured in a virtual construct. Quantifying the
impact of threats continues to be a major constraint to a realistic
simulator. Risk analysis and better metrics can assist in addressing this
issue. The ideas covered in the project serve as a foundation for further development. A game delivered in the context of a business scenario is easily understood by non-IT players and provides a means through which better security awareness can be achieved.

REFERENCES


Guzman, Y. (2003). Security budgets are up, so is accountability. http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gei932898,00.html


APPENDIX A

The following provides an example of how resources are calculated for players after each iteration of the game. Assuming all players initially begin with 100 units of resources, and each player outlays the following for computer security:

**Player resources (a)**

**IT spending (b)**

**Marketing (c)**

**Resources (d)**

1. 100 30 70 74.90
2. 100 50 50 53.50
3. 100 60 40 42.80

The amount allocated to marketing (c) to will therefore be (a) – (b). In this round, the economy has spent 160 for marketing, i.e., the sum of all players’ marketing. Given a 7% profitability rate for the cosmetic industry, the resources (d) after this round for player 1 will be:

\[
\frac{70}{160} \times (1.07 \times 160) = 74.90
\]

The approach ensures that competitive advantage reflects the proportion of outlays each player makes toward marketing, relative to other players in this ‘closed economy’. Business viability cannot be achieved without adequate forethought to both computer security and other competitive challenges.