ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

CRIME PROOFING TECHNIQUES IN ICT SYSTEMS USING INFORMATION INTEGRITY APPROACH

Kishor M. Dhole[1], Dr. Vinay Chavan[2]

Research Scholar, Department of CS and IT, S.K.Porwal College, Kamptee, Nagpur, India[1]

Associate Professor and Head, Department of CS and IT, S.K.Porwal College, Kamptee, Nagpur, India[2]

Abstract: This paper aims to discuss the crime proofing techniques using information communication technology (ICT). It suggests importance of information integrity in product proofing. Paper covers the issues of crime proofing with information integrity (I*I) attributes namely consistency, accuracy and reliability. It insists on concepts, needs and requirements of ICT in product proofing. This adds the authentic many techniques for crime proofing and prevention to reduce risk using I *I value. In order to do this it suggests issues with I *I attributes in crime proofing, which improves security, usefulness and usability of these products and services. In this context I*I attributes supports for minimizing I*I risk and improves the effectiveness of crime proofing services.

Keywords: Information Integrity (I*I), Information Security, Information System (IS), Crime Proofing, Information Value, Information Communication Technology (ICT).

I. INTRODUCTION

This Today's era is the world of ICT. Everyone wants to access and shared information from different available online sources. Hence there is a lot of possibility of information hacking and misconduct of useful data. It assures possibility of crime in this uncertain environment. Therefore crime proofing technique is the need of time. It has been observed that certain products and services have a tendency to become the target or instrument of crime. Criminologists suggested various means of identifying those products likely to display these tendencies. Security is very important for IS and ICT infrastructures. Information has to be secured to ensure that it cannot be read or modified by unauthorized parties, and that its origin and destination can be proved correctly. It requires more security envelope so that no one can open it easily. The information used in this context must show integrity features. Thus this requires Information Integrity attributes (CAR) for correctness of information, consistency of used information, and reliability of information. Its determinants are namely "consistency" (C), "accuracy" (A) and "reliability" (R) in the acronym defined as CAR [1].

In addition, the networks themselves have to be securely managed and protected against compromise or attack; criminals have to be prevented from misusing them and the potential for fraud has to be blocked. The increasing Complexity and rapid development of new systems present a real challenge when securing ICT systems. It is not feasible to eliminate felony hazard overall "crime proofing" should seek to elevate awareness among identified interest groups of the crime risk that may be linked with certain merchandise/service types by using I*I attributes. The aim is to reduce the level of crime risk associated with any significant merchandise, product type or service. The objective of product proofing values is to avoid circumstances which might give increase to a crime wave by reviewing, wherever possible in advance of a new product/service commence the crime risk intrinsic in products/services.

The European Commission services believe that European standardization in this area will contribute significantly to crime proofing products or services [2]. But researcher suggested that these product/services introduced with measures likely correctness, reliability and trustworthiness of information improves the quality and effectiveness of the products. One possible solution would be the development of a check list of factors to be taken into account at an appropriate stage in the product/service development process that will increase general crime prevention and contribute to the protection of citizens. Such a check list would enable products and services to be reviewed in terms of their crime hazard. These checklist examined under I*I attributes namely consistency, accuracy of information and reliability of information being used in it. Design or other technical alterations could be introduced, or recommendations for use made, taking account of recognized crime risk. Such yields or services could then be introduced as having been "crime proofed". A key aspect of product proofing is to encourage a greater degree of social responsibility on the part of industry in terms of user/consumer security from

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

crime associated with certain I*I based products and services. I*I have a tendency to be targeted for criminal purposes, effective "product/service proofing", should also promote active industry participation in designing crime out of products and services. These contacts are useful and necessary to support and enhance policy development in the area of integrity, freedom and security. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

II. CRIME PROOFING

"Crime proofing" or 'Proofing Products against Crime', illustrates the act of integrating or embedding crime-prevention features into products and services based on I*I attributes. This covers accuracy of information, error free correct data and reliability of information used in it. This aims to reduce risk and control their potential to become aims of criminal activity like as theft, scam and damage. It also supports to prevent their use as gadgets of crime.

III. I*I DEFINITION

Information Integrity (I*I) is dependability and trustworthiness of information and controlling. It is a key factor for determining strategic business advantage. Its attributes are consistency, accuracy and reliability of information system (IS) and information there from [3].

Need of Information Integrity

For competitive advantages in software development process, requirement then is to minimize informational errors due to loss of information in product/services, i.e., to ensure correctness aspect of information, which also includes exactness aspect. This demands going beyond "reliability" requirement and to ensure "consistency" (C), "accuracy" (A) and "reliability" (R), i.e., Information Integrity (I*I) of information system (IS) and information there from. This introduces requirement to originate information effectively and economically, which in turn calls for recognizing that information "origination" is a valuable activity [4].The term 'product' covers physical substances, electronic information, electronic services and computer software. The goal of crime proofing is to:

- Avert an offence;
- Control the risk value;
- Lower the impact of an offence;
- Integrity of information in it;
- Facilitate detection of an offence;
- Facilitate other responses to an offence, as appropriate.

There has been significant activity to increase awareness with reference to Product Proofing against Crime, especially in the Indian perspective [2] [5].

Requirement of ICT Product Proofing

Knowledge of the concepts of ICT Product Proofing is useful for professionals involved in analyzing, designing, developing, implementing or simply studying information systems, telecommunications, information technology and e-communication systems using I*I attributes. In European Commission there is a good progress to design such crime-proof products [5], but in Indian context, it needs to aware people to design and develop such products. This brings more assurance of high integrity and quality, with improved security in product software.

Concepts of Crime Proofing (*The 5 I's)*

The concept of Proofing products against crime [6] necessarily occurs as a process and this can be summarized with the factors namely: Intelligence, Intervention, Implementation, Involvement and Impact. These factors succeed in reducing crime levels using I*I attributes, improves standards, techniques, principles and achieves cost-effectiveness in acceptable manner.

CRAVED: 'Hot products' is a term applied to frequently stolen goods or services[7].Products in this sense could be mobile phones, satellite dishes, high-definition TVs, digital-audio players, cable TV airtime, internet bandwidth, or personal identity and financial information. Hot products have characteristics captured in the acronym CRAVED namely as: Concealable, Removable, Available, Valuable, Enjoyable**,** and Disposable. The set of techniques encourages the identification of crime-by-crime proofing efforts with I*I attributes (C, A, R).

IV. THE TECHNIQUES OF CRIME PREVENTION

The following 25 techniques are a cornerstone of the practice of Crime Proofing. Developed over a quarter of a century by Professor Ronald V Clarke, the techniques seek to modify aspects of situations relating to specific crimes in ways that reduce criminal opportunities [8].The following table depicts "25 techniques" aim to tackle specific crime problems. It is more useful to specify 'identity theft via email phishing' or 'identity theft via credit card theft' than it is to specify identity theft in general. This is because different types of identity theft typically will require different approaches to crime proofing. The same is true of almost all types of ICT related crime.

The origin of the techniques derives from environments different than electronic crime. Some effort is made to apply the techniques to ICT crimes, while realizing that these tactics can be tailored to specific types of electronic communication linked crime. The first step towards identifying new crime proofing approaches is the identification of existing good practice and determining the possibilities for their broader application using information integrity issues [8]. The overall goal of crime-proofing, identified by these techniques, is to make crime less attractive to offenders by increasing the effort and risks, reducing the rewards, or reducing provocations and

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

excuses that encourage crime. These considerations include the cost and crime risk assessment issues so that the creation and selling of a crime-proof product remains feasible and provides a viable business model.

The 25 techniques are not all equally appropriate to different situations or crimes[9]. The framework should be used as an aid to brainstorming and analysis that leads to identifying the mechanism by which crime proofing maybe achieved. The 25 techniques are grouped into 5 main categories: each of these five categories contains five techniques that can be applied as shown in table.

Table 1: Techniques of Crime Preventions
Source: Borrowed from [9]

Increase the Efforts	**Increase the Risk**	**Reduce the Rewards**	**Reduce Provocations**	**Remove Excuses**
Target harden	Extend Guardianship	Conceal targets	Reduce frustrations and stress	Set rules
Control access	Assist natural surveillance	Remove targets	Avoid disputes	Post instructions
Screen exits	Reduce anonymity	Identify property	Reduce Emotional arousal	Alert conscience
Deflect offenders	Utilize place Managers	Disrupt markets	Neutralize peer pressure	Assist compliance
Control tools/ weapons	Strengthen formal surveillance	Deny benefits	Discourage imitations	Control drugs and alcohol

i. **Increase Effort** needed to entrust the crime. Many potential offenders are deterred if a crime is too difficult. They do not have the required skills or are not willing to put in the time required.

ii. **Increase Risk** in committing the crime. Risk includes the risks of getting trapped, the risk of failure, the risk of loss of resources and other risks. The risk of being detected in the commission of a crime is increased through, for example, tracking on the internet, and more recently in relation to many telecommunications products, by the risk of GPRS and GPS or other tracking. More broadly however, risk is increased by shadowing and monitoring which can be formal (police and security) or occurs informally as part of everyday practice. Open platforms such as Linux, for example, encourage widespread surveillance and effort that protect and improve its code, whilst a busy street can provide close watch that reduces robbery.

iii. **Reduce Provocation which might lead to the** crime.

iv. **Remove Excuses** which allow people to 'justify' or 'allow' the crime. This can be in the form of simple reminders that certain types of offence are illegal. Digital audio players and computer software often carry a label stating that music or software piracy is theft and a criminal offence.

v. **Reducing Rewards** to the commission of a crime. For example, blacklisting mobile phone does not make them any harder to steal. Rather, it works by the mechanism of reducing the rewards to stealing them because, if they do not work, they have a lower re-sale value.

V. IMPLICATION OF I*I ATTRIBUTES IN CRIME PROOFING

The issues covered in crime proofing affects with I*I attributes. These attributes are accuracy, consistency and reliability of information in crime proofing. Consistency improves the link of information flow in crime invention techniques. Accuracy of information supports for proper selection of information decision at design and developing the strategy of product and services. Reliability features improves the effectiveness and efficiency of the crime invention mechanism. All these three attributes contributes risk reduction, uncertainty in product process and quality of the process. It also controls the loss of errors and delay in ICT systems. It also deployed to support Security and Privacy Issues of I*I. Actions to crime proof a product should be commensurate with the risks being addressed. Excessive or improper solutions may result in security violations or attack on the personal privacy of users.

VI. CONCLUSION

This Paper has presented some of the key concepts, approaches and frameworks relating to crime proofing, with the aim of facilitating the development of standards to support product proofing against crime. The paper covers information integrity issues for crime proofing techniques in ICT systems. It imposes that I*I attributes creates positive impact on product proofing techniques. Examples have been given of where crime takes place in ICT, and some instances presented of standards designed to combat such crime. This Paper has highlighted the fact that there are many types of crime of relevance to European Telecommunications Standards Institute (ETSI), and to ICT in general. It also indicates that many different types of crime proofing efforts are required. Standards for product proofing need to be built upon a knowledge platform concerning crime proofing using information integrity attributes. The study of the current situation in crime-proofing against ICT crime has resulted in a series of recommendations and issues in I*I likely consistency, accuracy and reliability.

REFERENCES

[1] Mandke V. V. and Nayar M. K., Information Integrity - A Structure for its Definition. Proceedings of the 1997 MIT Conference on Information Quality edited by Diane M. Strong and Beverly K. Kahn, Cambridge, Massachusetts, USA, October 25-26, 1997.

[2] EC DG Justice and Home Affairs – 'Minutes of the workshop of 26 September 2003 on Designing Crime out of Products and Services – an EU wide approach'.

[3] Mandke V.V. and Nayar M.K., Implementing Information Integrity Technology- A Feedback Control System Approach. IFIP TC11 WG11.5 Third Working Conference on IICIS, Amsterdam, The Netherlands,

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

November 18-19,1999,Edited by Magaret E. van Biene, and Leon A.M. Strous, Kluwer Academic Publishers, USA.

[4] Matthews Don Q., "The Design of the Management Information System", Auerback Publishers, NY1971.

[5] EC DG Justice and Home Affairs – EU Forum on the prevention of organized crime – "Minutes of the 2nd meeting of the workshop: the role of the private sector in the prevention of economic and financial crime"

[6] Ekblom, P. "Designing Products Against Crime", in N. Tilley (ed) Handbook of Crime Prevention and Community Safety, Cullompton: Willan Publishing (2005).

[7] Clarke, Ronald V., Hot Products: Understanding, Anticipating and Reducing the Demand for Stolen Goods, Police Research Series Paper 98. London: Home Office (1999).

[8] Cornish, D. B. and R. V. Clarke. 2003. 'Opportunities, precipitators and criminal decisions: A Reply to Wortley's Critique of Situational Crime Prevention' in M. Smith and D. Cornish (Eds.) Theory for Practice in Situational Crime Prevention, volume 16 of Crime Prevention Studies. Monsey, NY: Criminal Just Press.

[9] Tavani, H. and Grodzinsky, F., "Cyber stalking, personal privacy, and moral responsibility", Ethics and Information Technology, Volume 4, Number 2 / June, 2002.

BIOGRAPHY

Mr. KISHOR M. DHOLE had done M.Sc. (Comp. Science), MCA, M.Phil (Comp. Sci), B.Ed. and pursuing Ph.D in Computer Science from RTM, Nagpur University,Nagpur (INDIA). He is currently working in Seth Kesarimal Porwal College,Kamptee, Nagpur(India).

DR. VINAY CHAVAN, Ph. D., M.Sc, M.B.A., M.C.M., is Associate Professor and Head, Dept. of Computer Science at Seth Kesarimal, Porwal College, Kamptee, having vast experience of teaching in the diversified area of computer science. His current research interests are in the areas of data mining, cloud computing, software product development and its marketing. He is member of different bodies in academic field. He has published 35 research papers in National and International Research Journals and two books by international publisher. He has attended and chaired sessions in National and International conference.