ETSI White Paper No. 5

ICT Product Proofing Against Crime

Authors:

Charles Brookson (DTI UK)

Graham Farrell (Loughborough University, UK)

Jen Mailley (Loughborough University, UK)

Shaun Whitehead (Loughborough University, UK)

Dionisio Zumerle (ETSI)

February 2007

European Telecommunications Standards Institute
F-06921 Sophia Antipolis Cedex, France
Tel +33 4 92 94 42 00 Fax +33 4 93 65 47 16
info@etsi.org www.etsi.org

About the authors

Charles Brookson CEng FIEE FRSA

Standards, Assistant Director, UK Department of Trade and Industry

Charles Brookson works in the UK Department of Trade and Industry and is a Professional Electronic Engineer. He previously was Head of Security for one2one (now T-Mobile UK), and worked within British Telecom for twenty years before that.

He is Chairman of the NISSG, a group that was set up to co-ordinate security standards amongst the three European Security Standards Organisations and other bodies outside Europe. He is also on the Permanent Stakeholders group of ENISA, the European Network and Information Security Agency. He is also Chairman of ETSI OCG Security, which is responsible for security within ETSI, has been Chairman on the GSM Association Security Group (representing operators in over 200 countries) for many years, and has been involved in GSM and 3GPP security standards.

Dionisio Zumerle

Technical Officer, ETSI Secretariat

Dionisio Zumerle works in the Fixed Competence Centre of ETSI, where he is Technical Officer for the Technical Committees that deliver standards concerning IT and Telecommunications Security and Quality of Service aspects.

He received his MSc in Telecommunications Engineering from *La Sapienza* University of Rome. In the past he has worked in the ICT Central Directorate of *Poste Italiane* as Programme Management Officer for Service Oriented Architecture design and implementation.

Graham Farrell, PhD

Professor of Criminology and Director of the Midlands Centre for Criminology and Criminal Justice, Loughborough University, U.K.

Graham Farrell specialises in crime prevention research and has published widely in that field including 'Criminology and Security' in the *Handbook of Security* (Palgrave Macmillan, 2006). He recently directed research on designing-out mobile phone theft funded by the Engineering and Physical Sciences Research Council (UK), and is principal investigator on an EC project researching the theft and misuse of electronic services. He acknowledges the European Community funding under the AGIS Programme in relation to the Loughborough University contribution to this white paper.

Graham has previously worked at the United Nations office in Vienna, at the University of Oxford, at Rutgers University (New Jersey), at the University of Cincinnati, and was deputy research director at the Police Foundation in Washington D.C. He completed his doctorate at the University of Manchester in 1993.

Jen Mailley

Research Associate, Midlands Centre for Criminology and Criminal Justice, Loughborough University, U.K.

Jen Mailley recently completed research on designing out mobile phone theft and is currently working on a European Community project on the theft and misuse of electronic services. Prior to returning to academia, Jen worked as a Forensic Scientist and Expert Witness specialising in crimes against the person. She gained her MSc in Crime Science in September 2005 from University College London and is currently also undertaking doctoral studies.

Shaun Whitehead

Research Associate, Loughborough University, U.K.

Shaun Whitehead is a professional engineer. His previous experience includes several years as systems engineer on a range of space missions at Leicester University's Space Research Centre. Since moving into the field of crime science, he has worked on designing-out mobile phone theft on an EPSRC-funded project, and is currently working on an EC-funded project on the theft and misuse of electronic services.

ICT Product Proofing Against Crime

February 2007

This ETSI White Paper introduces the concept of Product Proofing (for ICT products and services) and provides a set of techniques that can be used for the identification and reduction of crime threats. An assessment of ICT crime and the state of knowledge concerning the nature of those crimes and their existing responses is then illustrated.

Finally, this ETSI White Paper identifies some key areas requiring further study that can lead to the development of crime proofing standards to promote the crime proofing of products and services.

Contents

Foreword

It is well established that certain products and services have a tendency to become the target or instrument of crime. Criminologists have suggested various means of identifying those products likely to display these tendencies.

Security is vital for ICT systems and infrastructures. Information has to be secured to ensure that it cannot be read or modified by unauthorised parties, and that its origin and destination can be proved.

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.

While it will never be possible to remove crime risk altogether, “product/service proofing” should aim to raise awareness among identified interest groups of the crime risk that may be associated with certain product/service types. The aim is to take account of and, where possible, attempt to reduce the level of crime risk associated with any relevant product, product type or service.

The objective of product proofing standards is to avoid circumstances which might give rise to a crime wave by assessing, wherever possible in advance of a new product/service launch, the crime risk inherent in products/services. The second stage is integrating relevant crime prevention measures into those products or services.

The European Commission services believe that European standardisation in this area will contribute significantly to crime proofing products or services. 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 assessed in terms of their crime risk. Design or other technical modifications could be introduced, or recommendations for use made, taking account of identified crime risk.

Such products or services could then be marketed as having been “crime proofed”. A “crime proofed” marking would mean that such products or services had been subject to a crime risk assessment and that appropriate measures had been taken to reduce identified crime risk. Over time such a mechanism could become not only a competitive marketing tool but also an effective mean of crime prevention.

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 protection from crime associated with certain products and services. In addition to being able to identify products and services which may have a tendency to be targeted for criminal purposes, effective “product/service proofing”, should also entail a mechanism to promote active industry participation in designing crime out of products and services.

The European Commission services attach a considerable importance to such activities and encourage their development under different possible forms of public and private partnership both at political and working level. These contacts are useful and necessary to support and enhance policy development in the area of justice, freedom and security.

In this context, the Hague Programme and its Action Plan provides for developing EU-wide Public Private Partnerships (PPP) to protect public organisations and private companies from organised crime, and to ensure that policy making in the area of security is based on state of the art research.

European Commission DG Justice, Freedom and Security

Introduction

'Proofing Products against Crime', or crime proofing, describes the act of integrating or embedding crime-prevention features into products and services. This aims to reduce their potential to become targets of criminal activity (such as theft, fraud, damage), as well as preventing their use as instruments of crime.

The term 'product' encompasses physical objects, electronic information, electronic services and computer software. Such products may be the direct targets of crime when they are stolen or otherwise harmed. They may also be used as tools to commit other crimes, such as stealing money from an online bank account. The overarching goal of crime proofing is to reduce the net harm from crime. This often includes reducing the overall frequency of crime but also includes reducing the impact or severity of crime.

The goal of product proofing is to:

- Prevent an offence;
- Lower the impact of an offence;
- Facilitate detection of an offence;
- Facilitate other responses to an offence, as appropriate.

There has been significant activity to raise awareness concerning Product Proofing Against Crime, especially in the European perspective (see [2] and [5]). The European Commission Mandate M/355 [1] explicitly requests concrete action from the European Standards Organizations on this topic.

Standardization, as a fundamental stage of the design phase for new products, should encompass an assessment of the crime threats, vulnerabilities and risks that products face.

Who should be interested in Product Proofing?

Knowledge of the concepts of ICT Product Proofing is useful for professionals involved in designing, developing, implementing or simply studying telecommunications, information technology and electronic communications systems.

Not only does crime-proof product development have the support of the European Commission (and very likely many other parts of the world), it also brings an assurance of high quality and improved security.

Key concepts for crime proofing

The Five I's

Proofing products against crime necessarily occurs as a process. This process can be summarised as the 5 I's:[9].

***Intelligence*:** The collection and analysis of information on the crime problem and its perpetrators, causes and consequences.

***Intervention*:** Applying generic principles, notably the 25 techniques introduced below through practical methods (for example reducing the black market value of a stolen product by tamper proof property marking).

***Implementation*:** Assuring genuine, practical solutions to crime prevention.

ETSI standards can help to encourage crime proofing at the manufacturing stage, preceded by consideration at the design stage of potential criminal opportunities.

Involvement: Mobilising individuals or organisations to act as responsible crime-proofers.

Leading standards bodies such as ETSI can have a key role in raising awareness, helping and ensuring that crime proofing occurs.

Impact: Assessing whether the intervention has succeeded in reducing crime levels, or the severity of crimes committed, and whether this has been achieved in a cost-effective and acceptable manner. In an area new to crime proofing, there is no point introducing anti-crime efforts without some indication of their efficacy.

Assessment of impact is critical to ensure feedback for the further improvement of crime proofing efforts.

Which products to crime-proof?

Crime proofing should be commensurate with risk. ICT products and services should, during their planning and development phase, be subject to a crime-risk analysis. The ensuing crime-proofing should not exceed in cost the potential social cost of the crimes involved, which include, but are not limited to, the financial loss of the asset to be protected. Other costs include those related to the health service, policing and the criminal justice system [42].

Whilst there are no precise estimates available, crime relating to ICT is thought to run into many billions of euros worldwide. As an example, hi-tech crime accounted for £74m of the £195m financial crime total identified in 201 surveyed firms in the United Kingdom in 2003 [39].

Some ways of thinking focus on categorising products under different levels of crime risk [10]. While a crime-proof analysis could prove to be complex and risk falling into the trap of subjective perspectives, a product-by-product approach and correspondent risk analysis seems to be the most suitable in this context.

Crime risk assessment should be conducted prior to the launch of a new product or service, and repeated throughout the product's life cycle, particularly when there is evidence of a change in the crime risk.

Crime targets and crime instruments

As stated in the introduction, this White Paper considers as a product anything a consumer may buy or own, including systems, information, services, and physical objects. Products can generally be divided into two categories:

- Products as targets of crime. Products that are stolen or damaged are targets.
- Products as instruments of crime. Products which are used to facilitate or conduct other crimes are instruments of crime.

These categories may overlap. Consider, for example, the theft of a mobile phone. Credit on the SIM card may be used before the SIM is blocked and the handset blacklisted. During the theft or robbery, both handset and SIM are arguably the target. The handset was a target because it may be re-sold. However, the handset was also an instrument to facilitate the theft of credit from the SIM.

CRAVED

'Hot products' is a term applied to frequently stolen goods or services.[3] 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:

- **Concealable** – and/or not easily identified as not belonging to the thief.
- **Removable** – not fixed and secured down (for physical objects)
- **Available** – cars were never stolen before cars were invented, and living next to a poorly lit car park increases the availability of potential targets.
- **Valuable** – in terms of monetary gain or psychological gain such as social status.
- **Enjoyable** – either from personal use, from the money gained when it is sold (see disposable below), or again from psychological gain.
- **Disposable** – the product can be sold on for monetary or other gain- there is a ready black market.

Theft is not just about value. A fridge may be as valuable as an expensive mp3 player, but it is less portable, less easily concealed, and probably less enjoyable.

The CRAVED concept allows the problem of theft to be considered on a product-by-product basis. It facilitates identification of key product characteristics that make it attractive to thieves. It therefore identifies which characteristics might be modified in order to proof that product against crime.

Moreover, the modification of one of the CRAVED characteristics may be sufficient to tip the balance such that the crime does not occur.

The characteristics which make a product attractive to thieves may be those which also make it attractive to legitimate customers, and crime proofing needs to take this into account. The set of techniques presented below encourages the identification of crime-by-crime proofing efforts.

The Techniques of Crime Prevention

The following 25 techniques are a cornerstone of the practice of Crime Proofing (within the field of crime prevention more generally they emerged from the area known as '*situational' crime prevention*). 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 [41].

The "25 techniques" aim to tackle specific, rather than generic, 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.

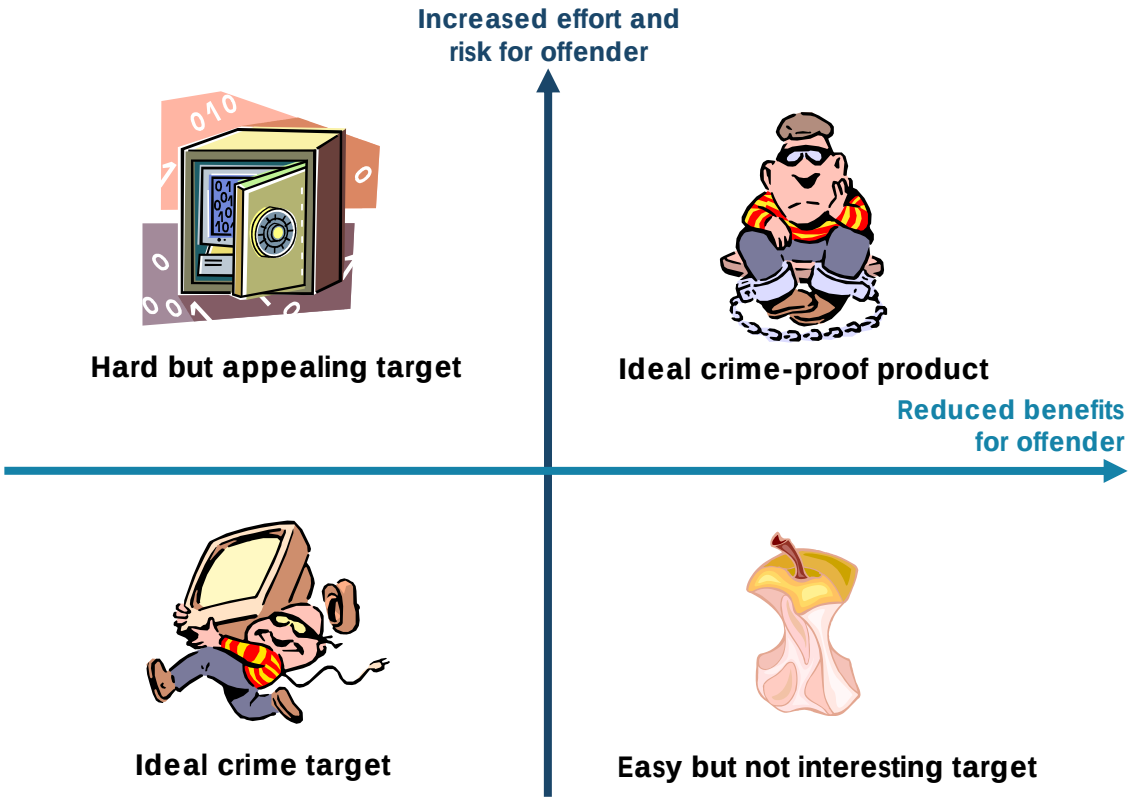
Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocations	Remove Excuses
1. Target harden	*6. Extend guardianship*	*11. Conceal targets*	*16. Reduce frustrations and stress*	*21. Set rules*
2. Control access	*7. Assist natural surveillance*	*12. Remove targets*	*17. Avoid disputes*	*22. Post instructions*
3. Screen exits	*8. Reduce anonymity*	*13. Identify property*	*18. Reduce emotional arousal*	*23. Alert conscience*
4. Deflect offenders	*9. Utilise place managers*	*14. Disrupt markets*	*19. Neutralise peer pressure*	*24. Assist compliance*
5. Control tools/ weapons	*10. Strengthen formal surveillance*	*15. Deny benefits*	*20. Discourage imitations*	*25. Control drugs and alcohol*

The origin of the techniques derives from environments different than electronic crime. Some effort is made to apply the techniques to ICT crimes in what follows, while realising that this is a preliminary exercise and the utility of the techniques will continue to emerge as this work evolves. What has emerged is that a wide range of these tactics can be tailored to specific types of electronic communication-related 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 [8].

Increasing the actual or perceived level of effort or risk involved in the commission of a crime will influence the likelihood of its occurrence. Likewise, reducing the actual or perceived benefit from committing a crime will reduce the likelihood it is committed.

The overall goal of crime-proofing, via the mechanisms identified as the 25 techniques, is to make crime less attractive to offenders by increasing the effort and risks, reducing the rewards, or reducing provocations and excuses

that encourage crime. The following picture illustrates this concept. These considerations must be borne in mind along with the aforementioned 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. The framework should be used as an aid to brainstorming and analysis that leads to identifying the mechanism by which crime proofing may be achieved.

It is interesting to observe among the 25 techniques the multitude of ways by which crime can be prevented. Crime proofing is sometimes improperly characterised as a simple notion of ‘target hardening’, which does not come close to conveying the impressive array of mechanisms by which crime or its harms can be reduced.

The 25 techniques are grouped into 5 main categories: each of these five categories contains five techniques that can be applied.

Increase Effort needed to commit the crime. Many potential offenders are deterred if a crime is too difficult. They do not have the requisite skills or are not willing to put in the time required. If it was easy to hack into banking systems then many more people would commit such crimes, but the amount of effort required (plus the risk and other issues addressed below) means they cannot.

1. **Target hardening:** inserting physical, technical or administrative barriers before reaching the point to commit a crime. A layered approach with several security layers may be useful.
2. **Control access** of subjects to facilities, networks, or resources. In the case of facilities this can be achieved for example with fences, CCTV and guards.
3. **Screen exits** of subjects that have entered the facilities or network. This may be as simple as having security guards checking departing staff and visitors.
4. **Deflect offenders** by reducing the possibility of them being in a situation to commit a crime. For example, a facility could close its premises to the public at a certain time and allow entrance only from a special entrance after that time.
5. **Control tools** that can be used by the offender. One typical example is the introduction of callerID in telephony, which led to the reduction of obscene telephone calls.

Increase Risk in committing the crime. Risk includes the risks of getting caught, 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 GPS or other tracking. More broadly however, risk is increased by surveillance 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 surveillance that reduces robbery.

6. **Extend guardianship** of the products to protect. Installing alarms that automatically make a call to the police is an example.
7. **Assist natural surveillance**, for example through the methodology of CPTED (Crime Prevention Through Environmental Design). As part of a facility's physical security, internal lighting of a banking institution during the night would be one example.

   In an ICT scenario, this might be translated into providing network awareness: where feasible, a product's identity and status should be visible to, and able to be monitored by, the network on demand across a trusted and secured channel.
8. **Reduce anonymity** of the offender. Anonymity is unavoidable to a certain extent when having to deal with large environments such as the

World Wide Web. Identification and access control mechanisms must be put in place.

For example, products may be electronically marked by adding an electronic identity to the product, in order to be able to track the physical or legal owner. The placement and integration of the electronic marking should be such that makes it economically unfeasible to remove, or impossible to repair the product.

An example of electronic marking is the use of RFID systems to identify and track products.

9. **Utilise place managers** that will be responsible for surveillance. Owners of systems or data can be responsible for these functions in an ICT environment.
10. **Strengthen formal surveillance** by police and security guards or personnel in charge of network security. This can be conducted in a number of ways, such as CCTV, Intrusion Detection Systems and other instruments.

Reduce Provocation which might lead to the crime.

11. **Conceal targets:** This can effectively reduce provocation. The product should be usable and easily reachable by the user, but not reveal too much information to a potential offender, nor arouse the will to commit a crime.
12. **Remove targets** of attacks. The products should not be unnecessarily available but should be put in place only for the duration of the desired service.
13. **Identify property**. Proper identification of the product can aid tracking the product, tracking the offender, and also raises awareness of user or owner of product on being "under his protection". Products may be physically and indelibly marked and, if possible, these markings should be tamper indicating: the markings should appear in as many places as possible and be of such nature to make changing them economically unfeasible.
14. **Disrupt markets** where the product can be resold and consequently reduce benefits for the perpetrator, or increase the risks.
15. **Deny benefits** from the crime. Products and services that are difficult to place in the market, or that have obstacles against their use by unauthorized subjects, reduce the benefits from crime-related activity. An ICT example would include removing ‘defaced’ websites rather than allowing hackers and others to view the results of their offences – since the reward here is psychological rather than monetary.

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. This means that people cannot validly claim they were unaware that illegal copying was an offence.

16. **Reduce frustration and stress,** which is one of the most common causes of unexpected violent episodes. For example, good customer services might reduce the likelihood of an ICT firm coming under threat of attack from frustrated customers with hacking skills.
17. **Avoid disputes** between subjects.
18. **Reduce emotional arousal:** situations that can potentially dangerous by creating violent attitudes should be avoided.
19. **Neutralise peer pressure** that can lead to collusion or individuals' crime activities.
20. **Discouraging imitation**. Imitation of hacking might be discouraged if publicity is not given to hacked websites.

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.

21. **Set rules:** setting rules about acceptable conduct can help avoid situational crime as any abnormal behaviour will stand out and be detected.
22. **Post instructions:** makes clear what is considered legal and what illegal activity in a specific situation. Making individuals aware that certain activity is illegal may discourage them from doing it
23. **Alert conscience:** helps raise awareness of the fact that an activity might be illegal.
24. **Assist compliance:** helping subjects to meet their needs in specific situations may discourage them from seeking alternative, unspecified and possibly illegal solutions.
25. **Control drugs and alcohol:** always a valid measure to assist crime prevention.

Additional considerations in Crime Proofing

Security and Privacy Issues

Actions to crime proof a product should be commensurate with the risks being addressed. Excessive or improper solutions may result in security breaches or invasion of the personal privacy of users. Products should ensure that the proofing techniques adopted do not compromise the privacy of their users.

Products that enable tracking and can give information on the location of people or their movements (such as RFIDs, mobile telephones or surveillance products) must ensure that only duly authorised organisations can access the relevant information. In addition, products should ensure that the security features introduced are such that they cannot be used for Denial of Service (DoS) attacks, do not block legitimate usage, and do not introduce vulnerabilities to the system they are applied to.

Usability Issues

The mechanisms and techniques introduced should not interfere significantly with the usability of the product. Security should be transparent, particularly for products that will be used by users without specific technical knowledge or skills. Expert users should be able to reduce the security level, but a default high level of security should be imposed for users of equipment and terminals.

Crime Detection: Lawful Interception and Retained Data

Lawful interception is legally sanctioned official access to private communications, such as telephone calls or e-mail messages. Lawful interception is a security process in which a service provider or network operator collects and provides the law enforcement officials with intercepted communications of private individuals or organizations.

Retained data refers to storage of this data, to be consulted by law enforcement authorities in case of need.

Lawful interception and Retained data play a crucial role in helping law enforcement agencies to combat criminal activity. ICT can be used by criminals to co-ordinate or even conduct serious criminal activities or terrorist activities. Products that store, transmit or process information from private communications should be able to provide this information to the Law Enforcement Authorities when requested.

Types of ICT Crime

The first step towards achieving an effective ICT product proofing methodology is to acquire a thorough knowledge base of the crimes committed, and of the techniques available to combat them. Thus awareness of the existing techniques of combating crime and fraud, as well as becoming familiar with the discipline of crime prevention, would be useful for ICT security professionals.

This section presents a summary of types of ICT crime and some of the countermeasures adopted.

Fixed Line Telephones

DISA (Direct Inward System Access) Fraud

Where the fraudster obtains information (for example a password) that is normally used legitimately by telecommunications employees, in order to make cheap calls via their Private Branch Exchange (PBX) connection [12].

Solutions:

- Enable automatic logging of calls if available.
- Regularly check the log records for repeated short duration calls to the same number. This could be an indication of an attempt to attack the system.
- Personal Identification Numbers (PINs) for voicemail, DISA and engineering access should, if enabled, be activated and changed regularly.
- If possible engineering access should only be permitted on a ‘call back’ basis; this will prevent unauthorised access to this privileged account**.**

(See also [25].)

Premium Rate Service (PRS) Fraud

In some instances a fraudster can attempt to make use of the service without paying for it. In other cases the PRS numbers may be dialled deliberately, in a fraudulent manner, by the same person that established the PRS service. This is a relatively easy form of fraud since often the agreement between the operator and PRS provider states that a share of the earnings will be due to the PRS provider, whether or not the operator is able to collect from the caller. This is because the PRS service provider is unable to ensure that all callers are legitimate [14].

Clip-on Fraud

Where the fraudster taps into an existing telephone line and can therefore communicate without being charged [14].

Calling Card Fraud

The fraudster obtains the calling card details from the victim by a variety of means. They then use those card details to make their own calls [14]. An obvious solution is for the caller to avoid displaying their calling card details.

Mobile Phones

Subscription Fraud

Subscription and superimposed or ‘surfing’ fraud are sometimes identified as the most prevalent types of fraud relating to telecommunications [33].

Subscription fraud occurs when a fraudster uses a false or fake identity to gain access to an electronic service, for example to obtain a subscription to a mobile phone. Since fake identification documentation is used to set up the account, the bill effectively goes to no-one and will never be paid, being absorbed instead by the company supplying the phone. The intention is to make costly phone calls, either for personal use or to generate income from a related Premium Rate Service (See Premium Rate Service Fraud).

Solutions:

- Credit worthiness checking software
- Cross-checks to external databases
- Biometric subscriber verification (voice recognition would be suited to this example)
- “ProFile”, an intercarrier database of accounts-receivable, write-offs and service shut-offs that provides on-line pre-screening of potentially fraudulent applicants. Helps identify applicants with a history of bad debt.
- “InSight”, a customer database that carriers scan for previously qualified applicants to eliminate the re-qualification process.

(See also [14]).

Superimposed fraud is where a service is used and charged to the account of an unsuspecting payee who has an account. In this scenario the person does exist and so they receive the bill for the services used by the fraudster [33].

Roaming fraud

Running up bills outside the home network (while ‘roaming’) with no intention of paying.

International roaming fraud is difficult to detect. Subscription fraud can be put into action to obtain mobile phones in one country, and then to ship them for use elsewhere. In the other countries, the phones may run up high rate and premium rate roaming call charges, and the legitimacy of a phone can be more difficult to check when it is used in a country far from its home network As a result, such abuses are estimated to run into billions of euros.

Solutions:

- Fraud Information Gathering System (FIGS) allows the network that roaming subscribers are entering to collect information about their activities. The network then sends this information back to the home

network of the subscriber, which can then clear certain types of calls and prevent fraudulent use of the system [13].

- Computer systems which speed the cross-checking system using neural network-based detection algorithms have the potential to speed up the checks, detect and deter such fraud. In some cases it has been noted that detection system speeds detection time by 50% and reduces fraudulent losses by 50% [32].

The following table gives an example of varieties of fraud, listing only those identified in relation to mobile phones [32].

Types of Mobile Phone Fraud

- Subscription fraud and identity theft
- Agent and reseller fraud
- Network and equipment hacking
- Internet exchange of fraud information
- Insider fraud and collusion
- Social engineering
- Premium rate service fraud
- Call selling operations
- International roaming fraud

Source: Based on Lloyd (2003) [32]

The GSM Association estimates that international mobile phone roaming fraud constitutes 24% of fraud relating to mobile phones [32]. Billing World estimates that wireless fraud accounts for between one and three percent of operator revenues, whilst the Gartner Group estimates that 50 to 70 percent of fraud losses are 'hidden' as bad debt, and there are reputed to have been single incidents of fraud of over half a million dollars per incident.

Cloning

Mobile phone cloning involves copying the identity of a mobile phone into another mobile phone, so that any calls made by the clone are billed to the account of the copied phone.

Solutions: Smart cards (see section on Smart Cards)

Theft of sensitive data

The crime in this case is self-explanatory. Sensitive data may include location information, identity-related information and the like.

Solutions:

- GSM and UMTS provide anonymity by using temporary identifiers when the feature is activated. When a user first switches on the mobile device,

the real identity is used and a temporary identifier is then issued. From then on, the temporary identifier is used, until the network requests the real identity again. Only by tracking the user is it possible to determine the temporary identity being used.

- For authentication and signalling protection ETSI has developed three security algorithms for GSM: A3, A5 and A8. The A3 and A8 algorithms are specific to the operator and are saved on the SIM card and in the authentication centre. A5 is saved in the mobile equipment and allows for data encryption and decryption over the air interface. Authentication is performed by a challenge and response mechanism.

Mobile Phone Theft

The crime in this case is self-explanatory.

Solutions: The GSM standards created by ETSI include the definition of a system (also adopted in UMTS) to prevent handset theft based on a handset identity number called the International Mobile Equipment Identity (IMEI). This is a unique number attributed during handset manufacturing, registered by the Mobile Network Operator (MNO) and held electronically on the mobile phone. MNOs may use the IMEI to blacklist mobile equipment that is reported stolen.

Internal or Accounting Fraud

A more conventional fraud, often involving insiders, where charges are reduced or discounts fraudulently claimed for mobile phone services. This crime is applied to mobile technology, but does not necessarily use the technology as an instrument.

Solutions:

- Use audit logs in the systems
- Separation of duties for employees
- Job rotation of employees to avoid collusion

Broadcast/Pay TV

Pay-per-view or subscription-based services fraud

Digital television, such as pay-per-view and satellite television, is subject to attacks that acquire access to content without proper authorization (see also the section below on Content Theft in the Internet).

According to AEPOC [35] , theft or piracy of Pay-TV in Europe takes two common forms:

- Coded Pay-TV signals for digital transmission are stolen by private viewers
- Local TV stations and cable networks illegally transmit content that does not belong to them.

In both cases, programming is illegally accessed by forging the smart cards and digital decoders necessary to receive the signals.

AEPOC [35] considers that at least one billion euros are spent in the European Union every year on pirate smart cards and decoding equipment used to hack into Pay-TV. A Datamonitor report [15] states that operators will lose 700 million euros between 2004 and 2010 in Eastern Europe.

Sometimes the term Conditional Access (CA) is used to describe the protection of content by requiring certain criteria to be met before granting access to this content. The corresponding content theft technique is called "pirate decryption".

Solutions: The Common Scrambling Algorithm (CSA) of the Digital Video Broadcasting (DVB) Project allows video streams to be encrypted. A set of encrypted control messages is sent out embedded in the video signal every 10-120 seconds. At the user end, the hardware (e.g. the pay-TV box) takes in those control messages and processes them (using an algorithm that is proprietary to the broadcaster, called the ‘conditional access mechanism’) to create ‘control words’.

The CSA is a product of the Joint Technical Committee (JTC) “Broadcast”, a collaboration between ETSI, the European Broadcasting Union (EBU) and CENELEC.

Internet

Hacking

A hacking *attack* can be defined as [31]:

> "a series of intentional steps taken by an attacker to achieve an unauthorised result".

A hacking *incident* can be defined as [31]:

> "a group of related attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites and timing".

Hacking takes various forms as described in the following table.

No	Type of Attack	Attack Variations
1	Denial of Service	Local process degradation
2		Local disk space exhaustion
3		Local Index node (Inode) exhaustion
4		Network client side aimed at a particular product
5		Network client side aimed at a particular service
6		Local process degradation or disk exhaustion achieved via a network e.g. SYN flooding
7	Information leakage	Service information leakage e.g. via error messages
8		Protocol information leakage e.g. via a system query command
9		Leaky by design e.g. SNMP
10		Inherently leaky e.g. some web design tools
11	Regular file access	Changes of permission
12		Symbolic link attacks
13	Misinformation	e.g. editing to create conflicting entries
14		Rootkits (packages designed to alter key programs)
15		Malicious kernel modules
16	Special file/database access	Special files such as RunAs in Windows 2000 can allow unauthorised users to log on as someone else
17		Data base files: attack through Web interfaces, inherent database software vulnerabilities and weaknesses in permission regimes
18	Remote arbitrary code execution	Usually prefaced by information gathering attack, uses automated tools to gain local administrative access
19	Elevation of privileges	Remote unprivileged access through, for example, Web interfaces
20		Remote privilege access exploiting operating system weaknesses

Source: CMA (2006; 30)

Other types of Internet fraud

Many types of 'conventional' fraud have migrated to ICT, thanks to the ease of access to potential victims afforded by modern communications technology. Examples include: online auction and retail fraud, online investment fraud, credit-card schemes, tele-working and business opportunity fraud.

For instance, in online auction and retail fraud, the fraudsters place high-value, but non-existent, items for sale on internet auction sites, or on their own

temporary website. They then take payment but do not provide the goods as specified.

The other frauds are similar: the general principle is that they offer a service or opportunity that is not provided, the objective being to either receive payment from the victim or to harvest credit card details etc.

Cyberstalking

In cyberstalking, the victim is harassed and threatened by unwanted e-mail and messages posted on bulletin board services by people with whom they have interacted on the Internet [30].

Content Theft

Content theft relates to file sharing networks for music and video; copying, sharing of software; ripping CDs and DVDs freely available via the Internet.

Solutions:

- Encryption prevents intercepted content from being used or resold without the key.
- DRM (Digital Rights Management) permits only the purchaser of the content to view it, and prevents copies being made.

The Illegal Use of Electronic Services

Copyright theft and identity theft touch on the issue of the illegal use of electronic services. Moreover, other forms of crime are greatly facilitated by electronic services, including the transmission of child pornography and other illicit material.

Misuse of Electronic Services

Electronic services are frequently misused. Bombardment with spam emails is an infamous form, as are spam SMS texts to mobile phones, and short-duration ‘dropped calls’ to mobile phones (where a recipient who returns the call to a revenue-share number is charged at a high rate). In some countries formal misuse of electronic services can warrant legal action (e.g. [34]).

Wireless Communications

Bluetooth

Bluetooth is a wireless technology that allows computers, phones and other devices to talk to each other over short distances (typically about 10 metres). Bluetooth uses radio waves (in the 2.4 GHz range), and is designed to be a secure and inexpensive way of connecting and exchanging information between devices without wires. Bluetooth capability is embedded in many of the newer mobile phones, handheld computers, laptops, printers, handheld organisers, and other devices.

The following Bluetooth-related crimes are well-known [27].

Bluesnarfing

Lets an attacker retrieve contact list, calendar data and any multimedia objects from Bluetooth devices.

Solutions: Avoid encryption mode 1 (no encryption), choosing either mode 2 (encrypt unicast but not broadcast traffic) or better still mode 3 (encrypt all traffic). Because data that has been encrypted with too short a key can be analysed to decrypt captured traffic, both devices should be configured to require 128-bit encryption keys.

Backdoor

In the backdoor attack, a trust relationship is established through the "pairing" mechanism. The attack is designed so that the attacking device does not appear in the target's register of paired devices. The victim does not notice the attack unless they happen to spot the pairing when it is first made. The attacker is then potentially free to continue to use any resource that a trusted relationship with that device grants access to. This means that not only can data be retrieved from the phone or other device, but other services, such as modems or Internet, WAP and GPRS gateways may be accessed without the owner's knowledge or consent. Once a backdoor is installed, (Blue)Snarf attacks may be possible on devices that previously denied access, and without the restrictions normally presented to a plain snarf attack.

Bluebug

Lets an attacker make calls on another Bluetooth phone.

BlueDump

Cracks PIN codes by watching Bluetooth devices bond (pair).

Bluejacking

Lets an attacker add contacts to a Bluetooth device's phonebook or send unsolicited messages to a phone without knowing its number. Currently relatively harmless (and therefore not illegal) but potentially threatening.

BlueSmack
Crashes a Bluetooth device by sending a "ping-of-death" message.

Bluestab
Uses badly formatted names to crash a device during Bluetooth discovery.

In general, the mere ability of an attacker to identify the presence of devices, even if they are physically hidden, by detecting their Bluetooth signals, puts those devices at greater risk of theft or other crime.

General best practices for Bluetooth:

- Turn off Bluetooth interfaces when not in use, and
- Disable Bluetooth's discovery feature, whereby each device announces itself to all nearby devices.
- Configure Bluetooth devices to use the lowest power that meets business needs. Class 3 devices transmit at 1 mW and cannot communicate beyond 10 metres, while class 1 devices transmit at 100 mW to reach up to 100 metres. Adjusting power does not eliminate outsider attack, but it can reduce that possibility.
- Because link keys are stored on paired Bluetooth devices, password protect both devices to prevent use of lost/stolen units.
- If possible, do not permanently store the pairing PIN code on Bluetooth devices.

Wireless Local Area Networks (WLANs)

Wireless Local Area Networks used typically for wireless networking in nomadic environments are faster and have a greater range than Bluetooth. Among the well-known attacks that can be applied to WLANs are the following:

Phishing
A phisher creates a fraudulent spoof website which appears to be the log-in page to a WLAN network. When the user logs in through the website script viruses and trojans are sent to the user’s computer.

“Evil Twin”
Associated with phishing. A hacker masquerades as a company or public wireless router (hotspot), often by using a portable router with a stronger antenna. Network software can then be used to monitor the WLAN network and obtain sensitive information.

Solutions:

- Wi-Fi Protected Access (WPA)
- WPA2

Applying the 25 Techniques to ICT Crimes

Taking the examples of possible ICT Crime described in the preceding pages, the following table is a preliminary attempt to map existing crime proofing efforts relating to ICT crimes against the 25 techniques. Some of the solutions presented are intentionally based on existing ICT standards, in order to illustrate the level of contribution that the standardization community can offer to Product Proofing.

In particular, solutions to which ETSI has contributed, or is in the process of contributing, are underlined.

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocations	Remove Excuses
1. Target harden	***6. Extend guardianship***	***11. Conceal targets***	***16. Reduce frustrations and stress***	***21. Set rules***
ETSI GSM and DECT algorithms for encryption and authentication	RFID tags	Temporary identifiers used for radio transmissions between authorisation requests	UICC allowing multiple separate user verifications.	Use of networks under specific policy to make unauthorised users stand out
Firewalls, antivirus, De-Militarised Zones (DMZs)	Fraud Information Gathering System (FIGS)	Turn off the 'discoverable' Bluetooth connection option	Reduce cost for end-users of products that are popular	
Common Scrambling Algorithm for Digital Video Broadcast (ETSI JTC Broadcast)		De-Militarised Zones (DMZs) in networks to conceal important resources		
2. Control access	***7. Assist natural surveillance***	***12. Remove targets***	***17. Avoid disputes***	***22. Post instructions***
Cordless telephony: ETSI DECT Standard Authentication Algorithm	Point out that bluesnarfing is in progress by a clear alert to the user via a change in Bluetooth connection symbol	Bluetooth devices which turn off when not in use.	Chat, blog and mailing list moderation	Log in screens that make it clear that the computer is for authorised access only
Smart Cards: ETSI SCP standards.				Security policy to be signed by employees

3. Screen exits	***8. Reduce anonymity***	***13. Identify property***	***18. Reduce emotional arousal***	***23. Alert conscience***
Implement audit logs	ETSI ESI standards for electronic signatures.	ETSI ESI standards for electronic signatures.		Pop-up windows declaring "illegal access attempt".
Practice lawful interception and retained data analysis	Prevent hackers from hiding behind spoofed IP addresses	RFID tags		Insert piracy awareness raising notifications
	Caller ID in telephony	IMEI of mobile phones registered		
4. Deflect offenders	***9. Utilise place managers***	***14. Disrupt markets***	***19. Neutralise peer pressure***	***24. Assist compliance***
	Intrusion Detection Systems with inference capability	Provide affordable mobile phones to stop black market	Encourage the attitude that hacking is illegal	UICC allowing multiple separate user verifications, so stopping sharing of passwords.
		Checks on mobile phone shops.		

5. Control tools/ weapons	*10. Strengthen formal surveillance*	*15. Deny benefits*	*20. Discourage imitations*	*25. Control drugs and alcohol*
Blacklisting stolen mobile phones via their IMEI renders them useless as instruments in other crimes.	Practice lawful interception and retained data analysis	Blacklist stolen IMEIs so the mobile no longer works.	Failure of hacking attempts being notified on forums, or peer-to-peer networks.	
	RFID tags	FIGS used to cut off fraudulent users.	Details of techniques of hacking attacks and crimes are not circulated in a vast manner	

Underlined text identifies solutions to which ETSI has contributed or is in the process of contributing.

Conclusions and Recommendations

This White 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 assist product proofing against crime. Examples have been given of where crime takes place in ICT, and some instances presented of standards designed to combat such crime.

The White Paper has highlighted the fact that there are many types of crime of relevance to 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: that knowledge platform is still in its early stages of development.

The assessment of the current situation in crime-proofing against ICT crime has resulted in a series of recommendations. These are embodied in the following key areas identified as requiring further work in response to the European Commission Mandate M/355:

1. **Further work in exploring the area of ICT product proofing against crime** is required to clarify more precisely which crimes fall within the area of ICT and ETSI. Also, the '25 techniques' need to be further studied with regard to the specific characteristics of ICT products and services".
2. A series of **areas where standardisation on crime proofing should take place** should be identified: this White Paper has illustrated how effective crime-proofing can only take place on a case-by-case basis. Some areas where technology-specific standards concerning crime proofing can be produced have been already identified in this document (e.g. *RFID* and *mobile telecommunications*).
3. Information on ICT crime proofing is currently largely fragmented. To promote standards for crime proofing, a **knowledge base of effective and efficient crime proofing techniques** should be built up and shared within the relevant communities, enabling best practice to be spread as efficiently as possible.
4. A **network of experts** should be set up to help share the knowledge and bring telecommunications, information technology and criminology professionals closer.

Within this ETSI White Paper the principles of crime proofing were illustrated. The continuing challenge is applying these principles within standards that will give life to products and services in the real world.

References

[1] EC DG Justice and Home Affairs – 'Programming mandate addressed to the ESOs for the elaboration of European Standards to identify and reduce crime risk in products and services'

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

[4] Grabosky, P.N. (1998). *Technology and Crime Control*, Trends and Issues in Crime and Criminal Justice, no. 78, Australian.

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

[6] Clarke, Ronald V.(ed). (1997) *Situational Crime Prevention: Successful Case Studies (2nd edition)*. New York: Harrow and Heston.

[7] Cornish, D. and Clarke, R. (1986). *The Reasoning Criminal*. New York, NY: Springer-Verlag.

[8] Newman, G. R. and Clarke, R.V. (2006) *Superhighway Robbery: Preventing E-Commerce Crime*. Cullompton: Willan publishing.

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

[10] Armitage, R.; Clarke, R.; Di Nicola, A.; Montauti, M.; Pease, K.; Savona, E. (2006) Definition of final crime risk assessment mechanism to measure the risk of theft of electronic products and proof them against theft

[11] Gamman, L and Pascoe, T. (2004) Design Out Crime? Using Practice-based Models of the Design Process. Crime Prevention and Community Safety Journal: An International Journal. 2004, 6 (4), 37-56.

[12] Pollard, Craig (2005) 'Telecom fraud: The cost of doing nothing just went up' (White Paper), accessed via www.insight.co.uk/downloads/whitepapers.htm November 2006.

[13] Brookson, C and Zumerle, D. (2006) 'Information Security Standardization – the ETSI perspective', ISSE 2006 Securing Electronic Business Processes.

[14] Wall, D.S. (2000) 'Policing the internet: maintaining order and law on the cyber-beat', Chapter 7 in Akdeniz, Y., Walker, C.P. and Wall. D.S. (eds) (2000) *The Internet, Law and Society*, London: Longman.

[15] Datamonitor (2005) 'Digital pay-TV Piracy in Eastern Europe. The need for a secure and flexible conditional access system.' Datamonitor, August 2005. Accessed via http://nds.com/pdfs/Datamonitor_EE_Piracy_whitepaper_August2005.pdf on 18 January 2005.

[16] Foresight Crime Prevention Panel (2000) *Just Around the Corner*, London: Department of Trade and Industry; URN 00/674.

[17] Whatis (2006) Search term 'Internet Protocol'. Accessed via www.whatis.com, November 2006.

[18] The Bunker (2006) Accessed via http://www.thebunker.net/resources/bluetooth, November 2006

[19] Filesaveas (2006) Accessed via http://www.filesaveas.com/wifi.html, November 2006

[20] 'MiniMe' and 'Mahajivana' (2006) 'RFID-Zapper', 22nd Chaos Communication Congress, December 27th to 30th, 2005, Berlin. Accessed via https://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN), November 2006.

[21] Mann, D. and Sutton, M. (1998) 'Netcrime: More change in the organisation of thieving', *British Journal of Criminology*, vol 38, pp. 210-229.

[22] Pease, K. (forthcoming) "Crime Futures: the challenge of crime in the information age" in Wall, D.S. (ed) (forthcoming) Crime and the Internet, London: Routledge.

[23] Saunders, K. and Zucker, B. (1999) 'Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act', in Wall, D. (ed), special issue on E-Commerce, *International Review of Law, Computers and Technology*, vol. 13, no. 2.

[24] Fraud Management – White Paper, Goulet Telecom (TBC)

[25] Garda Crime Prevention Advice. Accessed via http://www.garda.ie/angarda/crimeprevent9.html, Nov 2006.
[26] Long, M. Combating Wi-Fi's evil twin. *News Factor Network*; www.wirelessnewsfactor.com/story.xhtml?story_id=31469, Mar. 21, 2005 (accessed Nov, 2006).
[27] Phifer, L (2006) Accessed via "Taking the Bite out of Bluetooth", accessed via http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1223151,00.html, November 2006
[28] Rankl, W. , Effing, W. (1997) Smart Card Handbook, John Wiley & Sons, Inc., New York, NY
[29] Rieback, M., Crispo, B. and Tanenbaum A. (2006) "Is Your Cat Infected with a Computer Virus?", Fourth IEEE International Conference on Pervasive Computing and Communications (PerCom'06) pp. 169-179
[30] Tavani, H. and Grodzinsky, F. (2002) "Cyberstalking, personal privacy, and moral responsibility", Ethics and Information Technology, Volume 4, Number 2 / June, 2002, pp. 123-132.
[31] Moitra, S. D. and S.L. Konda. 2004. 'An empirical investigation of network attacks on computer systems' *Computers and Security*, 23, 43-51.
[32] Lloyd, D. 2003. *International Roaming Fraud: Trends and Prevention Techniques*. 17 December 2003: Fair Isaac Corporation.
[33] Bolton, R.J. and D.J. Hand. 2002. 'Statistical fraud detection: A review' *Statistical Sciences*, 17(3), 235-255.
[34] Ofcom. 2005. 'A consultation on persistent misuse' *In The Frame: The Regular TUFF Newsletter*. The Telecommunications United Kingdom Fraud Forum.
[35] AEPOC (undated) Accessed via http://www.aepoc.org/press_service/hi_aeback.html on 18 January 2005.)
[36] COM (2003) Commission of the European Communtities: On the legal protection of Electronic Pay Services. Accessed via http://www.eu.int/comm/internal_market/media/docs/elecpay/com-2003-198_en.pdf on 18 January 2005.
[37] Datamonitor (2005) "Digital pay-TV Piracy in Eastern Europe. The need for a secure and flexible conditional access system." Datamonitor, August 2005. Accessed via http://nds.com/pdfs/Datamonitor_EE_Piracy_whitepaper_August2005.pdf on 18 January 2005.
[38] BBC (2001) "Toasting the Crackers" Accessed via http://news.bbc.co.uk/1/hi/sci/tech/1138550.stm on 18 January 2005
[39] Financial Services Authority, "Countering Financial Crime Risks in Information Security" Financial Crime Sector Report, November 2004
[40] "Product Proofing Against Crime", Jen Mailley, Shaun Whitehead, and Professor Graham Farrell, Midlands Centre for Criminology and Criminal Justice, Loughborough University, U.K., ETSI 2nd Security Workshop
[41] An online interactive version of the 25 techniques is at www.popcenter.org/25techniques.htm. The most recent edition of the techniques is: 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 Justice Press. (at: http://www.popcenter.org/Library/CrimePrevention/Volume%2016/OpportunitiesPrecipitators.pdf).
[42] For cost of crime estimates see, for example, Dubourg, R., J. Hamed and J. Thorns. 2005. The Economic and Social Cost of Crime against Individuals and Households 2003/4. Online report 30/5. London: Home Office. (at: www.homeoffice.gov.uk/rds/pdfs05/rdsolr3005.pdf).

Abbreviations

AEPOC	European Association for the Protection of Encrypted Works and Services
CA	Conditional Access
CallerID	Caller Identity
CCTV	Closed-Circuit Television
CD	Compact Disk
CENELEC	European Committee for Electrotechnical Standardisation
CPTED	Crime Prevention Through Environmental Design
CRAVED	Concealable, Removable, Available, Valuable, Enjoyable, Disposable
CSA	Common Scrambling Algorithm
DECT	Digital Enhanced Cordless Telecommunication
DISA	Direct Inward System Access (PBX function)
DMZ	De-Militarised Zone
DoS	Denial of Service
DRM	Digital Rights Management
DVB	Digital Video Broadcasting
DVD	Digital Versatile Disk
EBU	European Broadcasting Union
ESI	(ETSI Committee) Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute
FIGS	Fraud Information Gathering System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile communication
ICT	Information and Communication Technologies
IMEI	International Mobile Equipment Identity
IT	Information Technology
JTC	Joint Technical Committee
MNO	Mobile Network Operator
PBX	Private Branch Exchange
PIN	Personal Identification Number
PRS	Premium Rate Service
RFID	Radio Frequency Identification
SCP	(ETSI Committee) Smart Card Platform
SIM	Subscriber Identity Module
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TV	Television
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
WAP	Wireless Application Protocol
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2